strongSwan - Issue #2337

Kernel 3.5.0: AED/GCM ciphers are not working with strongswan

25.05.2017 14:22 - Jiri Zendulka

Status:	Closed		
Priority:	Normal		
Assignee:	Noel Kuntze		
Category:	kernel		
Affected version:		**Resolution:**	Invalid

Description

I enabled AED/GCM ciphers in kernel 3.5.0 but strongswan 5.4.0 reports following:

```
2017-05-25 09:42:56 charon: 10[CFG]   proposal matches
2017-05-25 09:42:56 charon: 10[CFG] received proposals: ESP:AES_GCM_16_128/NO_EXT_SEQ
2017-05-25 09:42:56 charon: 10[CFG] configured proposals: ESP:AES_GCM_16_128/MODP_2048/NO_EXT_SEQ
2017-05-25 09:42:56 charon: 10[CFG] selected proposal: ESP:AES_GCM_16_128/NO_EXT_SEQ
2017-05-25 09:42:56 charon: 10[CFG] selecting traffic selectors for us:
2017-05-25 09:42:56 charon: 10[CFG]  config: 10.70.0.144/29, received: 10.70.0.144/29 = match: 10.
70.0.144/29
2017-05-25 09:42:56 charon: 10[CFG] selecting traffic selectors for other:
2017-05-25 09:42:56 charon: 10[CFG]  config: 10.5.0.0/24, received: 10.5.0.0/24 = match: 10.5.0.0/
24
2017-05-25 09:42:56 charon: 10[CHD]   using AES_GCM_16 for encryption
2017-05-25 09:42:56 charon: 10[CHD] adding inbound ESP SA
2017-05-25 09:42:56 charon: 10[CHD]   SPI 0xce98f5f8, src 192.168.7.7 dst 192.168.7.130
2017-05-25 09:42:56 charon: 10[KNL] adding SAD entry with SPI ce98f5f8 and reqid {1}  (mark 0/0x00
000000)
2017-05-25 09:42:56 charon: 10[KNL]   using encryption algorithm AES_GCM_16 with key size 160
2017-05-25 09:42:56 charon: 10[KNL]   using replay window of 32 packets
2017-05-25 09:42:56 charon: 10[KNL] sending XFRM_MSG_UPDSA 202: = 336 bytes @ 0xb22dd618
2017-05-25 09:42:56 charon: 10[KNL]    0: 50 01 00 00 1A 00 05 00 CA 00 00 00 B4 12 00 00  P.....
.........
2017-05-25 09:42:56 charon: 10[KNL]   16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
.........
2017-05-25 09:42:56 charon: 10[KNL]   32: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
.........
2017-05-25 09:42:56 charon: 10[KNL]   48: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
.........
2017-05-25 09:42:56 charon: 10[KNL]   64: 00 00 00 00 00 00 00 00 C0 A8 07 82 00 00 00 00  .....
.........
2017-05-25 09:42:56 charon: 10[KNL]   80: 00 00 00 00 00 00 00 00 CE 98 F5 F8 32 00 00 00  .....
.....2...
2017-05-25 09:42:56 charon: 10[KNL]   96: C0 A8 07 07 00 00 00 00 00 00 00 00 00 00 00 00  .....
.........
2017-05-25 09:42:56 charon: 10[KNL]  112: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  .....
.........
2017-05-25 09:42:56 charon: 10[KNL]  128: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  .....
.........
2017-05-25 09:42:56 charon: 10[KNL]  144: 7F 0B 00 00 00 00 00 00 10 0E 00 00 00 00 00 00  .....
.........
2017-05-25 09:42:56 charon: 10[KNL]  160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
.........
2017-05-25 09:42:56 charon: 10[KNL]  176: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
.........
2017-05-25 09:42:56 charon: 10[KNL]  192: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
.........
2017-05-25 09:42:56 charon: 10[KNL]  208: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
.........
2017-05-25 09:42:56 charon: 10[KNL]  224: 01 00 00 00 02 00 01 20 20 00 00 00 00 00 00 00  .....
  .......
2017-05-25 09:42:56 charon: 10[KNL]  240: 60 00 12 00 72 66 63 34 31 30 36 28 67 63 6D 28  `...rfc
4106(gcm(
```

```
2017-05-25 09:42:56 charon: 10[KNL]  256: 61 65 73 29 29 00 00 00 00 00 00 00 00 00 00 00  aes))..
................
2017-05-25 09:42:56 charon: 10[KNL]  272: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
................
2017-05-25 09:42:56 charon: 10[KNL]  288: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
................
2017-05-25 09:42:56 charon: 10[KNL]  304: 00 00 00 00 A0 00 00 00 80 00 00 00 40 2F 7A B6  ........
.....@/z.
2017-05-25 09:42:56 charon: 10[KNL]  320: AD 10 E8 5E C4 1C C7 AC 0E D4 D7 39 CB 19 8D FA  ...^....
....9....
2017-05-25 09:42:56 charon: 10[KNL] received (2) 202: = 356 bytes @ 0xb11017e0
2017-05-25 09:42:56 charon: 10[KNL]    0: 64 01 00 00 02 00 00 00 CA 00 00 00 B4 12 00 00  d.......
