strongSwan - Issue #1373

DH group 17 and 18 does not work (IKE, PFS)

30.03.2016 08:58 - Jiri Zendulka

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.4.0	**Resolution:**	No change required

Description

Hello,

I built strongswan for armv5 platform with following options:

```
./configure --prefix=/usr \
            --sysconfdir=/etc \
            --host=$CFGHOST \
            --enable-monolithic \
            --enable-openssl \
            --disable-gmp \
            --disable-scepclient \
            --disable-dnskey \
            --disable-sshkey \
            --disable-pgp \
            --disable-revocation \
            --disable-constraints \
            --disable-fips-prf \
            --disable-cmac \
            --disable-pkcs1 \
            --disable-pkcs7 \
            --disable-pkcs8 \
            --disable-pkcs12 \
            --disable-xauth-generic \
            --disable-pubkey \
            --disable-random \
            --disable-hmac \
            --disable-xcbc \
            --disable-x509 \
            --disable-resolve \
            --disable-attr \
            --disable-aes \
            --disable-des \
            --disable-sha1 \
            --disable-sha2 \
            --disable-rc2 \
            --disable-md5
```

Now I am struggling with DH group 17 and 18 which does not work for IKE even for PFS. I tested it on strongswan 5.4.0 and 5.3.5 and outcome is the same. DH group lower than 17 works.

ipsec status:

```
Status of IKE charon daemon (strongSwan 5.3.5, Linux 3.5.0-lsp-3.3.1, armv5tejl):
  uptime: 8 minutes, since Mar 30 06:50:57 2016
  malloc: sbrk 495616, mmap 0, used 170816, free 324800
  worker threads: 9 of 16 idle, 5/0/1/1 working, job queue: 0/0/0/0, scheduled: 0
  loaded plugins: charon nonce pem openssl kernel-netlink socket-default stroke updown
Listening IP addresses:
  192.168.7.110
Connections:
      ipsec1:  192.168.7.110...%any  IKEv1
```

```
      ipsec1:   local:  uses pre-shared key authentication
      ipsec1:   remote: uses pre-shared key authentication
      ipsec1:   child:  192.168.30.0/24 === 192.168.2.0/24 TUNNEL
Security Associations (0 up, 1 connecting):
  none
```

ipsec.conf:

```
config setup
      charondebug=dmn 2, mgr 2, ike 2, chd 2, job 2, cfg 2, knl 2, net 2, asn 2, enc 2, lib 2, esp
 2, tls 2, tnc 2, imc 2, imv 2, pts 2

conn ipsec1
      leftid=""
      rightid=""
      leftauth=psk
      rightauth=psk
      ikelifetime=3600
      keylife=3600
      rekeymargin=540
      rekeyfuzz=100%
      type=tunnel
      ike=aes128-sha1-modp6144
      esp=aes128-sha1
      keyexchange=ikev1
      right=%any
      left=192.168.7.110
      leftsubnet=192.168.30.0/24
      rightsubnet=192.168.2.0/24
      auto=add
      leftfirewall=yes
```

