strongSwan - Feature #762

EAP-TLS did not work with android client

10.11.2014 06:48 - chethan mallaiah

Status:	Closed	**Start date:**	10.11.2014
Priority:	Normal	**Due date:**	
Assignee:	Martin Willi	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.3.0		
Resolution:	Fixed		

Description

I had setup strongSwan vpn instance with eap-tls configuration. But whenever i tried to connect to the vpn server it fails with below error,

my ipsec.conf

```
conn %default
 keyexchange=ikev2

conn roadwarrior
 left=%any
 leftauth=eap-tls
 leftcert=serverCert.pem
 leftid=camellia.idc.devlab.motive.com
 leftsubnet=0.0.0.0/0,::/0
 right=%any
 rightsourceip=10.0.1.0/24
 #rightauth=pubkey
 rightcert=clientCert.pem
 #rightid="C=IN, O=motive, CN=client"
 #rightsendcert=never
 rightauth=eap-tls
 auto=add
 esp=aes-aes256-sha-modp1024,aes256-sha512-modp4096
 ike=aes-aes256-sha-modp1024,aes256-sha512-modp4096
```

my strongswan server log;

```
02[NET] received packet: from 135.250.91.52[36689] to 135.250.90.29[500] (996 bytes)
02[ENC] parsed IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N((16430)) ]
02[IKE] 135.250.91.52 is initiating an IKE_SA
02[IKE] remote host is behind NAT
02[IKE] DH group MODP_2048 inacceptable, requesting MODP_1024
02[ENC] generating IKE_SA_INIT response 0 [ N(INVAL_KE) ]
02[NET] sending packet: from 135.250.90.29[500] to 135.250.91.52[36689] (38 bytes)
03[NET] received packet: from 135.250.91.52[36689] to 135.250.90.29[500] (868 bytes)
03[ENC] parsed IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N((16430)) ]
03[IKE] 135.250.91.52 is initiating an IKE_SA
03[IKE] remote host is behind NAT
03[IKE] sending cert request for "C=IN, O=motive, CN=UDM Root CA"
03[ENC] generating IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(MULT_AUTH
) ]
03[NET] sending packet: from 135.250.90.29[500] to 135.250.91.52[36689] (337 bytes)
04[NET] received packet: from 135.250.91.52[36275] to 135.250.90.29[4500] (3532 bytes)
04[ENC] parsed IKE_AUTH request 1 [ IDi N(INIT_CONTACT) CERTREQ CPRQ(ADDR ADDR6 DNS DNS6) N(ESP_TF
C_PAD_N) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_ONLY) ]
04[IKE] received cert request for "C=IN, O=motive, CN=UDM Root CA"
04[IKE] received 148 cert requests for an unknown ca
04[CFG] looking for peer configs matching 135.250.90.29[%any]...135.250.91.52[C=IN, O=motive, CN=c
lient]
04[CFG] selected peer config 'roadwarrior'
04[IKE] initiating EAP_TLS method (id 0x0A)
```

```
04[IKE] received ESP_TFC_PADDING_NOT_SUPPORTED, not using ESPv3 TFC padding
04[IKE] peer supports MOBIKE
04[ENC] generating IKE_AUTH response 1 [ IDr EAP/REQ/TLS ]
04[NET] sending packet: from 135.250.90.29[4500] to 135.250.91.52[36275] (124 bytes)
05[NET] received packet: from 135.250.91.52[36275] to 135.250.90.29[4500] (252 bytes)
05[ENC] parsed IKE_AUTH request 2 [ EAP/RES/TLS ]
05[TLS] negotiated TLS 1.2 using suite TLS_DHE_RSA_WITH_AES_128_CBC_SHA
05[TLS] sending TLS server certificate 'C=IN, O=motive, CN=camellia.idc.devlab.motive.com'
05[TLS] sending TLS cert request for 'C=IN, O=motive, CN=UDM Root CA'
05[ENC] generating IKE_AUTH response 2 [ EAP/REQ/TLS ]
05[NET] sending packet: from 135.250.90.29[4500] to 135.250.91.52[36275] (1100 bytes)
06[NET] received packet: from 135.250.91.52[36275] to 135.250.90.29[4500] (76 bytes)
06[ENC] parsed IKE_AUTH request 3 [ EAP/RES/TLS ]
06[ENC] generating IKE_AUTH response 3 [ EAP/REQ/TLS ]
06[NET] sending packet: from 135.250.90.29[4500] to 135.250.91.52[36275] (876 bytes)
07[NET] received packet: from 135.250.91.52[36275] to 135.250.90.29[4500] (1100 bytes)
07[ENC] parsed IKE_AUTH request 4 [ EAP/RES/TLS ]
07[ENC] generating IKE_AUTH response 4 [ EAP/REQ/TLS ]
07[NET] sending packet: from 135.250.90.29[4500] to 135.250.91.52[36275] (76 bytes)
08[NET] received packet: from 135.250.91.52[36275] to 135.250.90.29[4500] (460 bytes)
08[ENC] parsed IKE_AUTH request 5 [ EAP/RES/TLS ]
08[TLS] received TLS peer certificate 'C=IN, O=motive, CN=client'
08[CFG]   using trusted ca certificate "C=IN, O=motive, CN=UDM Root CA"
08[CFG] checking certificate status of "C=IN, O=motive, CN=client"
08[CFG] certificate status is not available
08[CFG]   reached self-signed root ca with a path length of 0
08[CFG]   using trusted certificate "C=IN, O=motive, CN=client"
08[ENC] generating IKE_AUTH response 5 [ EAP/REQ/TLS ]
08[NET] sending packet: from 135.250.90.29[4500] to 135.250.91.52[36275] (156 bytes)
09[NET] received packet: from 135.250.91.52[36275] to 135.250.90.29[4500] (76 bytes)
09[ENC] parsed IKE_AUTH request 6 [ EAP/RES/TLS ]
09[IKE] EAP method EAP_TLS succeeded, MSK established
09[ENC] generating IKE_AUTH response 6 [ EAP/SUCC ]
09[NET] sending packet: from 135.250.90.29[4500] to 135.250.91.52[36275] (76 bytes)
10[NET] received packet: from 135.250.91.52[36275] to 135.250.90.29[4500] (92 bytes)
10[ENC] parsed IKE_AUTH request 7 [ AUTH ]
10[IKE] authentication of 'C=IN, O=motive, CN=client' with EAP successful
10[CFG] constraint check failed: peer not authenticated with peer cert 'C=IN, O=motive, CN=client'
.
10[CFG] selected peer config 'roadwarrior' inacceptable: non-matching authentication done
10[CFG] no alternative config found
10[ENC] generating IKE_AUTH response 7 [ N(AUTH_FAILED) ]
10[NET] sending packet: from 135.250.90.29[4500] to 135.250.91.52[36275] (76 bytes)
```

