



RIPE NCC
RIPE NETWORK COORDINATION CENTER

Hosted or Delegated RPKI?

It depends... and what about
publication?



“Hosted” RPKI



Good Fit for Most

The screenshot shows the RPKI dashboard interface. The main content area displays 'BGP Announcements and ROAs' for the network 'Reseaux IP Europeens Network Cc rLripeccc-ts'. It shows 2 BGP Announcements, 2 ROAs, and 0 Pending Changes. A table lists the ROAs:

Origin AS	Prefix	Max Length	Affected Announcements	Last Updated (UTC)	
<input type="checkbox"/> AS2121	193.0.24.0/21	21	0	12/30/2024, 16:35:27	Edit Delete
<input type="checkbox"/> AS2121	2001:67c:64::/48	48	0	8/12/2024, 10:12:22	Edit Delete

At the bottom of the table, it shows 'Rows per page: 25' and '1-2 of 2'.

- RPKI CA hosted by RIPE NCC
- Monitored 24/7
- Highly Redundant
- SOC2 type 1 Assurance Report

- You just configure:
 - ROAs
 - Alerts
 - Other RPKI objects in future: ASPA, BGPsec, RSC

Hosted RPKI - Review Effect



The screenshot shows the RPKI dashboard interface. A modal window titled "Review and Apply" is open, displaying the following data:

Staged ROAs

Origin AS	Prefix	Max Length
AS2121	193.0.24.0/21	21

Affected Announcements

Origin AS	Prefix	Current Status	Future Status
AS2121	193.0.24.0/21	<input checked="" type="checkbox"/> Valid	→ Unknown

At the bottom of the modal, there are two buttons: "Apply now" and "Add to pending changes".

