



**RIPE NCC**  
RIPE NETWORK COORDINATION CENTRE

# RPKI Repository Delta Protocol

New I-D version and  
first operational experience

# draft-ietf-sidr-delta-protocol-02



- Changes from previous version
  - The "hash" attribute in the update notification file is back
  - Implementation is now allowed to aggregate changes from multiple CAs in a single delta
  - Reworded text – hoping to make it more readable
  - Let us know if it works for you



# **First operational experience**

# RRDP Recap



<https://rrdp.ripe.net/notification.xml>

```
<?xml version="1.0"?>
<notification
  xmlns="http://www.ripe.net/rpki/rrdp"
  version="1"
  session_id="582a8873-bd02-46f3-9acb-5cdb09e52fc6"
  serial="2156"
>
  <snapshot
    uri="https://rrdp.ripe.net/582a8873-bd02-46f3-9acb-5cdb09e52fc6/2156/snapshot.xml"
    hash="2D5A80D497F2C87B03B4CE5C68485883DF732F583521B028C03637BFA9F31438"
  />
  <delta
    serial="2156"
    uri="https://rrdp.ripe.net/582a8873-bd02-46f3-9acb-5cdb09e52fc6/2156/delta.xml"
    hash="3C346F15F96D4F7821C9725E79557BFC8B6E7AF59405B686E668329DECE494D5"
  /><delta
    serial="2155"
    uri="https://rrdp.ripe.net/582a8873-bd02-46f3-9acb-5cdb09e52fc6/2155/delta.xml"
    hash="5F60AB688C3836808BDCF2B23CA5F984BBC7ECF9FAE78359B121ABB027D3FF6F"
  />
  ...
```

# RRDP Recap



<https://rrdp.ripe.net/notification.xml>

```
<?xml version="1.0"?>
<notification
  xmlns="http://www.ripe.net/rpki/rrdp"
  version="1"
  session_id="582a8873-bd02-46f3-9acb-5cdb09e52fc6"
  serial="2156"
>
  <snapshot
    uri="https://rrdp.ripe.net/582a8873-bd02-46f3-9acb-5cdb09e52fc6/2156/snapshot.xml"
    hash="2D5A80D497F2C87B03B4CE5C68485883DF732F583521B028C03637BFA9F31438"
  />
  <delta
    serial="2156"
    uri="https://rrdp.ripe.net/582a8873-bd02-46f3-9acb-5cdb09e52fc6/2156/delta.xml"
    hash="3C346F15F96D4F7821C9725E79557BFC8B6E7AF59405B686E668329DECE494D5"
  /><delta
    serial="2155"
    uri="https://rrdp.ripe.net/582a8873-bd02-46f3-9acb-5cdb09e52fc6/2155/delta.xml"
    hash="5F60AB688C3836808BDCF2B23CA5F984BBC7ECF9FAE78359B121ABB027D3FF6F"
  />
  ...
</notification>
```

<https://rrdp.ripe.net/.../2156/snapshot.xml>

```
<?xml version="1.0"?>
<snapshot xmlns="http://www.ripe.net/rpki/rrdp"
  version="1"
  session_id="582a8873-bd02-46f3-9acb-5cdb09e52fc6"
  serial="2156">
  <publish
    uri="rsync://rpki.ripe.net/repository/RIPE/la-QqJYiFPOxhXEEoUxZG6fBBTk.cer">
    MIIFgjCCBGqgAwIBAgIFAKvPeBAwDQYJKoZIhvcNA...S9Ou0LrA==
  </publish>
  <publish
    uri="rsync://rpki.ripe.net/repository/RIPE/.../nlr-QG_s2EvHYhrmxBDDhAWL0tE.roa">
    MIAGCSqGS1b3DQEHAqCAMIACAQMxDzANBgIghkg...AAAAAAAAA=
  </publish>
  ...
</snapshot>
```