then, below is my strongswan log for android device;

```
Nov  7 12:42:24 00[DMN] Starting IKE charon daemon (strongSwan 5.2.1dr1, Linux 3.4.42-g6c9aef2-001
10-gd543d01, armv7l)
Nov  7 12:42:24 00[KNL] kernel-netlink plugin might require CAP_NET_ADMIN capability
Nov  7 12:42:24 00[LIB] loaded plugins: androidbridge charon android-log openssl fips-prf random n
once pubkey pkcs1 pkcs8 pem xcbc hmac socket-default kernel-netlink eap-identity eap-mschapv2 eap-
md5 eap-gtc eap-tls
Nov  7 12:42:24 00[LIB] unable to load 9 plugin features (9 due to unmet dependencies)
Nov  7 12:42:24 00[JOB] spawning 16 worker threads
Nov  7 12:42:24 08[CFG] loaded user certificate 'C=IN, O=motive, CN=client' and private key
Nov  7 12:42:24 08[CFG] loaded CA certificate 'C=IN, O=motive, CN=UDM Root CA'
Nov  7 12:42:24 08[IKE] initiating IKE_SA android[8] to 135.250.90.29
Nov  7 12:42:24 08[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FR
AG_SUP) ]
Nov  7 12:42:24 08[NET] sending packet: from 192.168.0.190[60711] to 135.250.90.29[500] (996 bytes
)
Nov  7 12:42:24 11[NET] received packet: from 135.250.90.29[500] to 192.168.0.190[60711] (38 bytes
)
Nov  7 12:42:24 11[ENC] parsed IKE_SA_INIT response 0 [ N(INVAL_KE) ]
Nov  7 12:42:24 11[IKE] peer didn't accept DH group MODP_2048, it requested MODP_1024
Nov  7 12:42:24 11[IKE] initiating IKE_SA android[8] to 135.250.90.29
Nov  7 12:42:24 11[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FR
```

```
AG_SUP) ]
Nov  7 12:42:24 11[NET] sending packet: from 192.168.0.190[60711] to 135.250.90.29[500] (868 bytes
)
Nov  7 12:42:24 12[NET] received packet: from 135.250.90.29[500] to 192.168.0.190[60711] (337 byte
s)
Nov  7 12:42:24 12[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ
 N(MULT_AUTH) ]
Nov  7 12:42:24 12[IKE] local host is behind NAT, sending keep alives
Nov  7 12:42:25 12[IKE] received cert request for "C=IN, O=motive, CN=UDM Root CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, ST=UT, L=Salt Lake City, O=The USERTRUST N
etwork, OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=GeoTrust Inc., CN=GeoTrust Global CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=RO, O=certSIGN, OU=certSIGN ROOT CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=Digital Signature Trust, OU=DST ACES, CN
=DST ACES CA X6"
Nov  7 12:42:25 12[IKE] sending cert request for "C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Con
sulting cc, OU=Certification Services Division, CN=Thawte Premium Server CA, E=premium-server@thaw
te.com"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=GeoTrust Inc., OU=(c) 2007 GeoTrust Inc.
 - For authorized use only, CN=GeoTrust Primary Certification Authority - G2"
Nov  7 12:42:25 12[IKE] sending cert request for "C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalS
ign Root CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=GB, ST=Greater Manchester, L=Salford, O=Comodo
 CA Limited, CN=Secure Certificate Services"
Nov  7 12:42:25 12[IKE] sending cert request for "C=DE, O=D-Trust GmbH, CN=D-TRUST Root Class 3 CA
 2 2009"
Nov  7 12:42:25 12[IKE] sending cert request for "C=NO, O=Buypass AS-983163327, CN=Buypass Class 3
 CA 1"
Nov  7 12:42:25 12[IKE] sending cert request for "C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN
=AddTrust Class 1 CA Root"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, ST=Arizona, L=Scottsdale, O=Starfield Tech
nologies, Inc., CN=Starfield Services Root Certificate Authority - G2"
Nov  7 12:42:25 12[IKE] sending cert request for "O=RSA Security Inc, OU=RSA Security 2048 V3"
Nov  7 12:42:25 12[IKE] sending cert request for "C=ch, O=Swisscom, OU=Digital Certificate Service
s, CN=Swisscom Root CA 2"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=GeoTrust Inc., CN=GeoTrust Primary Certi
fication Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "C=PL, O=Unizeto Sp. z o.o., CN=Certum CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=HU, L=Budapest, O=NetLock Halozatbiztonsagi Kf
t., OU=Tanusitvanykiadok, CN=NetLock Uzleti (Class B) Tanusitvanykiado"
Nov  7 12:42:25 12[IKE] sending cert request for "CN=TÃ?RKTRUST Elektronik Sertifika Hizmet SaÄ?la