................
2017-05-25 09:42:56 charon: 10[KNL]   16: DA FF FF FF 50 01 00 00 1A 00 05 00 CA 00 00 00  ....P...
................
2017-05-25 09:42:56 charon: 10[KNL]   32: B4 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
................
2017-05-25 09:42:56 charon: 10[KNL]   48: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
................
2017-05-25 09:42:56 charon: 10[KNL]   64: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
................
2017-05-25 09:42:56 charon: 10[KNL]   80: 00 00 00 00 00 00 00 00 00 00 00 00 C0 A8 07 82  ........
................
2017-05-25 09:42:56 charon: 10[KNL]   96: 00 00 00 00 00 00 00 00 00 00 00 00 CE 98 F5 F8  ........
................
2017-05-25 09:42:56 charon: 10[KNL]  112: 32 00 00 00 C0 A8 07 07 00 00 00 00 00 00 00 00  2.......
................
2017-05-25 09:42:56 charon: 10[KNL]  128: 00 00 00 00 FF FF FF FF FF FF FF FF FF FF FF FF  ........
................
2017-05-25 09:42:56 charon: 10[KNL]  144: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........
................
2017-05-25 09:42:56 charon: 10[KNL]  160: FF FF FF FF 7F 0B 00 00 00 00 00 00 10 0E 00 00  ........
................
2017-05-25 09:42:56 charon: 10[KNL]  176: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
................
2017-05-25 09:42:56 charon: 10[KNL]  192: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
................
2017-05-25 09:42:56 charon: 10[KNL]  208: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
................
2017-05-25 09:42:56 charon: 10[KNL]  224: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
................
2017-05-25 09:42:56 charon: 10[KNL]  240: 00 00 00 00 01 00 00 00 02 00 01 20 20 00 00 00  ........
....  ...
2017-05-25 09:42:56 charon: 10[KNL]  256: 00 00 00 00 60 00 12 00 72 66 63 34 31 30 36 28  ....`...
.rfc4106(
2017-05-25 09:42:56 charon: 10[KNL]  272: 67 63 6D 28 61 65 73 29 29 00 00 00 00 00 00 00  gcm(aes
)).......
2017-05-25 09:42:56 charon: 10[KNL]  288: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
................
2017-05-25 09:42:56 charon: 10[KNL]  304: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
................
2017-05-25 09:42:56 charon: 10[KNL]  320: 00 00 00 00 00 00 00 00 A0 00 00 00 80 00 00 00  ........
................
2017-05-25 09:42:56 charon: 10[KNL]  336: 40 2F 7A B6 AD 10 E8 5E C4 1C C7 AC 0E D4 D7 39  @/z....
^.......9
2017-05-25 09:42:56 charon: 10[KNL]  352: CB 19 8D FA                                      ....
2017-05-25 09:42:56 charon: 10[KNL] received netlink error: Function not implemented (38)
2017-05-25 09:42:56 charon: 10[KNL] unable to add SAD entry with SPI ce98f5f8
2017-05-25 09:42:56 charon: 10[CHD] adding outbound ESP SA
2017-05-25 09:42:56 charon: 10[CHD]   SPI 0xcd13aedb, src 192.168.7.130 dst 192.168.7.7
2017-05-25 09:42:56 charon: 10[KNL] adding SAD entry with SPI cd13aedb and reqid {1}  (mark 0/0x00
000000)
2017-05-25 09:42:56 charon: 10[KNL]   using encryption algorithm AES_GCM_16 with key size 160
2017-05-25 09:42:56 charon: 10[KNL]   using replay window of 32 packets
2017-05-25 09:42:56 charon: 10[KNL] sending XFRM_MSG_NEWSA 203: = 336 bytes @ 0xb22dd618
2017-05-25 09:42:56 charon: 10[KNL]    0: 50 01 00 00 10 00 05 00 CB 00 00 00 B4 12 00 00  P.......
................
```

```
2017-05-25 09:42:56 charon: 10[KNL]   16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
2017-05-25 09:42:56 charon: 10[KNL]   32: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
2017-05-25 09:42:56 charon: 10[KNL]   48: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
2017-05-25 09:42:56 charon: 10[KNL]   64: 00 00 00 00 00 00 00 00 C0 A8 07 07 00 00 00 00  ................
2017-05-25 09:42:56 charon: 10[KNL]   80: 00 00 00 00 00 00 00 00 CD 13 AE DB 32 00 00 00  ............2...
2017-05-25 09:42:56 charon: 10[KNL]   96: C0 A8 07 82 00 00 00 00 00 00 00 00 00 00 00 00  ................
2017-05-25 09:42:56 charon: 10[KNL]  112: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
2017-05-25 09:42:56 charon: 10[KNL]  128: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
