Key rollover @RIPE NCC

draft-ietf-sidr-res-certs-18#section-8

draft-huston-sidr-keyroll-00.txt
Before rollover

**Certificate**

- Issuer: TA
  - Subject: parent

**AIA Pointers**

- Parent CRL
- Parent MFT

**SIA Pointers**

- Entry

**Repository Publication Point**

- Issuer: child
  - Subject: gr.child
  - CRL
- MFT

- Issuer: TA
  - Subject: parent
  - MFT

- Issuer: child
  - Subject: ROA
  - MFT
Phase 1 - Request new certificate

1. Generate *new* key

2. Generate certificate request

3. Request parent to issue and publish new certificate
   
   Publish manifest and CRL for new certificate (empty)

4. Wait for *staging period*
   
   ➡️ *Not implemented*
After phase 1
new certificate published
Phase 2 - Activate new certificate

5  a) Suspend request processing

b) Mark *current* CA *old*, and *new* CA *pending*

6  Re-issue all subordinate certificates using the *pending* CA

7  Re-issue subordinate signed objects using the *pending* CA (except for manifests)
Phase 2 - Activate new certificate

8  Re-issue manifest for *old CA*
   ➡ CRL is the only remaining entry

9  a) Mark *pending CA current*

   b) Resume processing requests
After phase 2
new certificate activated

CA “parent*”

CA “TA”

CA “parent”

Issuer: parent*
Subject: parent

Issuer: TA
Subject: parent

Issuer: TA
Subject: parent*

Issuer: TA
Subject: parent

parent CRL

parent MFT

parent* CRL

parent* MFT

NEW!

Issuer: child
Subject: gr.child

Issuer: child
Subject: ROA

child CRL

child MFT

After phase 2
new certificate activated
Phase 2

$ rsync --list-only rsync://certrepo.ripe.net/rta

CN=RTA,O=RIPE%20NCC,C=NL.cer
CN=RTA,O=RIPE%20NCC,C=NL.crl
CN=RTA,O=RIPE%20NCC,C=NL.mnf
CN=dkH6Hh8BYnfyVZoYaO2FcAXyn9Q.cer
CN=EQPBzzm03_gZdrqO6tOS7eHjyXY.cer
Phase 2

$ rsync --list-only rsync://certrepo.ripe.net/prod/

d7/0b38ff-44ce-44c2-805b-50b7489300ed/1

EQPBzzm03_gZdrqO6tOS7eHjYXY.crl
EQPBzzm03_gZdrqO6tOS7eHjYXY.mnf
dkH6Hh8BYnfyVZoYaO2FcAXyn9Q.crl
dkH6Hh8BYnfyVZoYaO2FcAXyn9Q.mnf
anhbxfSN3kbcKt61dEkIPlULUSk.cer
2fv72__yOQgInutV4qCKwmSdw14.cer
CfWKr5qQwLRdsnw67qLOqSAQq4g.cer
nKALymnMlRyMITi7oy49AlbUUhA.cer
Phase 3 - Revoke old CA

10 Generate revocation request for old key

11 Remove old CRL and manifest when request is performed
After phase 3
old key revoked
RIPE NCC repositories

- online CA & member CAs: rsync://certrepo.ripe.net/prod/
- resource trust anchor: rsync://certrepo.ripe.net/rta/
- external trust anchor: rsync://certrepo.ripe.net/eta/
Questions?