yÄ±cÄ±sÄ±, C=TR, L=Ankara, O=TÃ?RKTRUST Bilgi Ä°letiÅ?im ve BiliÅ?im GÃ¼venliÄ?i Hizmetleri A.Å?.
(c) KasÄ±m 2005"
Nov  7 12:42:25 12[IKE] sending cert request for "C=DE, O=T-Systems Enterprise Services GmbH, OU=T
-Systems Trust Center, CN=T-TeleSec GlobalRoot Class 3"
Nov  7 12:42:25 12[IKE] sending cert request for "C=BM, O=QuoVadis Limited, CN=QuoVadis Root CA 2"

Nov  7 12:42:25 12[IKE] sending cert request for "C=FR, O=Dhimyotis, CN=Certigna"
Nov  7 12:42:25 12[IKE] sending cert request for "C=CH, O=SwissSign AG, CN=SwissSign Silver CA - G
2"
Nov  7 12:42:25 12[IKE] sending cert request for "C=PL, O=Unizeto Technologies S.A., OU=Certum Cer
tification Authority, CN=Certum Trusted Network CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=VeriSign, Inc., OU=VeriSign Trust Networ
k, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certif
ication Authority - G5"
Nov  7 12:42:25 12[IKE] sending cert request for "C=IL, O=StartCom Ltd., OU=Secure Digital Certifi
cate Signing, CN=StartCom Certification Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "CN=Atos TrustedRoot 2011, O=Atos, C=DE"
Nov  7 12:42:25 12[IKE] sending cert request for "CN=TÃ?RKTRUST Elektronik Sertifika Hizmet SaÄ?la
yÄ±cÄ±sÄ±, C=TR, L=ANKARA, O=(c) 2005 TÃ?RKTRUST Bilgi Ä°letiÅ?im ve BiliÅ?im GÃ¼venliÄ?i Hizmetle
ri A.Å?."
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Di
giCert High Assurance EV Root CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=DK, O=TDC Internet, OU=TDC Internet Root CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=SK, L=Bratislava, O=Disig a.s., CN=CA Disig Ro
ot R2"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=GeoTrust Inc., OU=(c) 2008 GeoTrust Inc.
```

```
 - For authorized use only, CN=GeoTrust Primary Certification Authority - G3"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=Entrust, Inc., OU=See www.entrust.net/le
gal-terms, OU=(c) 2012 Entrust, Inc. - for authorized use only, CN=Entrust Root Certification Auth
ority - EC1"
Nov  7 12:42:25 12[IKE] sending cert request for "OU=GlobalSign Root CA - R2, O=GlobalSign, CN=Glo
balSign"
Nov  7 12:42:25 12[IKE] sending cert request for "C=ch, O=Swisscom, OU=Digital Certificate Service
s, CN=Swisscom Root EV CA 2"
Nov  7 12:42:25 12[IKE] sending cert request for "C=TR, L=Ankara, O=E-TuÄ?ra EBG BiliÅ?im Teknoloj
ileri ve Hizmetleri A.Å?., OU=E-Tugra Sertifikasyon Merkezi, CN=E-Tugra Certification Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "C=KR, O=KISA, OU=Korea Certification Authority C
entral, CN=KISA RootCA 3"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=GeoTrust Inc., CN=GeoTrust Universal CA"

Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=SecureTrust Corporation, CN=SecureTrust
CA"
Nov  7 12:42:25 12[IKE] sending cert request for "CN=ACCVRAIZ1, OU=PKIACCV, O=ACCV, C=ES"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=Equifax Secure Inc., CN=Equifax Secure e
Business CA-1"
Nov  7 12:42:25 12[IKE] sending cert request for "C=EU, L=Madrid (see current address at www.camer
firma.com/address), SN=A82743287, O=AC Camerfirma S.A., CN=Chambers of Commerce Root - 2008"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=Entrust, Inc., OU=See www.entrust.net/le
gal-terms, OU=(c) 2009 Entrust, Inc. - for authorized use only, CN=Entrust Root Certification Auth
ority - G2"
Nov  7 12:42:25 12[IKE] sending cert request for "C=IL, O=StartCom Ltd., CN=StartCom Certification
 Authority G2"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=VISA, OU=Visa International Service Asso
ciation, CN=Visa eCommerce Root"
Nov  7 12:42:25 12[IKE] sending cert request for "C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter C
lass 2 CA, CN=TC TrustCenter Class 2 CA II"
Nov  7 12:42:25 12[IKE] sending cert request for "C=TR, O=Elektronik Bilgi Guvenligi A.S., CN=e-Gu
ven Kok Elektronik Sertifika Hizmet Saglayicisi"
Nov  7 12:42:25 12[IKE] sending cert request for "C=GB, O=Trustis Limited, OU=Trustis FPS Root CA"

Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=AffirmTrust, CN=AffirmTrust Networking"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=SecureTrust Corporation, CN=Secure Globa
l CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Di
