# strongSwan - Issue #902

## Intermediate certificate is sent when enable hash and url and configured CA section with certuribase

20.03.2015 22:15 - Kathy Wan

| | | | |
|---|---|---|---|
| **Status:** | Closed | | |
| **Priority:** | Normal | | |
| **Assignee:** | | | |
| **Category:** | libcharon | | |
| **Affected version:** | 5.2.2 | **Resolution:** | No feedback |

**Description**

I am doing hash and url encoding of x509 certificate test with the strongswan running version 5.0.2 on Linux.
The connection profile I am testing is configured with PKI authentication as below.

in ipsec.conf

```
conn rw-pki
        left=%any
        leftsubnet=0.0.0.0/0
        leftcert=strongswan.cer
        leftid="CN=strongswan.net"
        leftfirewall=yes
        right=%any
        rightsourceip=x.x.x.x/n
        auto=add
        reauth=yes
```

The CA setction in ipsec.conf is as below:

```
ca strongswanIm
        cacert=Interca.strongswan.cer
        certuribase=http://xx.strongswan.xx/certs/
        auto=add
```

strongswan.cer is the entity certificate issued by Interca.strongswan.cer.
Interca.strongswan.cer is the intermediate certificate and issued by root ca certificate root.strongswan.cer.

If I put Interca.strongswan.cer in the folder ipsec.d/cacert, strongswan.cer is sent out as hash and url, but intermediate certificate Interca.strongswan.cer is also sent out with complete certificate in the certificate payload of auth response.

If I remove the Interca.strongswan.cer from the folder ipsec.d/cacerts, strongswan sends out strongswan.cer whole certificate instead of hash and url. It will not send out intermediate certificate since it is not there.

So, it looks to me that in the case that intermediate certificate exists, the intermediate certificate need be in the cacerts folder and will be sent out if we want to send hash and url of entity certificate.

Is there any way not to send out intermediate certificate while sending out the hash and url of entity certificate?

**Related issues:**

| | |
|---|---|
| Related to Feature #3234: Intermediate certificates sent when using hash-and-url | **Closed** |

### History

#### #1 - 20.03.2015 22:17 - Kathy Wan

miss "not" in the sentence below.
"It will not send out intermediate certificate since it is there."
should be "It will not send out intermediate certificate since it is not there."

#### #2 - 23.03.2015 15:06 - Tobias Brunner

*- Description updated*

*- Status changed from New to Feedback*

*- Priority changed from High to Normal*

Is there any way not to send out intermediate certificate while sending out the hash and url of entity certificate?

The hash-and-url functionality is currently limited to end-entity certificates. And there is currently no option to prevent the intermediate certificate from getting sent. Either no certificates are sent at all (*leftsendcert=never*), or all certificates are sent (except the root).

#### #3 - 11.01.2019 23:02 - Noel Kuntze

*- Category set to libcharon*

*- Status changed from Feedback to Closed*

*- Resolution set to No feedback*

#### #4 - 30.10.2019 11:38 - Tobias Brunner

*- Related to Feature #3234: Intermediate certificates sent when using hash-and-url added*