2017-05-25 09:42:56 charon: 10[KNL]  144: ED 0A 00 00 00 00 00 00 10 0E 00 00 00 00 00 00  ................
2017-05-25 09:42:56 charon: 10[KNL]  160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
2017-05-25 09:42:56 charon: 10[KNL]  176: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
2017-05-25 09:42:56 charon: 10[KNL]  192: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
2017-05-25 09:42:56 charon: 10[KNL]  208: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
2017-05-25 09:42:56 charon: 10[KNL]  224: 01 00 00 00 02 00 01 20 20 00 00 00 00 00 00 00  ....... .......
2017-05-25 09:42:56 charon: 10[KNL]  240: 60 00 12 00 72 66 63 34 31 30 36 28 67 63 6D 28  `...rfc4106(gcm(
2017-05-25 09:42:56 charon: 10[KNL]  256: 61 65 73 29 29 00 00 00 00 00 00 00 00 00 00 00  aes))..........
2017-05-25 09:42:56 charon: 10[KNL]  272: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
2017-05-25 09:42:56 charon: 10[KNL]  288: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
2017-05-25 09:42:56 charon: 10[KNL]  304: 00 00 00 00 A0 00 00 00 80 00 00 00 6A AA 3E C6  ............j.>.
2017-05-25 09:42:56 charon: 10[KNL]  320: 55 D7 B4 80 0A C4 9A CE 50 3F DD BD 88 34 0F F2  U.......P?...4..
2017-05-25 09:42:56 charon: 10[KNL] received (2) 203: = 356 bytes @ 0xb11018e8
2017-05-25 09:42:56 charon: 10[KNL]    0: 64 01 00 00 02 00 00 00 CB 00 00 00 B4 12 00 00  d...............
2017-05-25 09:42:56 charon: 10[KNL]   16: DA FF FF FF 50 01 00 00 10 00 05 00 CB 00 00 00  ....P...........
2017-05-25 09:42:56 charon: 10[KNL]   32: B4 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
2017-05-25 09:42:56 charon: 10[KNL]   48: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
2017-05-25 09:42:56 charon: 10[KNL]   64: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
2017-05-25 09:42:56 charon: 10[KNL]   80: 00 00 00 00 00 00 00 00 00 00 00 00 C0 A8 07 07  ................
2017-05-25 09:42:56 charon: 10[KNL]   96: 00 00 00 00 00 00 00 00 00 00 00 00 CD 13 AE DB  ................
2017-05-25 09:42:56 charon: 10[KNL]  112: 32 00 00 00 C0 A8 07 82 00 00 00 00 00 00 00 00  2...............
2017-05-25 09:42:56 charon: 10[KNL]  128: 00 00 00 00 FF FF FF FF FF FF FF FF FF FF FF FF  ................
2017-05-25 09:42:56 charon: 10[KNL]  144: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................
2017-05-25 09:42:56 charon: 10[KNL]  160: FF FF FF FF ED 0A 00 00 00 00 00 00 10 0E 00 00  ................
2017-05-25 09:42:56 charon: 10[KNL]  176: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
2017-05-25 09:42:56 charon: 10[KNL]  192: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
2017-05-25 09:42:56 charon: 10[KNL]  208: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
....
2017-05-25 09:42:56 charon: 10[KNL]  224: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
....
2017-05-25 09:42:56 charon: 10[KNL]  240: 00 00 00 00 01 00 00 00 02 00 01 20 20 00 00 00  ....
....  ...
2017-05-25 09:42:56 charon: 10[KNL]  256: 00 00 00 00 60 00 12 00 72 66 63 34 31 30 36 28  ....`..
.rfc4106(
2017-05-25 09:42:56 charon: 10[KNL]  272: 67 63 6D 28 61 65 73 29 29 00 00 00 00 00 00 00  gcm(aes
))....
2017-05-25 09:42:56 charon: 10[KNL]  288: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
....
2017-05-25 09:42:56 charon: 10[KNL]  304: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
....
2017-05-25 09:42:56 charon: 10[KNL]  320: 00 00 00 00 00 00 00 00 A0 00 00 00 80 00 00 00  ....
....
2017-05-25 09:42:56 charon: 10[KNL]  336: 6A AA 3E C6 55 D7 B4 80 0A C4 9A CE 50 3F DD BD  j..U...
....P?..
2017-05-25 09:42:56 charon: 10[KNL]  352: 88 34 0F F2                                      .4..
2017-05-25 09:42:56 charon: 10[KNL] received netlink error: Function not implemented (38)
2017-05-25 09:42:56 charon: 10[KNL] unable to add SAD entry with SPI cd13aedb
2017-05-25 09:42:56 charon: 10[IKE] unable to install inbound and outbound IPsec SA (SAD) in kerne
l
2017-05-25 09:42:56 charon: 10[IKE] failed to establish CHILD_SA, keeping IKE_SA
```