<https://dashboard.rpki.ripe.net/>

Hosted RPKI - Dashboard Availability



CORE Primary

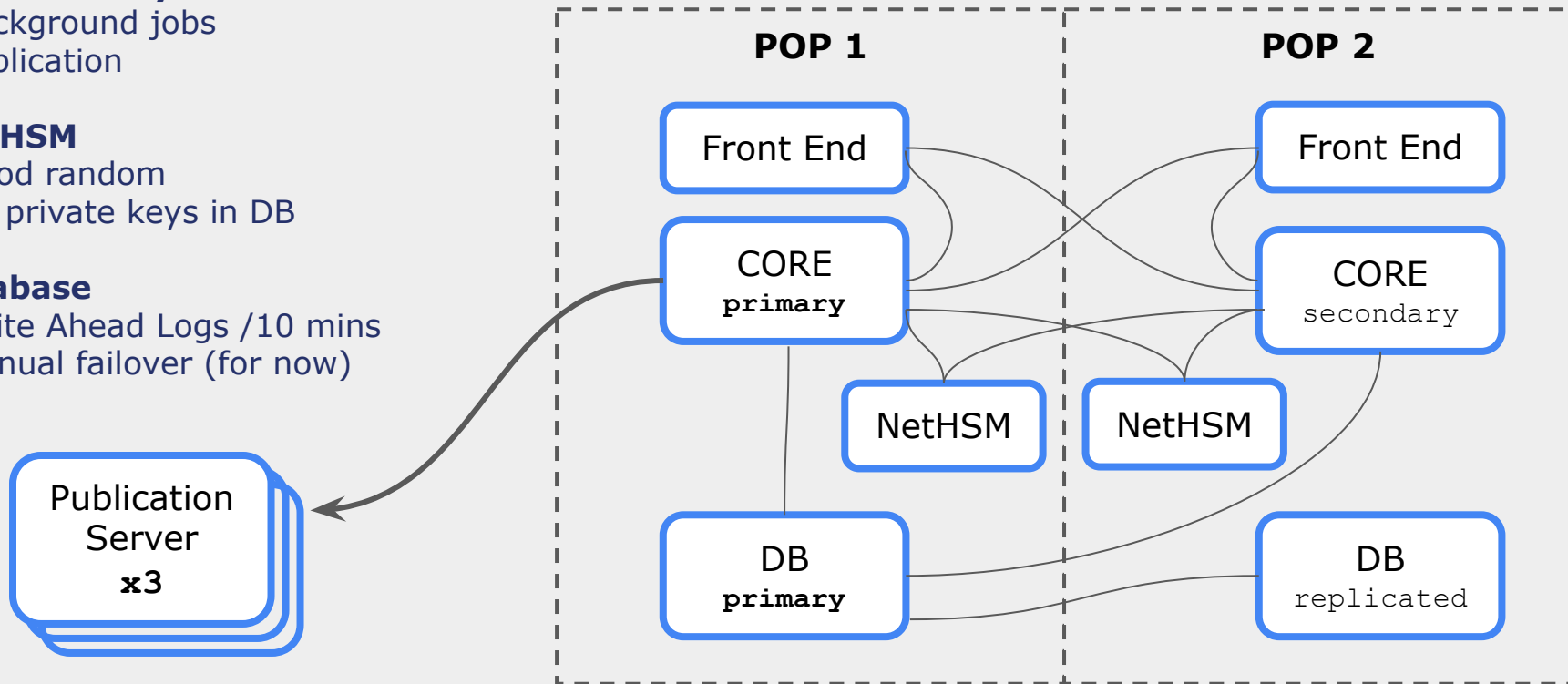
- Background jobs
- Publication

Net HSM

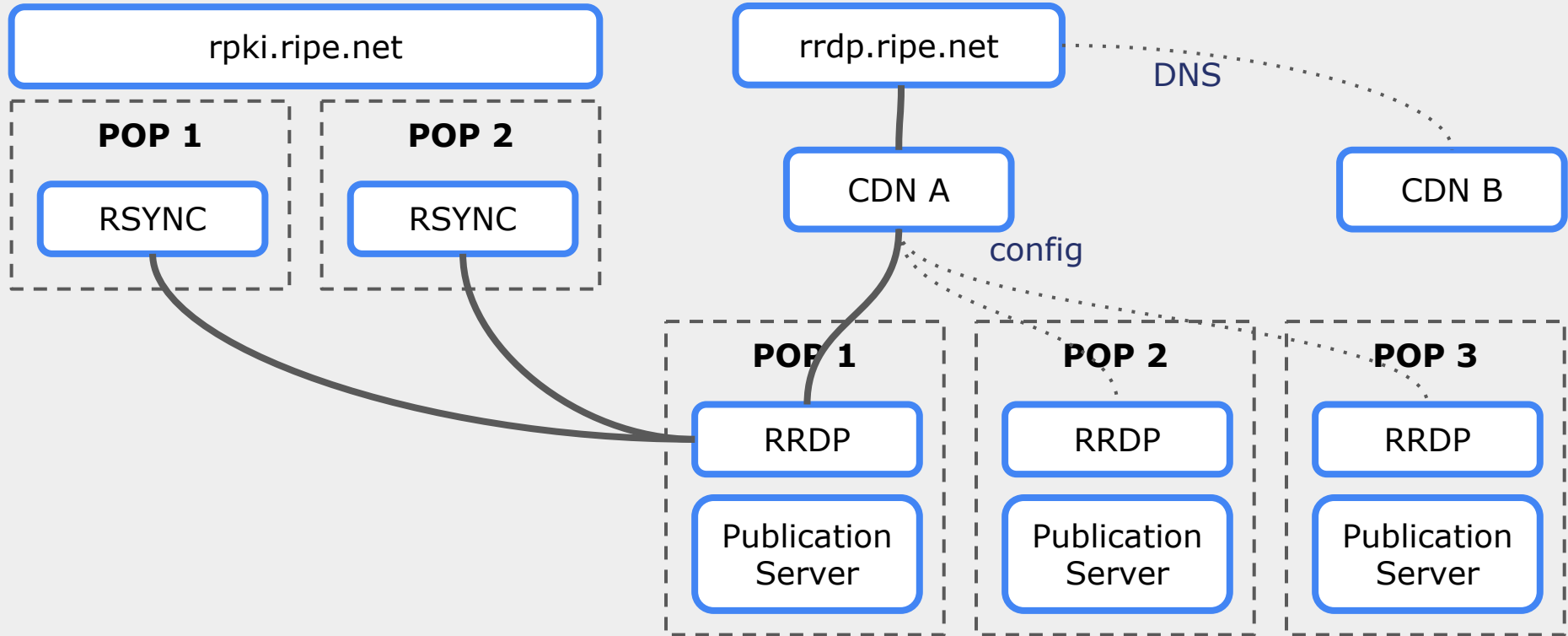
- Good random
- No private keys in DB

Database

- Write Ahead Logs /10 mins
- Manual failover (for now)



Hosted RPKI - Repository Availability

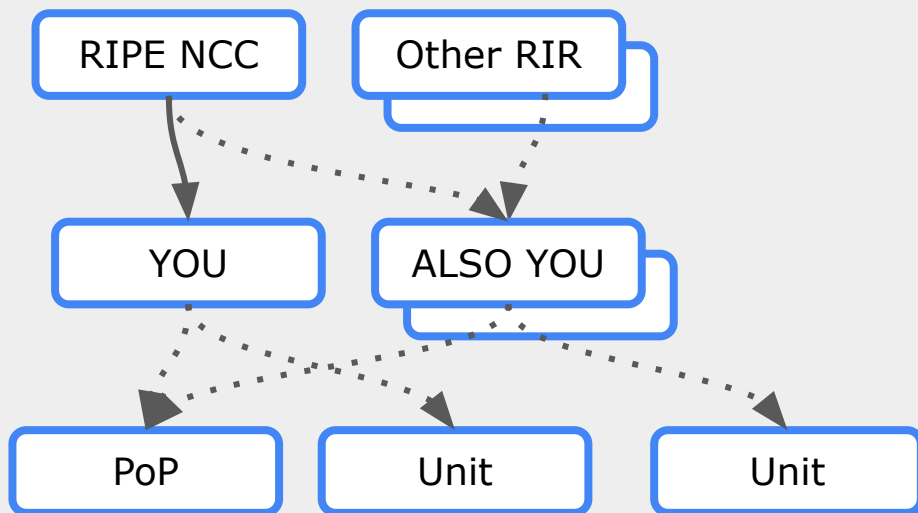




“Delegated” RPKI



For You? Maybe...



- One Tool / API for
 - Multiple Parents
 - Multiple LIRs
 - Multiple PI / Legacy “End-Users”
- Delegations
 - Partition ROA Management
- ASPA or BGPsec today
- Local Access Control
(but add/remove in RIPE NCC dashboard)



Options

- [NLnet Labs Krill](#)
 - Transparency: yours truly worked on this for 5 years
 - Used by several NIRs and many organisations
 - Rust based
 - Actively maintained
- [Dragon Research Labs RPKI Toolkit](#)
 - Used by several NIRs
 - Python2 code
 - New features uncertain
- No other options at this time, unfortunately



Create Delegated CA

Revoke Hosted CA

Important

Once your hosted CA (Certificate Authority) is revoked, it cannot be restored, and all of your ROAs will be deleted. Please note that you can create a new CA later, and you will need to use this option if you intend to switch from a Hosted to a Delegated CA.

Please Confirm

- I want to revoke the hosted CA. I understand that I need to initialise a new CA to keep using RPKI.
- I am aware that my ROAs are going to be deleted.
- I am aware that alerts for conflicting announcements will no longer be sent.

nLripec-1s

REVOKE

Revoke

1: Revoke Hosted CA

Create Certification Authority

Romeo Indira Echo November
rlripec-1s

Hosted

Select this option if you want the RIPE NCC to host your Certification Authority (CA) and publish your ROAs and other RPKI signed objects. You will only need to maintain your ROAs in our dashboard. We recommend this option if you do not want to run RPKI CA software.

Delegated

Select this option to run your own Certification Authority (CA) software. This may be useful if you wish to keep full control over your private key or want to delegate resources to child CAs, e.g. to allow different units in your organisation to manage ROAs for specific resources only. If you choose this option, we recommend you use the Publication Server provided by the RIPE NCC.