giCert Global Root CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=GB, ST=Greater Manchester, L=Salford, O=Comodo
 CA Limited, CN=AAA Certificate Services"
Nov  7 12:42:25 12[IKE] sending cert request for "C=GB, ST=Greater Manchester, L=Salford, O=Comodo
 CA Limited, CN=Trusted Certificate Services"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=AffirmTrust, CN=AffirmTrust Premium"
Nov  7 12:42:25 12[IKE] sending cert request for "C=NL, O=Staat der Nederlanden, CN=Staat der Nede
rlanden Root CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=HU, L=Budapest, O=Microsec Ltd., CN=Microsec e
-Szigno Root CA 2009, E=info@e-szigno.hu"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=America Online Inc., CN=America Online R
oot Certification Authority 2"
Nov  7 12:42:25 12[IKE] sending cert request for "C=IL, O=StartCom Ltd., OU=Secure Digital Certifi
cate Signing, CN=StartCom Certification Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=Network Solutions L.L.C., CN=Network Sol
utions Certificate Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "C=NO, O=Buypass AS-983163327, CN=Buypass Class 3
 Root CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=TW, O=Government Root Certification Authority"

Nov  7 12:42:25 12[IKE] sending cert request for "O=Digital Signature Trust Co., CN=DST Root CA X3
"
Nov  7 12:42:25 12[IKE] sending cert request for "C=HU, L=Budapest, O=NetLock Halozatbiztonsagi Kf
t., OU=Tanusitvanykiadok, CN=NetLock Expressz (Class C) Tanusitvanykiado"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, OU=www.xrampsecurity.com, O=XRamp Security
 Services Inc, CN=XRamp Global Certification Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "C=HU, L=Budapest, O=NetLock Kft., OU=TanÃ°sÃ-
tvÃ¡nykiadÃ³k (Certification Services), CN=NetLock Arany (Class Gold) FÅ?tanÃ°sÃtvÃ¡ny"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, ST=Arizona, L=Scottsdale, O=Starfield Tech
```

```
nologies, Inc., CN=Starfield Root Certificate Authority - G2"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=thawte, Inc., OU=Certification Services
Division, OU=(c) 2008 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA - G3"
Nov  7 12:42:25 12[IKE] sending cert request for "C=HK, O=Hongkong Post, CN=Hongkong Post Root CA
1"
Nov  7 12:42:25 12[IKE] sending cert request for "CN=TÃ?RKTRUST Elektronik Sertifika Hizmet SaÄ?la
yÄ±cÄ±sÄ±, C=TR, L=Ankara, O=TÃ?RKTRUST Bilgi Ä°letiÅ?im ve BiliÅ?im GÃ¼venliÄ?i Hizmetleri A.Å?.
(c) AralÄ±k 2007"
Nov  7 12:42:25 12[IKE] sending cert request for "C=EU, L=Madrid (see current address at www.camer
firma.com/address), SN=A82743287, O=AC Camerfirma S.A., CN=Global Chambersign Root - 2008"
Nov  7 12:42:25 12[IKE] sending cert request for "C=ES, O=FNMT, OU=FNMT Clase 2 CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=ES, O=IZENPE S.A., CN=Izenpe.com"
Nov  7 12:42:25 12[IKE] sending cert request for "OU=GlobalSign Root CA - R3, O=GlobalSign, CN=Glo
balSign"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=Equifax, OU=Equifax Secure Certificate A
uthority"
Nov  7 12:42:25 12[IKE] sending cert request for "C=ES, O=Agencia Catalana de Certificacio (NIF Q-
0801176-I), OU=Serveis Publics de Certificacio, OU=Vegeu https://www.catcert.net/verarrel (c)03, O
U=Jerarquia Entitats de Certificacio Catalanes, CN=EC-ACC"
Nov  7 12:42:25 12[IKE] sending cert request for "C=SK, L=Bratislava, O=Disig a.s., CN=CA Disig Ro
ot R1"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, I
nc., CN=Go Daddy Root Certificate Authority - G2"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=thawte, Inc., OU=Certification Services
Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Di
giCert Assured ID Root CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=CH, O=SwissSign AG, CN=SwissSign Gold CA - G2"

Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=thawte, Inc., OU=(c) 2007 thawte, Inc. -
 For authorized use only, CN=thawte Primary Root CA - G2"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=Entrust, Inc., OU=www.entrust.net/CPS is
