# strongSwan - Issue #3614

## Certificate renewal for about to expire certificates

30.10.2020 10:34 - Digambar Ingale

| | | | |
|---|---|---|---|
| **Status:** | Feedback | | |
| **Priority:** | Normal | | |
| **Assignee:** | | | |
| **Category:** | configuration | | |
| **Affected version:** | 5.9.0 | **Resolution:** | |

**Description**

1. Certificate Configuration.:
Same configuration is there on the both hosts.
I have setup where we have created self signed root certificate, intermediate cert1... intermediate cert5, then device2Cert and device1Cert generated from intermediate cert5.
I have active tunnel created using these certificates.

2. Now, We want to test the certificate expiration/renewal impact on active tunnel. Suppose my device2Cert is about to expire. Before the old certificate gets expired I created new device2Cert with new expiration date.

I have following doubts regarding certificate renewal :
i ) What is the best way to replace the old device2Cert which is about to expire (without impacting the tunnel)?
ii) Do I need to take the tunnel down to renew certificates (swanctl --terminate --ike <conn_name>)?
iii) I tried to remove the (device2Cert)expired certificates with swanctl --flush-cert but it just removes the peer certificates from the device and the certificate which is expired still remain listed in swanctl --list-cert.

I am using following strongswan version:
[root@dipsechost1 ~]# swanctl --version
strongSwan swanctl 5.9.0

### History

**#1 - 30.10.2020 13:30 - Tobias Brunner**

*- Category set to configuration*

*- Status changed from New to Feedback*

*- Assignee deleted (Andreas Steffen)*

*- Priority changed from High to Normal*

> 1. Certificate Configuration.:
> Same configuration is there on the both hosts.

So you have all certificates installed on both? Or are the end-entity certificates only on the respective host?

> 2. Now, We want to test the certificate expiration/renewal impact on active tunnel.

Active tunnels are not affected by this. Certificates are only checked during authentication (or re-authentication if that's used). See ExpiryRekey for details.

> Suppose my device2Cert is about to expire. Before the old certificate gets expired I created new device2Cert with new expiration date.

OK. Device 1 will only see this new certificate if it receives it during authentication (unless you install it on both hosts, but then the expiration date has no effect at all because local certificates are always fully trusted).

> i ) What is the best way to replace the old device2Cert which is about to expire (without impacting the tunnel)?

As mentioned above, active tunnels are not affected at all, they can be rekeyed indefinitely. Only if the SA is reestablished (e.g. due to connectivity issues) or reauthenticated will the certificates checked again.

ii) Do I need to take the tunnel down to renew certificates (swanctl --terminate --ike <conn_name>)?

On the initiator, yes. When reestablishing/reauthenticating, the previous certificate will be reused (the same applies to the other configuration parameters).

iii) I tried to remove the (device2Cert)expired certificates with swanctl --flush-cert but it just removes the peer certificates from the device and the certificate which is expired still remain listed in swanctl --list-cert.

If you explicitly referred to the certificate in the configuration, you will also have to reload that via --load-conns. But if you referred to it via identity and loaded the old/new certificate via --load-creds, you only need to re-initiate after terminating the connection to use the new one.