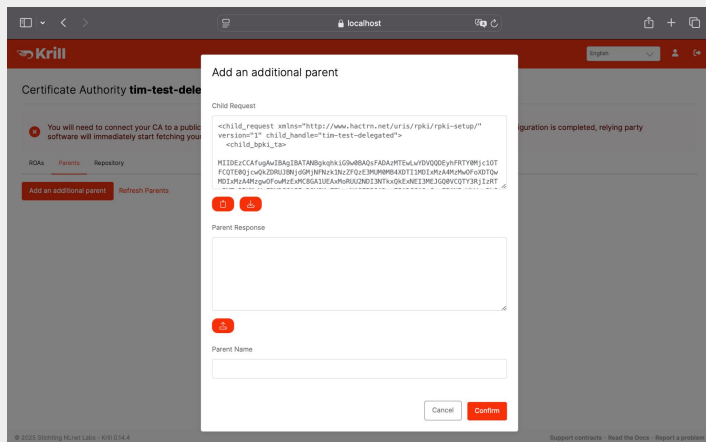
I have read and agreed to the [RIPE NCC Certification Service Terms and Conditions](#)

Create Certification Authority

2: Create Delegated CA

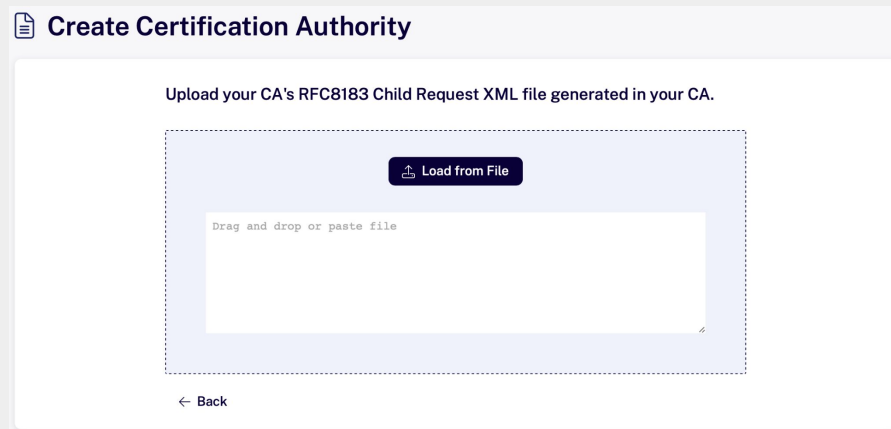
⚠ Existing ROAs removed, announcements become ROV not-found

Introduce Child to Parent



Get RF8183 Child Request XML

Create Certification Authority



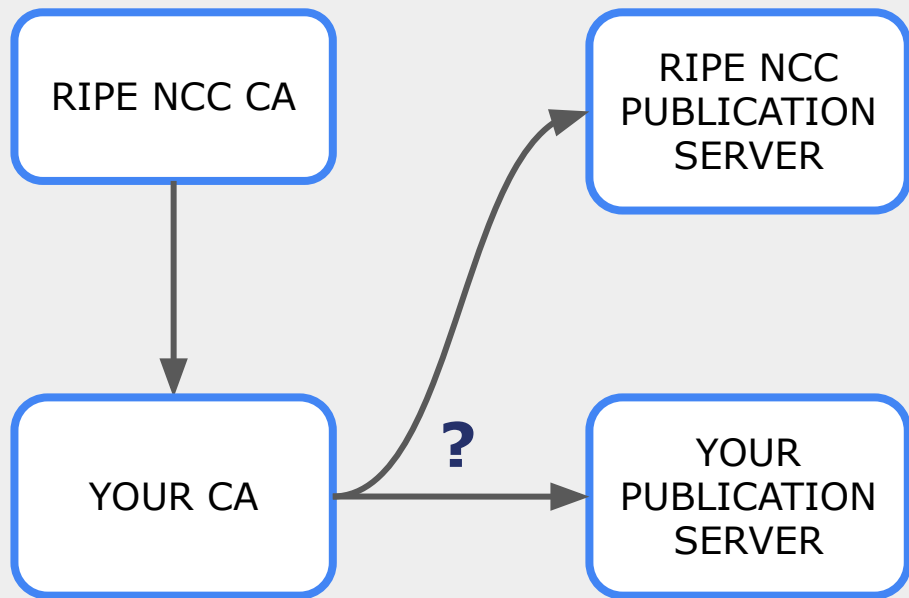
Upload it to create your Delegated "child" CA under the RIPE NCC "parent"



Hey wait!
What about publication?