 incorporated by reference, OU=(c) 2006 Entrust, Inc., CN=Entrust Root Certification Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "CN=ACEDICOM Root, OU=PKI, O=EDICOM, C=ES"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=GeoTrust Inc., CN=GeoTrust Global CA 2"
Nov  7 12:42:25 12[IKE] sending cert request for "CN=EBG Elektronik Sertifika Hizmet SaÄ?layÄ±cÄ±s
Ä±, O=EBG BiliÅ?im Teknolojileri ve Hizmetleri A.Å?., C=TR"
Nov  7 12:42:25 12[IKE] sending cert request for "C=CH, O=WISeKey, OU=Copyright (c) 2005, OU=OISTE
 Foundation Endorsed, CN=OISTE WISeKey Global Root GA CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=BM, O=QuoVadis Limited, OU=Root Certification
Authority, CN=QuoVadis Root Certification Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "C=AT, O=A-Trust Ges. f. Sicherheitssysteme im el
ektr. Datenverkehr GmbH, OU=A-Trust-nQual-03, CN=A-Trust-nQual-03"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=Equifax Secure Inc., CN=Equifax Secure G
lobal eBusiness CA-1"
Nov  7 12:42:25 12[IKE] sending cert request for "C=TW, O=TAIWAN-CA, OU=Root CA, CN=TWCA Root Cert
ification Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=Wells Fargo, OU=Wells Fargo Certificatio
n Authority, CN=Wells Fargo Root Certificate Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "C=JP, O=SECOM Trust Systems CO.,LTD., OU=Securit
y Communication EV RootCA1"
Nov  7 12:42:25 12[IKE] sending cert request for "C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter C
lass 3 CA, CN=TC TrustCenter Class 3 CA II"
Nov  7 12:42:25 12[IKE] sending cert request for "C=HU, L=Budapest, O=Microsec Ltd., OU=e-Szigno C
A, CN=Microsec e-Szigno Root CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=EU, O=AC Camerfirma SA CIF A82743287, OU=http:
//www.chambersign.org, CN=Global Chambersign Root"
Nov  7 12:42:25 12[IKE] sending cert request for "C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root
 Certification Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Con
sulting cc, OU=Certification Services Division, CN=Thawte Server CA, E=server-certs@thawte.com"
Nov  7 12:42:25 12[IKE] sending cert request for "C=GR, O=Hellenic Academic and Research Instituti
ons Cert. Authority, CN=Hellenic Academic and Research Institutions RootCA 2011"
Nov  7 12:42:25 12[IKE] sending cert request for "C=JP, O=SECOM Trust Systems CO.,LTD., OU=Securit
y Communication RootCA2"
Nov  7 12:42:25 12[IKE] sending cert request for "C=IT, L=Milan, O=Actalis S.p.A./03358520967, CN=
Actalis Authentication Root CA"
```

```
Nov  7 12:42:25 12[IKE] sending cert request for "O=Entrust.net, OU=www.entrust.net/CPS_2048 incor
p. by ref. (limits liab.), OU=(c) 1999 Entrust.net Limited, CN=Entrust.net Certification Authority
 (2048)"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=The Go Daddy Group, Inc., OU=Go Daddy Cl
ass 2 Certification Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "C=KR, O=KISA, OU=Korea Certification Authority C
entral, CN=KISA RootCA 1"
Nov  7 12:42:25 12[IKE] sending cert request for "C=FR, O=Certplus, CN=Class 2 Primary CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=AffirmTrust, CN=AffirmTrust Premium ECC"

Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=Wells Fargo WellsSecure, OU=Wells Fargo
Bank NA, CN=WellsSecure Public Root Certificate Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=Starfield Technologies, Inc., OU=Starfie
ld Class 2 Certification Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "C=EU, O=AC Camerfirma SA CIF A82743287, OU=http:
//www.chambersign.org, CN=Chambers of Commerce Root"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=AffirmTrust, CN=AffirmTrust Commercial"
Nov  7 12:42:25 12[IKE] sending cert request for "C=CN, O=CNNIC, CN=CNNIC ROOT"
Nov  7 12:42:25 12[IKE] sending cert request for "C=FI, O=Sonera, CN=Sonera Class2 CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=BM, O=QuoVadis Limited, CN=QuoVadis Root CA 3"

Nov  7 12:42:25 12[IKE] sending cert request for "C=CN, O=China Internet Network Information Cente
r, CN=China Internet Network Information Center EV Certificates Root"
Nov  7 12:42:25 12[IKE] sending cert request for "C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter U
niversal CA, CN=TC TrustCenter Universal CA I"
