Description
Charon crashes when I activate load-tester plugin.

- strongwan 5.1.0
- gcc version 4.4.5 (Debian 4.4.5-8)
- compiled with --enable-load-tester

Got this from GDB:

```
01[NET] received packet: from 127.0.0.1[500] to 127.0.0.1[500] (272 bytes)
03[NET] sending packet: from 127.0.0.1[500] to 127.0.0.1[500] (305 bytes)
03[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(MULT_AUTH) ]
03[IKE] received cert request for "C=AR, ST=C.A.B.A., O=LuisV.com.ar, CN=CA LuisV.com.ar"
03[IKE] received cert request for "C=AR, ST=C.A.B.A., O=LuisV.com.ar, CN=CA LuisV.com.ar"
02[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(MULT_AUTH) ]
02[IKE] received cert request for "C=AR, ST=C.A.B.A., O=LuisV.com.ar, CN=CA LuisV.com.ar"
01[ENC] parsed IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ]
01[IKE] received retransmit of request with ID 0, retransmitting response
01[NET] sending packet: from 127.0.0.1[500] to 127.0.0.1[500] (305 bytes)
01[NET] received packet: from 127.0.0.1[500] to 127.0.0.1[500] (305 bytes)
01[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(MULT_AUTH) ]
01[IKE] received cert request for "C=AR, ST=C.A.B.A., O=LuisV.com.ar, CN=CA LuisV.com.ar"
01[IKE] received cert request for "C=AR, ST=C.A.B.A., O=LuisV.com.ar, CN=CA LuisV.com.ar"
04[IKE] sending cert request for "C=AR, ST=C.A.B.A., O=LuisV.com.ar, CN=CA LuisV.com.ar"
02[IKE] sending cert request for "C=AR, ST=C.A.B.A., O=LuisV.com.ar, CN=CA LuisV.com.ar"
04[IKE] sending cert request for "C=AR, ST=C.A.B.A., O=LuisV.com.ar, CN=CA LuisV.com.ar"
02[IKE] sending cert request for "C=AR, ST=C.A.B.A., O=LuisV.com.ar, CN=CA LuisV.com.ar"
```

Program received signal SIGSEGV, Segmentation fault.

```
[Switching to Thread 0x7ffff160e700 (LWP 29082)]
0x00007fff3244c64 in create_cert_enumerator (this=0x6308d0, cert=<value optimized out>,
    key=<value optimized out>, id=0x7ffff87b09d0, trusted=<value optimized out>)
at load_tester creds.c:369
369          peer_key = this->private->get_public_key(this->private);
(gdb) trace
Tracepoint 1 at 0x7ffff3244c64: file load_tester creds.c, line 369.
```

Got this from GDB:

```
Program received signal SIGSEGV, Segmentation fault.

[Switching to Thread 0x7ffff160e700 (LWP 29082)]
0x00007fff3244c64 in create_cert_enumerator (this=0x6308d0, cert=<value optimized out>,
    key=<value optimized out>, id=0x7ffff87b09d0, trusted=<value optimized out>)
at load_tester creds.c:369
369          peer_key = this->private->get_public_key(this->private);
```

19.03.2020 1/2
Let me know if I have to give more details.

cheers

**Associated revisions**

Revision 90031b2f - 24.09.2013 09:27 - Tobias Brunner
load-tester: Fix crash if private key was not loaded successfully

Fixes #417.

**History**

#1 - 24.09.2013 10:32 - Tobias Brunner
- Tracker changed from Issue to Bug
- Description updated
- Status changed from New to Closed
- Assignee set to Tobias Brunner
- Target version set to 5.1.1
- Resolution set to Fixed

There were no checks in the constructor or create_cert_enumerator() in source/src/libcharon/plugins/load_tester/load_tester_creds.c that verified that the private key was loaded successfully (there is a check, though, in create_private_enumerator()). So if the load-tester plugin was in fact unable to load the private key you configured in charon.plugins.load-tester.issuer_key it would explain the crash here:

```
369         peer_key = this->private->get_public_key(this->private);
```

When you start charon you should see a message like

```
01[CFG] loading load-tester private key from '/etc/ssl/vpnca/vpnca.key'
```

followed by at least one error message.

The associated commit should fix the crash, but you have to correct the issue with the private key to make this actually work.