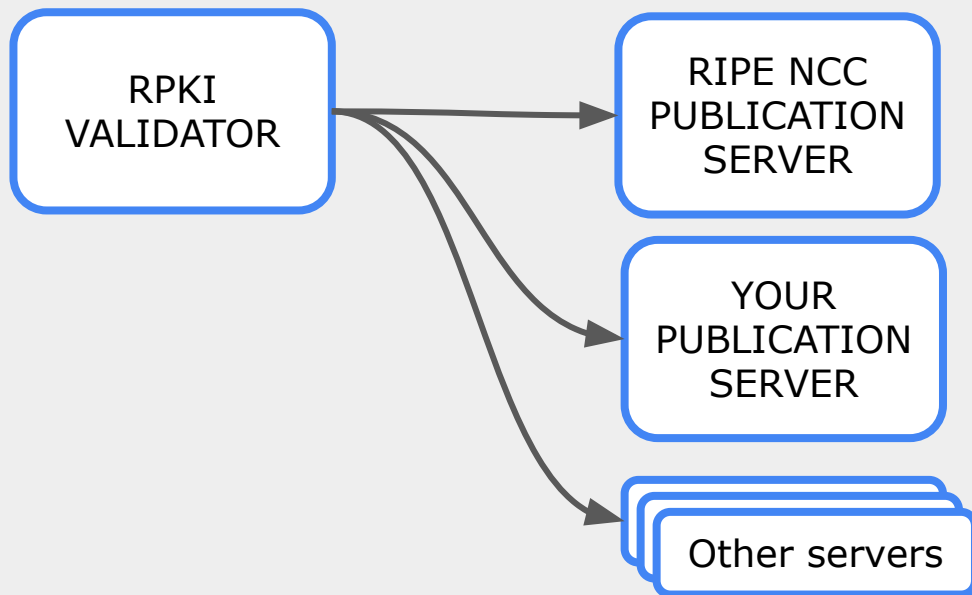
Host Your Own?



- RIPE NCC “Publication as a Service”
 - Up to 10 CAs / member (talk to us if you need more)
 - You sign
 - RIPE NCC publishes and monitors
 - RIPE NCC uses CDN
- Your own server
 - RRDP 24/7 availability
 - RRDP file timing
 - rsync 24/7
 - rsync consistent view / connection
 - And more... (see [BCP](#))



Won't Somebody Please Think of the Validators??