Nov  7 12:42:25 12[IKE] sending cert request for "C=HU, ST=Hungary, L=Budapest, O=NetLock Halozatb
iztonsagi Kft., OU=Tanusitvanykiadok, CN=NetLock Kozjegyzoi (Class A) Tanusitvanykiado"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=America Online Inc., CN=America Online R
oot Certification Authority 1"
Nov  7 12:42:25 12[IKE] sending cert request for "C=JP, O=Japan Certification Services, Inc., CN=S
ecureSign RootCA11"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=VeriSign, Inc., OU=VeriSign Trust Networ
k, OU=(c) 2008 VeriSign, Inc. - For authorized use only, CN=VeriSign Universal Root Certification
Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "C=DE, O=Deutsche Telekom AG, OU=T-TeleSec Trust
Center, CN=Deutsche Telekom Root CA 2"
Nov  7 12:42:25 12[IKE] sending cert request for "C=SK, L=Bratislava, O=Disig a.s., CN=CA Disig"
Nov  7 12:42:25 12[IKE] sending cert request for "E=pki@sk.ee, C=EE, O=AS Sertifitseerimiskeskus,
CN=Juur-SK"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, ST=UT, L=Salt Lake City, O=The USERTRUST N
etwork, OU=http://www.usertrust.com, CN=UTN - DATACorp SGC"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=VeriSign, Inc., OU=VeriSign Trust Networ
k, OU=(c) 2007 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certif
ication Authority - G4"
Nov  7 12:42:25 12[IKE] sending cert request for "C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN
=AddTrust Public CA Root"
Nov  7 12:42:25 12[IKE] sending cert request for "C=JP, O=Japanese Government, OU=ApplicationCA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=FR, ST=France, L=Paris, O=PM/SGDN, OU=DCSSI, C
N=IGC/A, E=igca@sgdn.pm.gouv.fr"
Nov  7 12:42:25 12[IKE] sending cert request for "C=ch, O=Swisscom, OU=Digital Certificate Service
s, CN=Swisscom Root CA 1"
Nov  7 12:42:25 12[IKE] sending cert request for "C=NO, O=Buypass AS-983163327, CN=Buypass Class 2
 CA 1"
Nov  7 12:42:25 12[IKE] sending cert request for "O=TeliaSonera, CN=TeliaSonera Root CA v1"
Nov  7 12:42:25 12[IKE] sending cert request for "C=CO, O=Sociedad Cameral de CertificaciÃ³n Digit
al - CerticÃ¡mara S.A., CN=AC RaÃz CerticÃ¡mara S.A."
Nov  7 12:42:25 12[IKE] sending cert request for "C=TW, O=TAIWAN-CA, OU=Root CA, CN=TWCA Global Ro
ot CA"
Nov  7 12:42:25 12[IKE] sending cert request for "O=Cybertrust, Inc, CN=Cybertrust Global Root"
Nov  7 12:42:25 12[IKE] sending cert request for "C=ES, O=Generalitat Valenciana, OU=PKIGVA, CN=Ro
ot CA Generalitat Valenciana"
Nov  7 12:42:25 12[IKE] sending cert request for "C=NL, O=Staat der Nederlanden, CN=Staat der Nede
rlanden Root CA - G2"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=Entrust.net, OU=www.entrust.net/CPS inco
rp. by ref. (limits liab.), OU=(c) 1999 Entrust.net Limited, CN=Entrust.net Secure Server Certific
ation Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "C=SE, O=AddTrust AB, OU=AddTrust External TTP Ne
```

```
twork, CN=AddTrust External CA Root"
Nov  7 12:42:25 12[IKE] sending cert request for "C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN
=AddTrust Qualified CA Root"
Nov  7 12:42:25 12[IKE] sending cert request for "CN=ComSign Secured CA, O=ComSign, C=IL"
Nov  7 12:42:25 12[IKE] sending cert request for "C=GB, ST=Greater Manchester, L=Salford, O=COMODO
 CA Limited, CN=COMODO Certification Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "C=US, O=GeoTrust Inc., CN=GeoTrust Universal CA
2"
Nov  7 12:42:25 12[IKE] sending cert request for "C=JP, O=SECOM Trust.net, OU=Security Communicati
on RootCA1"
Nov  7 12:42:25 12[IKE] sending cert request for "C=DE, O=D-Trust GmbH, CN=D-TRUST Root Class 3 CA
 2 EV 2009"
Nov  7 12:42:25 12[IKE] sending cert request for "C=GB, ST=Greater Manchester, L=Salford, O=COMODO
 CA Limited, CN=COMODO ECC Certification Authority"
Nov  7 12:42:25 12[IKE] sending cert request for "C=TR, L=Gebze - Kocaeli, O=TÃ¼rkiye Bilimsel ve
Teknolojik AraÅ?tÄ±rma Kurumu - TÃ?BÄ°TAK, OU=Ulusal Elektronik ve Kriptoloji AraÅ?tÄ±rma EnstitÃ¼
sÃ¼ - UEKAE, OU=Kamu Sertifikasyon Merkezi, CN=TÃ?BÄ°TAK UEKAE KÃ¶k Sertifika Hizmet SaÄ?layÄ±cÄ±s
Ä± - SÃ¼rÃ¼m 3"
Nov  7 12:42:25 12[IKE] sending cert request for "C=ES, CN=Autoridad de Certificacion Firmaprofesi