With kernel 3.10.12 works fine:

```
2017-05-25 14:11:27 charon: 13[CFG]   proposal matches
2017-05-25 14:11:27 charon: 13[CFG] received proposals: ESP:AES_GCM_16_128/NO_EXT_SEQ
2017-05-25 14:11:27 charon: 13[CFG] configured proposals: ESP:AES_GCM_16_128/MODP_2048/NO_EXT_SEQ
2017-05-25 14:11:27 charon: 13[CFG] selected proposal: ESP:AES_GCM_16_128/NO_EXT_SEQ
2017-05-25 14:11:27 charon: 13[CFG] selecting traffic selectors for us:
2017-05-25 14:11:27 charon: 13[CFG]  config: 10.70.0.144/29, received: 10.70.0.144/29 = match: 10.
70.0.144/29
2017-05-25 14:11:27 charon: 13[CFG] selecting traffic selectors for other:
2017-05-25 14:11:27 charon: 13[CFG]  config: 10.5.0.0/24, received: 10.5.0.0/24 = match: 10.5.0.0/
24
2017-05-25 14:11:27 charon: 13[CHD]   using AES_GCM_16 for encryption
2017-05-25 14:11:27 charon: 13[CHD] adding inbound ESP SA
2017-05-25 14:11:27 charon: 13[CHD]   SPI 0xc8ebaa57, src 192.168.7.7 dst 192.168.7.110
2017-05-25 14:11:27 charon: 13[KNL] adding SAD entry with SPI c8ebaa57 and reqid {1}  (mark 0/0x00
000000)
2017-05-25 14:11:27 charon: 13[KNL]   using encryption algorithm AES_GCM_16 with key size 160
2017-05-25 14:11:27 charon: 13[KNL]   using replay window of 32 packets
2017-05-25 14:11:27 charon: 13[KNL] sending XFRM_MSG_UPDSA 202: = 336 bytes @ 0xafa63610
2017-05-25 14:11:27 charon: 13[KNL]    0: 50 01 00 00 1A 00 05 00 CA 00 00 00 D6 30 00 00  P....
......0..
2017-05-25 14:11:27 charon: 13[KNL]   16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
....
2017-05-25 14:11:27 charon: 13[KNL]   32: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
....
2017-05-25 14:11:27 charon: 13[KNL]   48: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
....
2017-05-25 14:11:27 charon: 13[KNL]   64: 00 00 00 00 00 00 00 00 C0 A8 07 6E 00 00 00 00  ....
....n....
2017-05-25 14:11:27 charon: 13[KNL]   80: 00 00 00 00 00 00 00 00 C8 EB AA 57 32 00 00 00  ....
....W2...
2017-05-25 14:11:27 charon: 13[KNL]   96: C0 A8 07 07 00 00 00 00 00 00 00 00 00 00 00 00  ....
....
2017-05-25 14:11:27 charon: 13[KNL]  112: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....
....
2017-05-25 14:11:27 charon: 13[KNL]  128: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ....
....
2017-05-25 14:11:27 charon: 13[KNL]  144: 60 0A 00 00 00 00 00 00 10 0E 00 00 00 00 00 00  `...
....
2017-05-25 14:11:27 charon: 13[KNL]  160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
....
```

```
2017-05-25 14:11:27 charon: 13[KNL]  176: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..........
..........
2017-05-25 14:11:27 charon: 13[KNL]  192: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..........