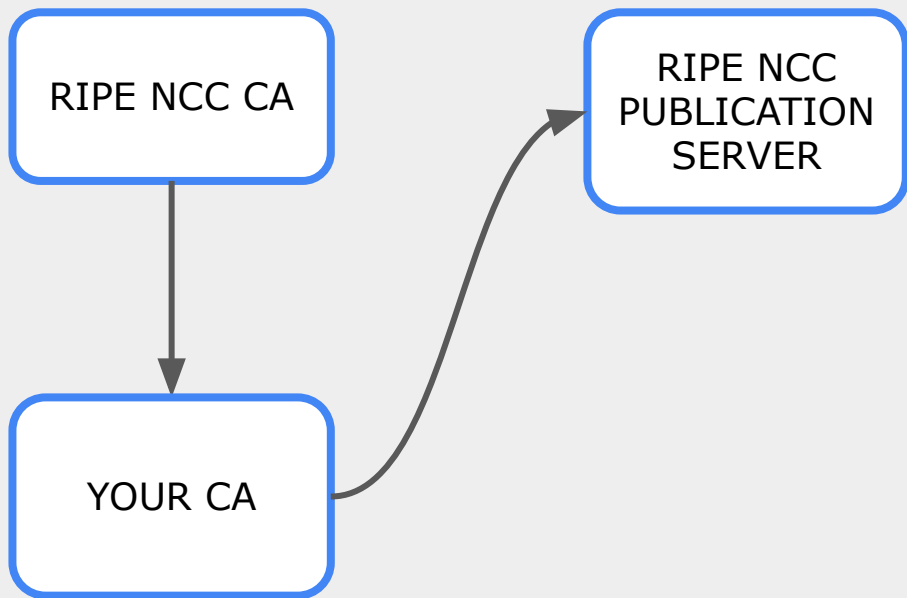


- Validator Issues With Repositories:
 - Many repos, but [decreasing](#)
 - Slow
 - Unavailable
 - Keep State
 - Noisy logs
 - Delayed propagation

Publication as a Service is preferred



“Hybrid” / Publish at Parent / Publication as a Service



- No need for 24/7 repo management
- Short CA downtime okay..
 - Your ROAs, Manifest and CRL are still valid
 - Child CAs can reconnect later
- Be nice to RPKI Validators!
- Used by 2500+ member of nic.br

See:


<https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/paas-onboarding-with-krill/>



Set Up Publication as a Service

Publication as a Service

+ Add publisher

If you use a delegated CA you may want to use the [Publication as a Service](#)  provided by the RIPE NCC, saving you the burden of maintaining a 24/7 RPKI repository. Please note that if you use your delegated CA to delegate to your own child CAs (e.g. to delegate the use of resources to departments in your organisation), you can configure multiple publishers.

- Similar exchange of (RFC8183 format) XML files
- Up to 10 Publishers can be added (i.e. for you delegated CAs)
- Allows files under non-RIPE-NCC parents, for your RPKI files issued under a certificate received from another RIR



Before you start...

Be prepared to take care of your CA!



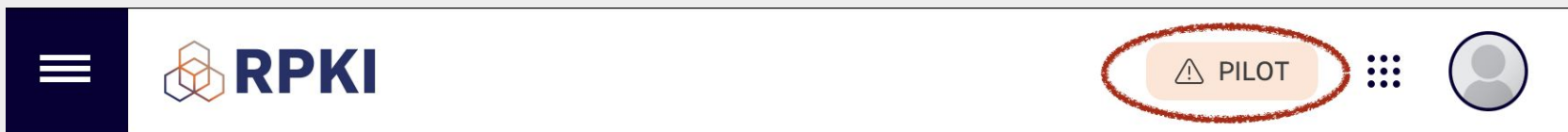
Non-functional CAs affect RPKI Validators

- Proposal:
 - “Automatic Revocation of Persistently Non-functional Delegated RPKI CAs”
- Discussion started on the [Routing Working Group mailing list](#)
- Criteria to be discussed:
 - Revoke after 100 days of invalidity?
 - Should the RIPE NCC send warnings sooner?
 - Publication as a Service for functional CAs with dysfunctional repositories?

Testing?



- [RIPE NCC RPKI Pilot Environment](#)
 - Your own LIR and resources
 - Under test Trust Anchor
 - No support for Publication as a Service (yet)



- [NLnet Labs Krill Testbed](#)
 - Test with any resources
 - Under test Trust Anchor
 - Supports Publication as a Service

Things you may want?



- Delegated CAs as children of your Hosted CA?
- Hosted CAs as children of your Hosted CA?
- Concurrent Hosted and Delegated CA?
 - To support migration without ROA downtime
- More than 10 publishers needed?
- Anything else?



- Hosted CA is the right choice for most users:
 - Fully managed
 - Just configure your ROAs and go
- Delegated CA has use cases for some:
 - Multiple parent RIRs
 - Multiple LIRs
 - Further delegations
- Delegated CA publication:
 - Make sure the repository is available 24/7 (not trivial)
 - Or consider using Publication as a Service from your RIR/NIR



Questions & Comments



tbruijnzeels@ripe.net