# RRDP Recap



<https://rrdp.ripe.net/notification.xml>

```
<?xml version="1.0"?>
<notification
  xmlns="http://www.ripe.net/rpki/rrdp"
  version="1"
  session_id="582a8873-bd02-46f3-9acb-5cdb09e52fc6"
  serial="2156"
>
  <snapshot
    uri="https://rrdp.ripe.net/582a8873-bd02-46f3-9acb-5cdb09e52fc6/2156/snapshot.xml"
    hash="2D5A80D497F2C87B03B4CE5C68485883DF732F583521B028C03637BFA9F31438"
  />
  <delta
    serial="2156"
    uri="https://rrdp.ripe.net/582a8873-bd02-46f3-9acb-5cdb09e52fc6/2156/delta.xml"
    hash="3C346F15F96D4F7821C9725E79557BFC8B6E7AF59405B686E668329DECE494D5"
  />
  <delta
    serial="2155"
    uri="https://rrdp.ripe.net/582a8873-bd02-46f3-9acb-5cdb09e52fc6/2155/delta.xml"
    hash="5F60AB688C3836808BDCF2B23CA5F984BBC7ECF9FAE78359B121ABB027D3FF6F"
  />
  ...
</notification>
```

<https://rrdp.ripe.net/.../2156/snapshot.xml>

```
<?xml version="1.0"?>
<snapshot xmlns="http://www.ripe.net/rpki/rrdp"
  version="1"
  session_id="582a8873-bd02-46f3-9acb-5cdb09e52fc6"
  serial="2156">
  <publish
    uri="rsync://rpki.ripe.net/repository/RIPE/la-QqJYiFPOxhXEEoUxZG6fBBTk.cer">
    MIIFGjCCBGqgAwIBAgIFAKvPeBAwDQYJKoZIhvcNA...S9Ou0LrA==
  </publish>
  <publish
    uri="rsync://rpki.ripe.net/repository/RIPE/.../nlr-QG_s2EvHYhrmxBDDhAWL0tE.roa">
    MIAGCSqGSib3DQEHAqCAMIACAQMxDzANBgIghkg...AAAAAAAA=
  </publish>
  ...
</snapshot>
```

<https://rrdp.ripe.net/.../2156/delta.xml>

```
<?xml version="1.0"?>
<delta
  xmlns="http://www.ripe.net/rpki/rrdp"
  version="1"
  session_id="582a8873-bd02-46f3-9acb-5cdb09e52fc6"
  serial="2156"
>
  <publish
    uri="rsync://rpki.ripe.net/repository/RIPE/.../RSD5LhrS-GezrtmsTozaS7KmN8.mft"
    hash="FFA1F300...CC2D9FB85A7F13EE11BEE0">
    MIAGCSqGSib3DQEHAqCAMIACAQMxDzANBgIghkgBZQM...SYAAAAAAAA=
  </publish>
  <withdraw
    uri="rsync://rpki.ripe.net/repository/.../BYLUBbmBp-ZSQudQNvxATPXzpqk.cer"
    hash="C3C3853A10E4A551...3E844F0D307D"
  />
  ...
</delta>
```

# RP's typical use-cases – #1



## No previous state

- Fetch notification file
- Fetch snapshot file
- Parse and store snapshot objects
- Remember session and serial

# RP's typical use-cases – #2



## With previous state

- Fetch notification file if it changed
- Compare remote session with local
- Compare remote serial with local
- Parse delta definitions
- Fetch, parse and apply deltas starting from local serial + 1 up to the remote serial
- Remember new serial