syslog:

```
...
2016-03-30 06:46:14 charon: 11[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/
MODP_6144
2016-03-30 06:46:14 charon: 11[IKE] sending DPD vendor ID
2016-03-30 06:46:14 charon: 11[ENC] added payload of type VENDOR_ID_V1 to message
2016-03-30 06:46:14 charon: 11[ENC] added payload of type SECURITY_ASSOCIATION_V1 to message
2016-03-30 06:46:14 charon: 11[ENC] order payloads in message
2016-03-30 06:46:14 charon: 11[ENC] added payload of type SECURITY_ASSOCIATION_V1 to message
2016-03-30 06:46:14 charon: 11[ENC] added payload of type VENDOR_ID_V1 to message
2016-03-30 06:46:14 charon: 11[ENC] generating ID_PROT response 0 [ SA V ]
2016-03-30 06:46:14 charon: 11[ENC] not encrypting payloads
2016-03-30 06:46:14 charon: 11[ENC] generating payload of type HEADER
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 0 IKE_SPI
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 1 IKE_SPI
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 2 U_INT_8
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 3 U_INT_4
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 4 U_INT_4
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 5 U_INT_8
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 6 RESERVED_BIT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 7 RESERVED_BIT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 8 FLAG
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 9 FLAG
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 10 FLAG
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 11 FLAG
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 12 FLAG
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 13 FLAG
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 14 U_INT_32
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 15 HEADER_LENGTH
2016-03-30 06:46:14 charon: 11[ENC] generating HEADER payload finished
2016-03-30 06:46:14 charon: 11[ENC] generating payload of type SECURITY_ASSOCIATION_V1
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 0 U_INT_8
```

```
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 1 RESERVED_BIT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 2 RESERVED_BIT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 3 RESERVED_BIT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 4 RESERVED_BIT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 5 RESERVED_BIT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 6 RESERVED_BIT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 7 RESERVED_BIT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 8 RESERVED_BIT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 9 PAYLOAD_LENGTH
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 10 U_INT_32
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 11 U_INT_32
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 12 (1259)
2016-03-30 06:46:14 charon: 11[ENC] generating payload of type PROPOSAL_SUBSTRUCTURE_V1
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 0 U_INT_8
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 1 RESERVED_BYTE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 2 PAYLOAD_LENGTH
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 3 U_INT_8
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 4 U_INT_8
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 5 SPI_SIZE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 6 U_INT_8
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 7 SPI
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 8 (1261)
2016-03-30 06:46:14 charon: 11[ENC] generating payload of type TRANSFORM_SUBSTRUCTURE_V1
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 0 U_INT_8
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 1 RESERVED_BYTE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 2 PAYLOAD_LENGTH
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 3 U_INT_8
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 4 U_INT_8
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 5 RESERVED_BYTE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 6 RESERVED_BYTE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 7 (1263)
2016-03-30 06:46:14 charon: 11[ENC] generating payload of type TRANSFORM_ATTRIBUTE_V1
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 0 ATTRIBUTE_FORMAT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 1 ATTRIBUTE_TYPE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 2 ATTRIBUTE_LENGTH_OR_VALUE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 3 ATTRIBUTE_VALUE
2016-03-30 06:46:14 charon: 11[ENC] generating TRANSFORM_ATTRIBUTE_V1 payload finished
2016-03-30 06:46:14 charon: 11[ENC] generating payload of type TRANSFORM_ATTRIBUTE_V1
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 0 ATTRIBUTE_FORMAT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 1 ATTRIBUTE_TYPE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 2 ATTRIBUTE_LENGTH_OR_VALUE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 3 ATTRIBUTE_VALUE