onal CIF A62634068"
Nov  7 12:42:25 12[IKE] sending cert request for "C=NO, O=Buypass AS-983163327, CN=Buypass Class 2
 Root CA"
Nov  7 12:42:25 12[IKE] sending cert request for "C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore C
yberTrust Root"
Nov  7 12:42:25 12[IKE] sending cert request for "C=FR, O=Certinomis, OU=0002 433998903, CN=Certin
omis - AutoritÃ© Racine"
Nov  7 12:42:25 12[IKE] sending cert request for "C=EE, O=AS Sertifitseerimiskeskus, CN=EE Certifi
cation Centre Root CA, E=pki@sk.ee"
Nov  7 12:42:25 12[IKE] sending cert request for "C=IN, O=motive, CN=UDM Root CA"
Nov  7 12:42:25 12[IKE] establishing CHILD_SA android
Nov  7 12:42:25 12[ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) CERTREQ CPRQ(ADDR ADDR
6 DNS DNS6) N(ESP_TFC_PAD_N) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_ONLY) ]
Nov  7 12:42:25 12[NET] sending packet: from 192.168.0.190[47525] to 135.250.90.29[4500] (3532 byt
es)
Nov  7 12:42:26 13[NET] received packet: from 135.250.90.29[4500] to 192.168.0.190[47525] (124 byt
es)
Nov  7 12:42:26 13[ENC] parsed IKE_AUTH response 1 [ IDr EAP/REQ/TLS ]
Nov  7 12:42:26 13[IKE] server requested EAP_TLS authentication (id 0x0B)
Nov  7 12:42:26 13[IKE] allow mutual EAP-only authentication
Nov  7 12:42:26 13[ENC] generating IKE_AUTH request 2 [ EAP/RES/TLS ]
Nov  7 12:42:26 13[NET] sending packet: from 192.168.0.190[47525] to 135.250.90.29[4500] (252 byte
s)
Nov  7 12:42:26 14[NET] received packet: from 135.250.90.29[4500] to 192.168.0.190[47525] (1100 by
tes)
Nov  7 12:42:26 14[ENC] parsed IKE_AUTH response 2 [ EAP/REQ/TLS ]
Nov  7 12:42:26 14[ENC] generating IKE_AUTH request 3 [ EAP/RES/TLS ]
Nov  7 12:42:26 14[NET] sending packet: from 192.168.0.190[47525] to 135.250.90.29[4500] (76 bytes
)
Nov  7 12:42:26 15[NET] received packet: from 135.250.90.29[4500] to 192.168.0.190[47525] (876 byt
es)
Nov  7 12:42:26 15[ENC] parsed IKE_AUTH response 3 [ EAP/REQ/TLS ]
Nov  7 12:42:26 15[TLS] negotiated TLS 1.2 using suite TLS_DHE_RSA_WITH_AES_128_CBC_SHA
Nov  7 12:42:26 15[TLS] received TLS server certificate 'C=IN, O=motive, CN=camellia.idc.devlab.mo
tive.com'
Nov  7 12:42:26 15[CFG]   using certificate "C=IN, O=motive, CN=camellia.idc.devlab.motive.com"
Nov  7 12:42:26 15[CFG]   using trusted ca certificate "C=IN, O=motive, CN=UDM Root CA"
Nov  7 12:42:26 15[CFG]   reached self-signed root ca with a path length of 0
Nov  7 12:42:26 15[TLS] received TLS cert request for 'C=IN, O=motive, CN=UDM Root CA
Nov  7 12:42:26 15[TLS] sending TLS peer certificate 'C=IN, O=motive, CN=client'
Nov  7 12:42:26 15[ENC] generating IKE_AUTH request 4 [ EAP/RES/TLS ]
Nov  7 12:42:26 15[NET] sending packet: from 192.168.0.190[47525] to 135.250.90.29[4500] (1100 byt
es)
Nov  7 12:42:26 09[NET] received packet: from 135.250.90.29[4500] to 192.168.0.190[47525] (76 byte
s)
Nov  7 12:42:26 09[ENC] parsed IKE_AUTH response 4 [ EAP/REQ/TLS ]
Nov  7 12:42:26 09[ENC] generating IKE_AUTH request 5 [ EAP/RES/TLS ]
Nov  7 12:42:26 09[NET] sending packet: from 192.168.0.190[47525] to 135.250.90.29[4500] (460 byte
```

```
s)
Nov  7 12:42:26 08[NET] received packet: from 135.250.90.29[4500] to 192.168.0.190[47525] (156 byt
es)
Nov  7 12:42:26 08[ENC] parsed IKE_AUTH response 5 [ EAP/REQ/TLS ]
Nov  7 12:42:26 08[ENC] generating IKE_AUTH request 6 [ EAP/RES/TLS ]
Nov  7 12:42:26 08[NET] sending packet: from 192.168.0.190[47525] to 135.250.90.29[4500] (76 bytes
)
Nov  7 12:42:26 11[NET] received packet: from 135.250.90.29[4500] to 192.168.0.190[47525] (76 byte
s)
Nov  7 12:42:26 11[ENC] parsed IKE_AUTH response 6 [ EAP/SUCC ]
Nov  7 12:42:26 11[IKE] EAP method EAP_TLS succeeded, MSK established
Nov  7 12:42:26 11[IKE] authentication of 'C=IN, O=motive, CN=client' (myself) with EAP
Nov  7 12:42:26 11[ENC] generating IKE_AUTH request 7 [ AUTH ]
Nov  7 12:42:26 11[NET] sending packet: from 192.168.0.190[47525] to 135.250.90.29[4500] (92 bytes
)
Nov  7 12:42:26 12[NET] received packet: from 135.250.90.29[4500] to 192.168.0.190[47525] (76 byte
s)
Nov  7 12:42:26 12[ENC] parsed IKE_AUTH response 7 [ N(AUTH_FAILED) ]
Nov  7 12:42:26 12[IKE] received AUTHENTICATION_FAILED notify error
```