# RP's typical use-cases – #3



## With previous state – but too old

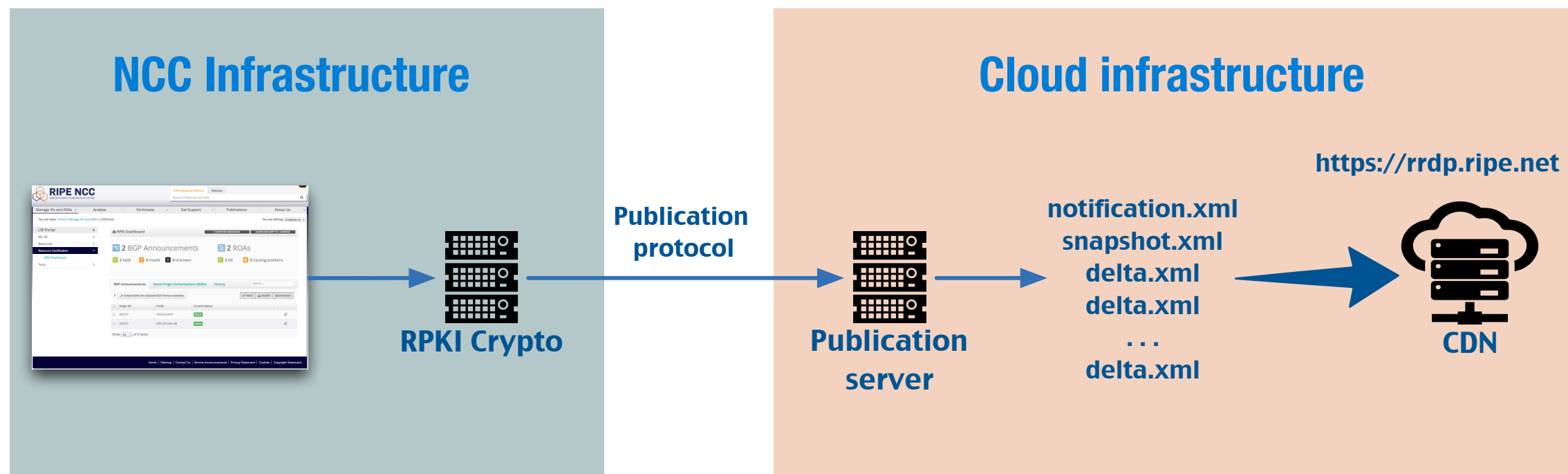
- Fetch notification file if it changed
- Compare remote session with local
- Compare remote serial with local
- Parse delta definitions
- (not enough deltas published)
- Fetch snapshot file
- Parse and store snapshot objects
- Remember new serial

# RIPE NCC RPKI Repository



- 3487 CER / MFT / CRL
- 3557 ROA
- 14018 objects total
  
- `du -s .../repository = 85M`
- `tar c .../repository = 43M`
- `snapshot.xml = 28M`