2016-03-30 06:46:14 charon: 11[ENC] generating TRANSFORM_ATTRIBUTE_V1 payload finished
2016-03-30 06:46:14 charon: 11[ENC] generating payload of type TRANSFORM_ATTRIBUTE_V1
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 0 ATTRIBUTE_FORMAT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 1 ATTRIBUTE_TYPE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 2 ATTRIBUTE_LENGTH_OR_VALUE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 3 ATTRIBUTE_VALUE
2016-03-30 06:46:14 charon: 11[ENC] generating TRANSFORM_ATTRIBUTE_V1 payload finished
2016-03-30 06:46:14 charon: 11[ENC] generating payload of type TRANSFORM_ATTRIBUTE_V1
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 0 ATTRIBUTE_FORMAT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 1 ATTRIBUTE_TYPE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 2 ATTRIBUTE_LENGTH_OR_VALUE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 3 ATTRIBUTE_VALUE
2016-03-30 06:46:14 charon: 11[ENC] generating TRANSFORM_ATTRIBUTE_V1 payload finished
2016-03-30 06:46:14 charon: 11[ENC] generating payload of type TRANSFORM_ATTRIBUTE_V1
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 0 ATTRIBUTE_FORMAT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 1 ATTRIBUTE_TYPE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 2 ATTRIBUTE_LENGTH_OR_VALUE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 3 ATTRIBUTE_VALUE
2016-03-30 06:46:14 charon: 11[ENC] generating TRANSFORM_ATTRIBUTE_V1 payload finished
2016-03-30 06:46:14 charon: 11[ENC] generating payload of type TRANSFORM_ATTRIBUTE_V1
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 0 ATTRIBUTE_FORMAT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 1 ATTRIBUTE_TYPE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 2 ATTRIBUTE_LENGTH_OR_VALUE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 3 ATTRIBUTE_VALUE
2016-03-30 06:46:14 charon: 11[ENC] generating TRANSFORM_ATTRIBUTE_V1 payload finished
```

```
2016-03-30 06:46:14 charon: 11[ENC] generating payload of type TRANSFORM_ATTRIBUTE_V1
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 0 ATTRIBUTE_FORMAT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 1 ATTRIBUTE_TYPE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 2 ATTRIBUTE_LENGTH_OR_VALUE
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 3 ATTRIBUTE_VALUE
2016-03-30 06:46:14 charon: 11[ENC] generating TRANSFORM_ATTRIBUTE_V1 payload finished
2016-03-30 06:46:14 charon: 11[ENC] generating TRANSFORM_SUBSTRUCTURE_V1 payload finished
2016-03-30 06:46:14 charon: 11[ENC] generating PROPOSAL_SUBSTRUCTURE_V1 payload finished
2016-03-30 06:46:14 charon: 11[ENC] generating SECURITY_ASSOCIATION_V1 payload finished
2016-03-30 06:46:14 charon: 11[ENC] generating payload of type VENDOR_ID_V1
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 0 U_INT_8
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 1 FLAG
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 2 RESERVED_BIT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 3 RESERVED_BIT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 4 RESERVED_BIT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 5 RESERVED_BIT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 6 RESERVED_BIT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 7 RESERVED_BIT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 8 RESERVED_BIT
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 9 PAYLOAD_LENGTH
2016-03-30 06:46:14 charon: 11[ENC]   generating rule 10 CHUNK_DATA
2016-03-30 06:46:14 charon: 11[ENC] generating VENDOR_ID_V1 payload finished
2016-03-30 06:46:14 charon: 11[NET] sending packet: from 192.168.7.110[500] to 192.168.7.100[500]
(104 bytes)
2016-03-30 06:46:14 charon: 07[NET] sending packet: from 192.168.7.110[500] to 192.168.7.100[500]
2016-03-30 06:46:14 charon: 11[MGR] checkin IKE_SA (unnamed)[3]
2016-03-30 06:46:14 charon: 11[MGR] check-in of IKE_SA successful.
2016-03-30 06:46:14 charon: 06[NET] received packet: from 192.168.7.100[500] to 192.168.7.110[500]

2016-03-30 06:46:14 charon: 06[ENC] parsing header of message
2016-03-30 06:46:14 charon: 06[ENC] parsing HEADER payload, 820 bytes left
2016-03-30 06:46:14 charon: 06[ENC]   parsing rule 0 IKE_SPI
2016-03-30 06:46:14 charon: 06[ENC]   parsing rule 1 IKE_SPI
2016-03-30 06:46:14 charon: 06[ENC]   parsing rule 2 U_INT_8
2016-03-30 06:46:14 charon: 06[ENC]   parsing rule 3 U_INT_4
2016-03-30 06:46:14 charon: 06[ENC]   parsing rule 4 U_INT_4
2016-03-30 06:46:14 charon: 06[ENC]   parsing rule 5 U_INT_8
2016-03-30 06:46:14 charon: 06[ENC]   parsing rule 6 RESERVED_BIT
2016-03-30 06:46:14 charon: 06[ENC]   parsing rule 7 RESERVED_BIT
2016-03-30 06:46:14 charon: 06[ENC]   parsing rule 8 FLAG
2016-03-30 06:46:14 charon: 06[ENC]   parsing rule 9 FLAG
2016-03-30 06:46:14 charon: 06[ENC]   parsing rule 10 FLAG