..........
2017-05-25 14:11:27 charon: 13[KNL]  208: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..........
..........
2017-05-25 14:11:27 charon: 13[KNL]  224: 01 00 00 00 02 00 01 20 20 00 00 00 00 00 00 00  ..........
  ........
2017-05-25 14:11:27 charon: 13[KNL]  240: 60 00 12 00 72 66 63 34 31 30 36 28 67 63 6D 28  `...rfc
4106(gcm(
2017-05-25 14:11:27 charon: 13[KNL]  256: 61 65 73 29 29 00 00 00 00 00 00 00 00 00 00 00  aes))..
..........
2017-05-25 14:11:27 charon: 13[KNL]  272: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..........
..........
2017-05-25 14:11:27 charon: 13[KNL]  288: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..........
..........
2017-05-25 14:11:27 charon: 13[KNL]  304: 00 00 00 00 A0 00 00 00 80 00 00 00 6D BE 29 A1  ..........
.....m.).
2017-05-25 14:11:27 charon: 13[KNL]  320: 3F 20 0B E3 D7 27 59 11 F2 5F E2 2C 87 B7 75 4A  ? ...'Y
..._.,..uJ
2017-05-25 14:11:27 charon: 13[KNL] received (2) 202: = 36 bytes @ 0xae7012c0
2017-05-25 14:11:27 charon: 13[KNL]    0: 24 00 00 00 02 00 00 00 CA 00 00 00 D6 30 00 00  $.........
......0..
2017-05-25 14:11:27 charon: 13[KNL]   16: 00 00 00 00 50 01 00 00 1A 00 05 00 CA 00 00 00  ....P...
..........
2017-05-25 14:11:27 charon: 13[KNL]   32: D6 30 00 00                                     .0..
2017-05-25 14:11:27 charon: 13[CHD] adding outbound ESP SA
2017-05-25 14:11:27 charon: 13[CHD]   SPI 0xc69b7c85, src 192.168.7.110 dst 192.168.7.7
2017-05-25 14:11:27 charon: 13[KNL] adding SAD entry with SPI c69b7c85 and reqid {1}  (mark 0/0x00
000000)
2017-05-25 14:11:27 charon: 13[KNL]   using encryption algorithm AES_GCM_16 with key size 160
```

Do you have any idea how to get it working? I need to use 3.5.0 kernel due to memory limited embedded device.
Many thanks

History

#1 - 25.05.2017 14:29 - Jiri Zendulka

Correction: With kernel 3.12.10 GCM works fine.

#2 - 25.05.2017 20:59 - Noel Kuntze

- Category set to kernel

- Status changed from New to Feedback

- Assignee set to Noel Kuntze

I strongly doubt that this is a problem of strongSwan, especially because the kernel responds with "Not implemented". Make sure the module for AES-GCM is loaded in the kernel and the modules path is correct.

#3 - 29.05.2017 13:08 - Jiri Zendulka

Yes, you are right. The embedded device has SPEAR320 CPU with C3 crypto accelarator. C3 was enabled in kernel config so all crypto were performed via C3 which does not support GCM.
You can close the issue.

Many thanks.

#4 - 29.05.2017 14:54 - Noel Kuntze

- Status changed from Feedback to Closed

- Affected version deleted (5.4.0)

- Resolution set to Invalid