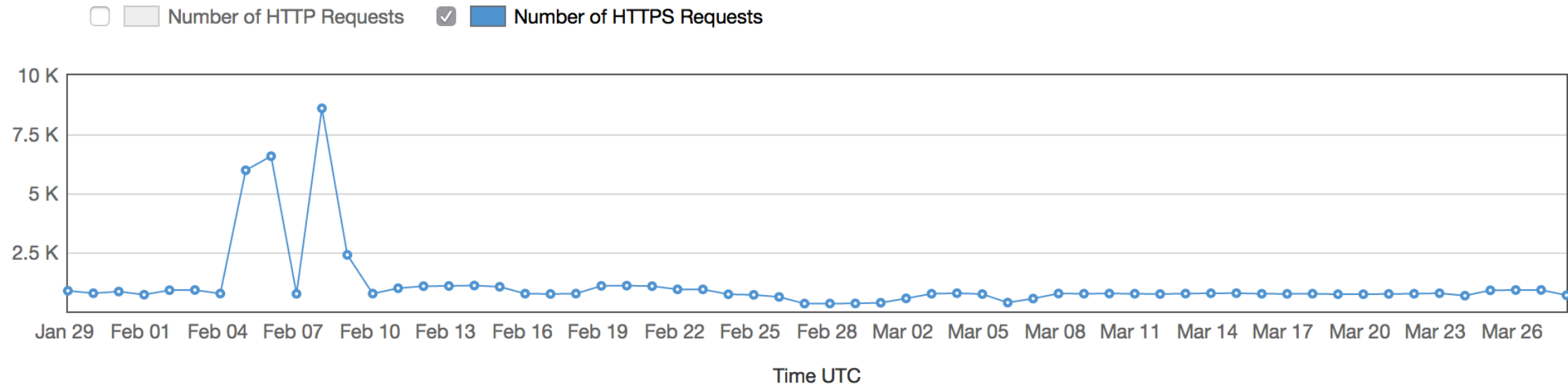
# Current deployment



# Some graphs

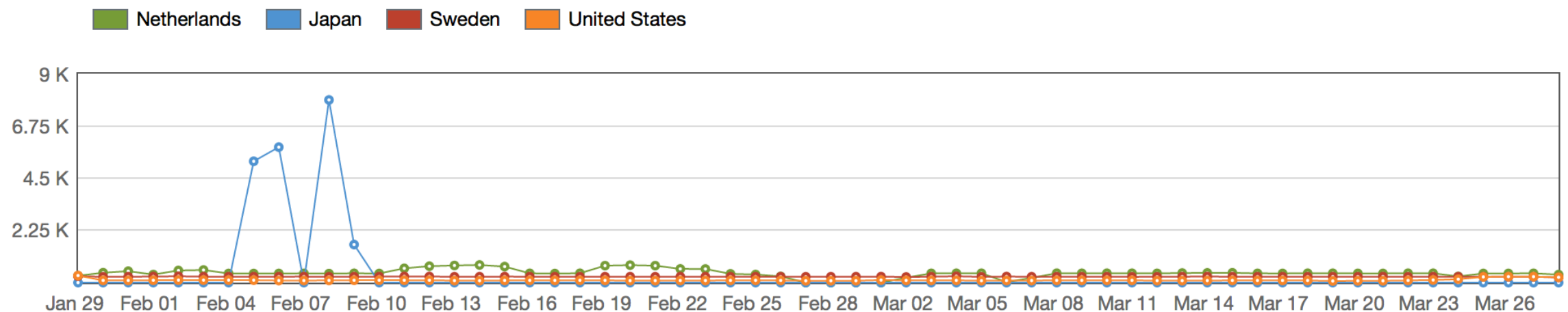


## Number of Requests ([Millions](#) | [Thousands](#) | [Not Scaled](#)) [Show Details](#)



**HTTP Requests:** Total: 0.011 K Average: 0.0002 K Minimum: 0 K Maximum: 0.004 K  
**HTTPS Requests:** Total: 66.49 K Average: 1.1082 K Minimum: 0.33 K Maximum: 8.599 K  
**All Requests:** Total: 66.501 K Average: 1.1084 K Minimum: 0 K Maximum: 8.599 K

## Location Trends ([Millions](#) | [Thousands](#) | [Not Scaled](#)) [Show Details](#)



# How often to generate deltas?



- 1 CA change → new delta → new notification

# How often to generate deltas?



- 1 CA change → new delta → new notification
  - 6407 deltas in notification file
  - notification.xml ~ 1MB

# How often to generate deltas?



- 1 CA change → new delta → new notification
  - 6407 deltas in notification file
  - notification.xml ~ 1MB
- 30 seconds

# How often to generate deltas?



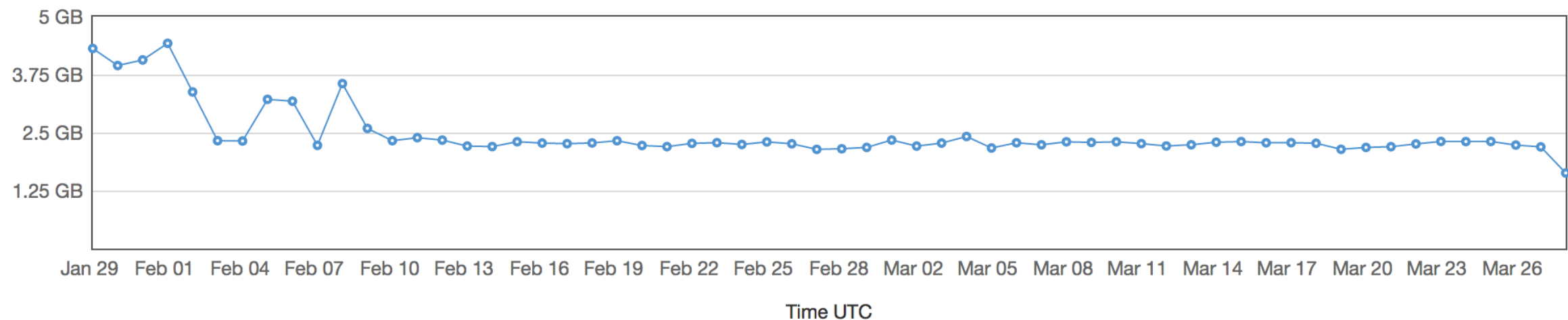
- 1 CA change → new delta → new notification
  - 6407 deltas in notification file
  - notification.xml ~ 1MB
- 30 seconds
  - 110 deltas in notification file
  - notification.xml ~ 20KB



