strongSwan - Issue #3482

Not able to set RSA authentication via swanctl.conf

12.06.2020 14:47 - Jiri Zendulka

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.8.4	**Resolution:**	No change required

Description

Hello,

I try to migrate from ipsec.conf to swanctl.conf(vici) but I am not successfull with RSA authentication.

My swanctl.conf:

```
connections {
  ipsec2 {
    local_addrs = 0.0.0.0
    remote_addrs = 10.65.0.64
    local {
      auth = rsa
      certs = /etc/ipsec.d/certs/local-cert2.pem
    }
    remote {
      auth = rsa
      certs = /etc/ipsec.d/certs/remote-cert2.pem
    }
    children {
      ipsec2 {
        local_ts = 192.168.202.0/24
        remote_ts = 192.168.102.0/24
        mode = tunnel
        updown = /etc/scripts/updown
        life_time = 3600
        rekey_time = 3060
        rand_time = 540
        esp_proposals = aes128-sha1,3des-sha1
        start_action = start
      }
    }
    version = 1
    rekey_time = 3060
    over_time = 540
    rand_time = 540
    keyingtries = 0
    send_cert = always
    send_certreq = yes
    proposals = aes128-sha256-modp3072,aes128-sha1-modp2048,3des-sha1-modp1536
  }
}
secrets {
  rsa-2 {
    file = /etc/ipsec.d/private/local-key2.pem
  }
}
authorities {
  authorities-2 {
    cacert = /etc/ipsec.d/cacerts/cacert2.pem
  }
```

IPsec status

```
strongSwan swanctl 5.8.4
uptime: 2 hours, since Jun 12 12:18:23 2020
worker threads: 16 total, 11 idle, working: 4/0/1/0
job queues: 0/0/0/0
jobs scheduled: 0
IKE_SAs: 0 total, 0 half-open
mallinfo: sbrk 532480, mmap 0, used 283552, free 248928
loaded plugins: charon nonce pubkey pem openssl kernel-netlink socket-default vici updown xauth-ge
neric
ipsec2: IKEv1, reauthentication every 3060s
  local:  0.0.0.0
  remote: 10.65.0.64
  local public key authentication:
    id: C=CZ, ST=CESKO, O=CONEL, CN=client, E=xxx@host.conel
    certs: C=CZ, ST=CESKO, O=CONEL, CN=client, E=xxx@host.conel
  remote public key authentication:
    id: C=CZ, ST=CESKO, O=CONEL, CN=server, E=xxx@host.conel
    certs: C=CZ, ST=CESKO, O=CONEL, CN=server, E=xxx@host.conel
  ipsec2: TUNNEL, rekeying every 3060s
    local:  192.168.202.0/24
    remote: 192.168.102.0/24
```

Charon complains on "unsupported authentification"

```
2020-06-12 14:00:51 charon: 15[IKE] no private key found for 'xxxxxx'
2020-06-12 14:00:51 charon: 15[CFG] configuration uses unsupported authentication
```

Could you help me how should I set RSA authentication?
There are lot of examples for pubkey authentication but not for rsa. There are some for rsa/pss-sha512 but I am not sure if it is equivalent to left/rightauth=rsa in ipsec.conf

PSK works me OK.

Many thanks.

History

#1 - 12.06.2020 15:01 - Tobias Brunner

- Category set to configuration

- Status changed from New to Feedback

```
secrets {
  rsa-2 {
    file = /etc/ipsec.d/private/local-key2.pem
  }
}
```

That's not actually how this works. Such *rsa<suffix>* sections are only used to provide passwords for encrypted keys and they only work with relative filenames (in this case to the rsa directory). They can't be used to load keys from arbitrary locations. If you don't want to move your key to /etc/swanctl/private (or rsa) you can put a symlink there that points to the other location.

Using absolute paths does work for the certificates (also in *authorities* sub-sections), though.

#2 - 15.06.2020 10:27 - Jiri Zendulka

OK, I moved key file to /etc/swanctl/rsa but it still does not work. Charon reports the same.

Is authentication rsasig set correctly by "auth = rsa" ?

#3 - 15.06.2020 11:24 - Tobias Brunner

> OK, I moved key file to /etc/swanctl/rsa but it still does not work. Charon reports the same.

Check swanctl --list-certs (if the private key was loaded successfully, the certificate is marked with "has private key"). Read the log and look for errors when credentials are loaded.

> Is authentication rsasig set correctly by "auth = rsa" ?

Yes, that's OK (*rsa* is just an alias for *pubkey*, though).

#4 - 15.06.2020 14:31 - Jiri Zendulka

It works now. You close the issue.

Many thanks for support.

#5 - 15.06.2020 14:40 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No change required