Updating RPKI Validation software to the APNIC single TA

George Michaelson

February 27 2018

Updating RPKI Validation software to the APNIC single TA

On February 4, APNIC deprecated all the Trust Anchor Locators (TAL) other than the one active TAL which points to currently active RPKI products. At this time APNIC also remove the related .cer top level Trust Anchor Certificates.

Anyone operating an RPKI validator, or acting as a relying party should re-configure your system to remove the old TAL, and related certificates. No live products lie under these old trust anchors. All live products lie under one trust anchor now.

Re-configuration for three popular RPKI validation systems is as follows:

1. rpki.net rcynic validator

The rcynic system supports three modes of run-time configuration of TAL. In a directory, by reference to the certificate, or by reference to a TAL file. The current head GIT state of the rcynic validator code has the correct APNIC TAL in the `sample-trust-anchors/` sub-directory. If you cannot install this version of code, to reconfigure rcynic, perform one of the three following operations depending on how you configured your system.

a. using `trust-anchor-directory` as a directory of configured TAL

Consult the installed `rcynic.conf` runtime configuration file for the location of the `trust-anchor-directory` setting.

In this example, it is `/etc/rpki/trust-anchors`

```
cd /etc/rpki/trust-anchors
rm apnic-rpki-root-ripe-origin.tal
rm apnic-rpki-root-arin-origin.tal
rm apnic-rpki-root-lacnic-origin.tal
rm apnic-rpki-root-afrinic-origin.tal
```

b. using embedded references to the TA certificates as .cer files.

Edit the installed `rcynic.conf` runtime configuration file for the location of the `trust-anchor.x` setting. There will be a number of lines, one per trust anchor, each numbered uniquely.

For the list of five trust anchors which referred to APNIC, remove all but the one which references the file sourced from `rsync://rpki.apnic.net/repository/apnic-rpki-root-iana-origin.cer`

Eg, if this file has been placed in `/etc/rpki/trust-anchors/ta-apnic.cer` and is your first trust anchor, the file would be set to say:

```
trust-anchor.1          = /etc/rpki/trust-anchors/ta-apnic.cer
```

c. using embedded references to the TAL.

Edit the installed `rcynic.conf` runtime configuration file for the location of the `trust-anchor-locator.x` setting. There will be a number of lines, one per trust anchor locator, each numbered uniquely.

For the list of five trust anchor locators which referred to APNIC, remove all but the one which references the current TAL. The tal is as follows:

```
rsync://rpki.apnic.net/repository/apnic-rpki-root-iana-origin.cer

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAx9RWSL61YAAYumEiU8z8
qH2ETVIL01ilxZlzIL9JYSORMN5Cmtf8V2JblIealSqgOTGjvSjEsiV73s67zYQI
7C/iSOb96uf3/s86NqbxDiFQGN8qG7RNcdgVuUlAidl8WxvLNI8VhqbAB5uSg/Mr
LeSOvXRja041VptAxIhcGzDMvlAJRwkrYK/Mo8P4E2rSQgwqCgae0ebY1CsJ3Cjf
i67C1nw7oXqJJovvXJ4apGmEv8az23OLC6Ki54Ul/E6xk227BFttqFV3YMtKx42H
cCcDVZZy01n7JjzvO8ccaXmHIgR7utnqhBRNNq5Xc5ZhbkrUsNtiJmrZzVlgU6Ou
0wIDAQAB
```

Eg, if this file has been placed in `/etc/rpki/trust-anchors/ta-apnic.tal` and is your first trust anchor Locator, the file would be set to say:

```
trust-anchor-locator.1          = /etc/rpki/trust-anchors/ta-apnic.tal
```

2. RIPE NCC rpki-validator

The simplest method to run with the current single APNIC TAL is to upgrade to version 2.24 or later ie `rpki-validator-app-2.24`

If upgrading to the current version is not possible, locate the `conf/tal/` directory on your system and remove all APNIC related files except `conf/tal/apnic.tal`

This file should contain the following:

```
ca.name = APNIC RPKI Root
certificate.location = rsync://rpki.apnic.net/repository/apnic-rpki-root-iana-origin.cer
public.key.info = MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAx9RWSL61YAAYumEiU8z8
qH2ETVIL01ilxZlzIL9JYSORMN5Cmtf8V2JblIealSqgOTGjvSjEsiV73s67zYQI
7C/iSOb96uf3/s86NqbxDiFQGN8qG7RNcdgVuUlAidl8WxvLNI8VhqbAB5uSg/Mr
LeSOvXRja041VptAxIhcGzDMvlAJRwkrYK/Mo8P4E2rSQgwqCgae0ebY1CsJ3Cjf
i67C1nw7oXqJJovvXJ4apGmEv8az23OLC6Ki54Ul/E6xk227BFttqFV3YMtKx42H
cCcDVZZy01n7JjzvO8ccaXmHIgR7utnqhBRNNq5Xc5ZhbkrUsNtiJmrZzVlgU6Ou
0wIDAQAB
prefetch.uris = rsync://rpki.apnic.net/member_repository/
```

3. RPSTIR

If you update RPSTIR to the current GIT state from `https://github.com/bgpsecurity/rpstir.git` it already includes only the APNIC single TA in its example configuration directory `sample-ta/`

To modify an installed RPSTIR system, locate the `/usr/local/etc/rpstir` directory and remove all but the current live APNIC TAL. This should be in a file with contents as follows:

```
rsync://rpki.apnic.net/repository/apnic-rpki-root-iana-origin.cer
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAx9RWSL61YAAYumEiU8z8
qH2ETVIL01ilxZlzIL9JYSORMN5Cmtf8V2JblIealSqgOTGjvSjEsiV73s67zYQI
7C/iSOb96uf3/s86NqbxDiFQGN8qG7RNcdgVuUlAidl8WxvLNI8VhqbAB5uSg/Mr
LeSOvXRja041VptAxIhcGzDMvlAJRwkrYK/Mo8P4E2rSQgwqCgae0ebY1CsJ3Cjf
i67C1nw7oXqJJovvXJ4apGmEv8az23OLC6Ki54Ul/E6xk227BFttqFV3YMtKx42H
```

```
cCcDVZZy01n7JjzvO8ccaXmHIgR7utnqhBRNNq5Xc5ZhbkrUsNtiJmrZzVlgU6Ou
0wIDAQAB
```

then, in the `rpstir.conf` file, modify the `TrustAnchorLocators` setting

For example, given the apnic TAL in a file `/usr/local/etc/rpstir/apnic.tal`

```
TrustAnchorLocators \
  /usr/local/etc/rpstir/apnic.tal
```