# How often to generate deltas?



- 1 CA change → new delta → new notification
  - 6407 deltas in notification file
  - notification.xml ~ 1MB
- 30 seconds
  - 110 deltas in notification file
  - notification.xml ~ 20KB



<b>HTTP Data:</b>	<b>Total:</b> 0 GB	<b>Average:</b> 0 GB	<b>Minimum:</b> 0 GB	<b>Maximum:</b> 0 GB
<b>HTTPS Data:</b>	<b>Total:</b> 147.4048 GB	<b>Average:</b> 2.4567 GB	<b>Minimum:</b> 1.6297 GB	<b>Maximum:</b> 4.425 GB
<b>All Data:</b>	<b>Total:</b> 147.4048 GB	<b>Average:</b> 2.4567 GB	<b>Minimum:</b> 0 GB	<b>Maximum:</b> 4.425 GB

# How many deltas to list in the notification file?



- Until total size of deltas  $<$  snapshot size

# How many deltas to list in the notification file?



- Until total size of deltas  $<$  snapshot size
  - deltas for ~17 hours back
  - notification.xml ~ 20KB

# How many deltas to list in the notification file?



- Until total size of deltas  $<$  snapshot size
  - deltas for ~17 hours back
  - notification.xml ~ 20KB
- For some time (8 hours)
  - notification.xml ~ 11KB

# How many deltas to list in the notification file?



- Until total size of deltas  $<$  snapshot size
  - deltas for  $\sim 17$  hours back
  - notification.xml  $\sim 20$ KB
- For some time (8 hours)
  - notification.xml  $\sim 11$ KB
- Not more than  $X$  deltas (or notification file size  $<$   $Y$  bytes)

# For how long to provide not referenced files?



- RP downloaded notification file, learned URL to the snapshot
- RP started downloading snapshot
- RRDP server generated new snapshot and published new notification file

# For how long to provide not referenced files?



- RP downloaded notification file, learned URL to the snapshot
- RP started downloading snapshot
- RRDP server generated new snapshot and published new notification file
- When to remove the old snapshot and delta files?

# For how long to provide not referenced files?



- RP downloaded notification file, learned URL to the snapshot
- RP started downloading snapshot
- RRDP server generated new snapshot and published new notification file
- When to remove the old snapshot and delta files?
- Currently 1 hour:
  - 7 snapshots – 198MB
  - whole RRDP repository – 228MB



# Useful vs. not-so-much-useful data



- Every CA updates it's .mft and .crl every X hours

# Useful vs. not-so-much-useful data



- Every CA updates it's .mft and .crl every X hours
- Take all deltas (18 hours, 30 MB) and compare how many .cer, .roa, .mft, and .crl files are in there

# Useful vs. not-so-much-useful data



- Every CA updates it's .mft and .crl every X hours
- Take all deltas (18 hours, 30 MB) and compare how many .cer, .roa, .mft, and .crl files are in there

.mft	7715
.crl	7713
.roa	4
.cer	0

# Useful vs. not-so-much-useful data



- Every CA updates it's .mft and .crl every X hours
- Take all deltas (18 hours, 30 MB) and compare how many .cer, .roa, .mft, and .crl files are in there

.mft	7715	10215
.crl	7713	10209
.roa	4	11
.cer	0	6

# Useful vs. not-so-much-useful data



- Every CA updates it's .mft and .crl every X hours
- Take all deltas (18 hours, 30 MB) and compare how many .cer, .roa, .mft, and .crl files are in there

.mft	7715	10215
.crl	7713	10209
.roa	4	11
.cer	0	6

- 43 MB per day per RP

# Useful vs. not-so-much-useful data



- Every CA updates it's .mft and .crl every X hours
- Take all deltas (18 hours, 30 MB) and compare how many .cer, .roa, .mft, and .crl files are in there

.mft	7715	10215
.crl	7713	10209
.roa	4	11
.cer	0	6

- 43 MB per day per RP
- Maybe we should do that differently?



# Questions



[github.com/RIPE-NCC/rpki-publication-server](https://github.com/RIPE-NCC/rpki-publication-server)  
[github.com/RIPE-NCC/rpki-validator](https://github.com/RIPE-NCC/rpki-validator)