Multiple Repository Publication Points support in the Resource Public Key Infrastructure (RPKI)

Roque Gagliano
Carlos Martinez
Terry Manderson

SIDR WG Meeting – IETF87

Recap, what problem we are solving?

- Provide means for repository operators to indicate the presence of multiple publication points of repository data
- Motivation:
  - An additional tool for repository HA engineering
  - Multiple transport protocols for the same repo data
  - Break DNS dependencies
- Document organizations:
  - Update on TAL format (RFC 6490)
  - Recommendation on Multi-operator support in certificates

TAL Changes

```
rsync://rpki-fe1.lacnic.net/rpki/lacnic/rta-lacnic-rpki.cer
rsync://rpki-fe2.lacnic.net/rpki/lacnic/rta-lacnic-rpki.cer

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqZEzhYK0+PtDOPfuk
VIppgSKAhlO0H60DRP48by9gr5/yDHu2KXhOmnMg46sYsUIpfgtBS9+VtrqWz
SZx8tk9GS/3SMQ+YfMVwwAyYjsex14Uzto4GjONALE5oh1M3+glRQduD6vzSv
KXEqdfqDRktwyoD74cV57bW3tBAexB7GglITbInyQAsmdngtfg2LUMrcROHHF
```

Testing existing resolvers:

1) One URI with line break

```
rsync://repository.lacnic.net/rpki/lacnic/rta-lacnic-rpki.cer

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqZEzhYK0+PtDOPfub/K
VIppgSKAhlO0H60DRP48by9gr5/yDHu2KXhOmnMg46sYsUIpfgtBS9+VtrqWziJ
SZx8tk9GS/3SMQ+YfMVwwAyYjsex14Uzto4GjONALE5oh1M3+glRQduD6vzSwOD
KXEqdfqDRktwyoD74cV57bW3tBAexB7GglITbInyQAsmdngtfg2LUMrcROHHP86
```

2) Several “working” URI:

```
rsync://rpki-fe1.lacnic.net/rpki/lacnic/rta-lacnic-rpki.cer
rsync://rpki-fe2.lacnic.net/rpki/lacnic/rta-lacnic-rpki.cer

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqZEzhYK0+PtDOPfub/
VIppgSKAhlO0H60DRP48by9gr5/yDHu2KXhOmnMg46sYsUIpfgtBS9+VtrqWz
SZx8tk9GS/3SMQ+YfMVwwAyYjsex14Uzto4GjONALE5oh1M3+glRQduD6vzSw
KXEqdfqDRktwyoD74cV57bW3tBAexB7GglITbInyQAsmdngtfg2LUMrcROHHP8
```

3) Several, URI with first one not working:

```
rsync://bad.lacnic.net/rpki/lacnic/rta-lacnic-rpki.cer
rsync://rpki-fe2.lacnic.net/rpki/lacnic/rta-lacnic-rpki.cer

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqZEzhYK0+PtDOPfub/K
VIppgSKAhlO0H60DRP48by9gr5/yDHu2KXhOmnMg46sYsUIpfgtBS9+VtrqWziJ
SZx8tk9GS/3SMQ+YfMVwwAyYjsex14Uzto4GjONALE5oh1M3+glRQduD6vzSwOD
KXEqdfqDRktwyoD74cV57bW3tBAexB7GglITbInyQAsmdngtfg2LUMrcROHHP86
```

Testing results:

	RIPE NCC	RCYNIC	BBN
One URI with line break	✓	✓	✓
Several “working” URI	✓	✓	✗
Several, URI with first one not working	✗	✗	✗

Additionally:

Successfully modified RIPE NCC validator CLI with simple logic to overcome last test (2 files, 10 lines):

```
$ bin/certification-validator -t tal/lacnic_bad_new.tal -o validate
lenght: 2
try: rsync://bad.lacnic.net/rpki/lacnic/rta-lacnic-rpki.cer
try: rsync://rpki-fe2.lacnic.net/rpki/lacnic/rta-lacnic-rpki.cer
```

Conclusions and next steps:

Conclusions:

- Simple change in TAL format provides higher HA
- Most existing RP not impacted
- Simple change available to change RP logic

Next Steps:

- Do similar test on certificates multi-pub support
- Publishes reviewed version if needed for WGLC before Vancouver

Question to WG:

- Should this document obsolete RFC 6490?

References and Ack

- Modified RIPE-cli validator code and testing TAL files:

https://github.com/carlosm3011/rpki-validator-mpp

Thanks Gerardo Rada for the hacking help!