2016-03-30 06:46:14 charon: 06[ENC]   parsing rule 11 FLAG
2016-03-30 06:46:14 charon: 06[ENC]   parsing rule 12 FLAG
2016-03-30 06:46:14 charon: 06[ENC]   parsing rule 13 FLAG
2016-03-30 06:46:14 charon: 06[ENC]   parsing rule 14 U_INT_32
2016-03-30 06:46:14 charon: 06[ENC]   parsing rule 15 HEADER_LENGTH
2016-03-30 06:46:14 charon: 06[ENC] parsing HEADER payload finished
2016-03-30 06:46:14 charon: 06[ENC] parsed a ID_PROT message header
2016-03-30 06:46:14 charon: 10[MGR] checkout IKE_SA by message
2016-03-30 06:46:14 charon: 10[MGR] IKE_SA (unnamed)[3] successfully checked out
2016-03-30 06:46:14 charon: 10[NET] received packet: from 192.168.7.100[500] to 192.168.7.110[500]
 (820 bytes)
2016-03-30 06:46:14 charon: 10[ENC] parsing body of message, first payload is KEY_EXCHANGE_V1
2016-03-30 06:46:14 charon: 10[ENC] starting parsing a KEY_EXCHANGE_V1 payload
2016-03-30 06:46:14 charon: 10[ENC] parsing KEY_EXCHANGE_V1 payload, 792 bytes left
2016-03-30 06:46:14 charon: 10[ENC]   parsing rule 0 U_INT_8
2016-03-30 06:46:14 charon: 10[ENC]   parsing rule 1 RESERVED_BYTE
2016-03-30 06:46:14 charon: 10[ENC]   parsing rule 2 PAYLOAD_LENGTH
2016-03-30 06:46:14 charon: 10[ENC]   parsing rule 3 CHUNK_DATA
2016-03-30 06:46:14 charon: 10[ENC] parsing KEY_EXCHANGE_V1 payload finished
2016-03-30 06:46:14 charon: 10[ENC] verifying payload of type KEY_EXCHANGE_V1
2016-03-30 06:46:14 charon: 10[ENC] KEY_EXCHANGE_V1 payload verified, adding to payload list
2016-03-30 06:46:14 charon: 10[ENC] starting parsing a NONCE_V1 payload
2016-03-30 06:46:14 charon: 10[ENC] parsing NONCE_V1 payload, 20 bytes left
2016-03-30 06:46:14 charon: 10[ENC]   parsing rule 0 U_INT_8
2016-03-30 06:46:14 charon: 10[ENC]   parsing rule 1 FLAG
```

```
2016-03-30 06:46:14 charon: 10[ENC]   parsing rule 2 RESERVED_BIT
2016-03-30 06:46:14 charon: 10[ENC]   parsing rule 3 RESERVED_BIT
2016-03-30 06:46:14 charon: 10[ENC]   parsing rule 4 RESERVED_BIT
2016-03-30 06:46:14 charon: 10[ENC]   parsing rule 5 RESERVED_BIT
2016-03-30 06:46:14 charon: 10[ENC]   parsing rule 6 RESERVED_BIT
2016-03-30 06:46:14 charon: 10[ENC]   parsing rule 7 RESERVED_BIT
2016-03-30 06:46:14 charon: 06[NET] waiting for data on sockets
2016-03-30 06:46:14 charon: 10[ENC]   parsing rule 8 RESERVED_BIT
2016-03-30 06:46:14 charon: 10[ENC]   parsing rule 9 PAYLOAD_LENGTH
2016-03-30 06:46:14 charon: 10[ENC]   parsing rule 10 CHUNK_DATA
2016-03-30 06:46:14 charon: 10[ENC] parsing NONCE_V1 payload finished
2016-03-30 06:46:14 charon: 10[ENC] verifying payload of type NONCE_V1
2016-03-30 06:46:14 charon: 10[ENC] NONCE_V1 payload verified, adding to payload list
2016-03-30 06:46:14 charon: 10[ENC] process payload of type KEY_EXCHANGE_V1
2016-03-30 06:46:14 charon: 10[ENC] process payload of type NONCE_V1
2016-03-30 06:46:14 charon: 10[ENC] verifying message structure
2016-03-30 06:46:14 charon: 10[ENC] found payload of type KEY_EXCHANGE_V1
2016-03-30 06:46:14 charon: 10[ENC] found payload of type NONCE_V1
2016-03-30 06:46:14 charon: 10[ENC] parsed ID_PROT request 0 [ KE No ]
2016-03-30 06:46:24 charon: 06[NET] received packet: from 192.168.7.100[500] to 192.168.7.110[500]

2016-03-30 06:46:24 charon: 06[ENC] parsing header of message
2016-03-30 06:46:24 charon: 06[ENC] parsing HEADER payload, 820 bytes left
2016-03-30 06:46:24 charon: 06[ENC]   parsing rule 0 IKE_SPI
2016-03-30 06:46:24 charon: 06[ENC]   parsing rule 1 IKE_SPI
2016-03-30 06:46:24 charon: 06[ENC]   parsing rule 2 U_INT_8
2016-03-30 06:46:24 charon: 06[ENC]   parsing rule 3 U_INT_4
2016-03-30 06:46:24 charon: 06[ENC]   parsing rule 4 U_INT_4
2016-03-30 06:46:24 charon: 06[ENC]   parsing rule 5 U_INT_8
2016-03-30 06:46:24 charon: 06[ENC]   parsing rule 6 RESERVED_BIT
2016-03-30 06:46:24 charon: 06[ENC]   parsing rule 7 RESERVED_BIT
2016-03-30 06:46:24 charon: 06[ENC]   parsing rule 8 FLAG
2016-03-30 06:46:24 charon: 06[ENC]   parsing rule 9 FLAG
2016-03-30 06:46:24 charon: 06[ENC]   parsing rule 10 FLAG
2016-03-30 06:46:24 charon: 06[ENC]   parsing rule 11 FLAG
2016-03-30 06:46:24 charon: 06[ENC]   parsing rule 12 FLAG
2016-03-30 06:46:24 charon: 06[ENC]   parsing rule 13 FLAG
2016-03-30 06:46:24 charon: 06[ENC]   parsing rule 14 U_INT_32
2016-03-30 06:46:24 charon: 06[ENC]   parsing rule 15 HEADER_LENGTH
2016-03-30 06:46:24 charon: 06[ENC] parsing HEADER payload finished
2016-03-30 06:46:24 charon: 06[ENC] parsed a ID_PROT message header
2016-03-30 06:46:24 charon: 02[MGR] checkout IKE_SA by message
2016-03-30 06:46:24 charon: 02[MGR] ignoring request with ID 505224074, already processing
2016-03-30 06:46:24 charon: 06[NET] waiting for data on sockets
2016-03-30 06:46:31 charon: 10[LIB] size of DH secret exponent: 6143 bits
2016-03-30 06:46:44 charon: 04[JOB] got event, queuing job for execution
2016-03-30 06:46:44 charon: 04[JOB] no events, waiting
2016-03-30 06:46:44 charon: 12[MGR] checkout IKE_SA
...
```