Associated revisions

Revision ec575274 - 03.03.2015 14:08 - Martin Willi

Merge branch 'eap-constraints'

Introduces basic support for EAP server module authentication constraints. With
EAP-(T)TLS, public key, signature and end entity or CA certificate constraints
can be enforced for connections.

Fixes #762.

History

#1 - 10.11.2014 10:22 - Martin Willi

- Status changed from New to Feedback

- Priority changed from Urgent to Normal

rightcert=clientCert.pem
rightauth=eap-tls

10[CFG] constraint check failed: peer not authenticated with peer cert 'C=IN, O=motive, CN=client'.

Evaluating constraints for EAP authentication is currently not supported, i.e. you can't apply restricted authentication rules to EAP authentication methods.

rightcert, however, does not only load the certificate, but also defines a constraint that the peer MUST use that specific certificate. This currently won't work for EAP-TLS.

If you have a CA certificate, you may place that into the cacerts directory the establish trust in all issued certificates (but you may not set rightca, as this again creates a constraint). If you have a self-signed certificate, you may as a work-around set rightcert2 to your certificate instead. If I remember correctly this should load your certificate, but doesn't set a constraint (as there is no second authentication round defined).

#2 - 10.11.2014 13:07 - Tobias Brunner

- Category set to android

- Assignee set to Tobias Brunner

In addition to what Martin said, the Android client does currently not support EAP-only authentication (see Changelog). Therefore, you'll have to configure *leftauth=pubkey* on the server intead of *leftauth=eap-tls*.

#3 - 03.03.2015 14:38 - Martin Willi

- Tracker changed from Issue to Feature

- Category changed from android to libcharon

- Status changed from Feedback to Closed

- Assignee changed from Tobias Brunner to Martin Willi

- Target version set to 5.3.0

- Resolution set to Fixed

The referenced commit introduces support for certificate constraints in EAP methods. This should fix the *peer not authenticated with...* issue.

I'm closing the issue for now, feel free to open a different ticket for any not directly related issues.

Regards
Martin