Thanks.

History

#1 - 30.03.2016 10:09 - Jiri Zendulka

I built strongswan with gmp instead of openssl but without success. The issue persists...

#2 - 30.03.2016 11:07 - Tobias Brunner

- Description updated

- Category set to libstrongswan

- Status changed from New to Feedback

I don't see any indication in the log that it does not work. It might just take a long time (also see PublicKeySpeed).

#3 - 30.03.2016 11:23 - Jiri Zendulka

Yes, this would be a cause... Is it any way how to reduce the time of generating DH key?
When I used openswan on the same platform (hardware) I did not have this issue.

Many thanks.

#4 - 30.03.2016 11:44 - Jiri Zendulka

...I set option "dh_exponent_ansi_x9_42 = no" to charon/strongswan.conf file. Is it safe/correct solution?
Tunnel is estabilished immediately then...

#5 - 30.03.2016 12:14 - Tobias Brunner

> ...I set option "dh_exponent_ansi_x9_42 = no" to charon/strongswan.conf file. Is it safe/correct solution?

If it is set to *no* the exponent length is shortened (from equaling the length of the modulus) and roughly determined by the recommendations given in RFC 3766 (with some help of keylength.com). You should read that and decide for yourself whether you want to use that option. For the actual exponent lengths in bytes refer to opt_exp in source:src/libstrongswan/crypto/diffie_hellman.c.

#6 - 30.03.2016 13:34 - Jiri Zendulka

Thanks. You can close this issue.

#7 - 30.03.2016 14:04 - Tobias Brunner

- Category changed from libstrongswan to configuration

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No change required