Gott ist tot
George and I are Friends
Well, maybe more like brothers; we fight

But we, not our masters, are responsible for our actions
RPKI Publication, What are the Actual Problems?

IEPG / Montréal
2018.07.15
Don’t Panic

• I am an Engineer, we always think about the problems
• I am also a Researcher, we are only interested in the problems
• The RPKI is going fairly well
• But I want to talk about the problems
• Some of these data are old
Routing Relies on It!

• If my routing relies on the RPKI, then I care a lot about publication reliability
• Of course, good relying party software will expect failures, so this is not a killer
• But when we look at current publication, much is not operational quality
• This has to be fixed
What Matters

• What matters is what the normal customer sees when they install RP software and just run it.

• Do not tell them to tune it. What do you not understand about ‘normal user?’
### Configured Trust Anchors

<table>
<thead>
<tr>
<th>Enabled</th>
<th>Trust anchor</th>
<th>Processed Items</th>
<th>Expires in</th>
<th>Last updated</th>
<th>Next update in</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>APNIC RPKI Root</td>
<td>4699 0 2</td>
<td>2 years and 6 months</td>
<td>3 minutes ago</td>
<td>Updating ROAs</td>
</tr>
<tr>
<td>✓</td>
<td>ARIN</td>
<td>1754 0 0</td>
<td>9 years and 2 months</td>
<td>5 minutes ago</td>
<td>5 minutes</td>
</tr>
<tr>
<td>✓</td>
<td>AfriNIC RPKI Root</td>
<td>465 0 0</td>
<td>9 years and 2 months</td>
<td>5 minutes ago</td>
<td>5 minutes</td>
</tr>
<tr>
<td>✓</td>
<td>LACNIC RPKI Root</td>
<td>4333 0 0</td>
<td>94 years and 3 months</td>
<td>6 minutes ago</td>
<td>4 minutes</td>
</tr>
<tr>
<td>✓</td>
<td>RIPE NCC RPKI Root</td>
<td>22793 0 0</td>
<td>99 years and 4 months</td>
<td>10 minutes ago</td>
<td>31 seconds</td>
</tr>
<tr>
<td>✓</td>
<td>altCA</td>
<td>38 0 0</td>
<td>9 months and 3 weeks</td>
<td>4 minutes ago</td>
<td>6 minutes</td>
</tr>
</tbody>
</table>

[RIPE NCC](https://ripe.net)  

Copyright ©2009-2018 the Réseaux IP Européens Network Coordination Centre RIPE NCC. All rights reserved. Version 2.24
Same for Dragon Research RP
Except Eye Candy Has Less Sugar
And there is NO RPKI Trust Anchor Roll Protocol

Oops!
Certification Problems

For a few hours this weekend, everything certified below your RPKI working CA went missing, because the EE certificate in your working CA's manifest expired, thus the signature on the manifest was invalid, thus the working CA had no verifiable children.
Three of the five RIRs have now been through a cycle of having some accident take their CA offline for a few days (weekend or on that order), only to discover that the manifest EE certificate lifetimes they were using was not long enough to survive the CA outage. This is not about stale manifests (thisUpdate/nextUpdate), it's about manifest EE certificates expiring (EE certificate notAfter).
For years now I've been trying to get the attention of the RIRs on this issue, but their implementers keep telling me that they believe that having a relatively short manifest EE certificate lifetime is important to protect them from something, not really clear what when I press them on this point, but they don't want to change it. Last time I checked, the combination of the three outages mentioned above and my whining has gotten them to push back to perhaps one week for the manifest lifetime, which means that they can now survive having their CA down for a week.
Following Graphs are from DRL's Relying Party Software Web Page

Many are old
Not Bad

An ISP

pubd-pilot.lab.dtag.de last week

Sync time (seconds)

Objects (Count)

Average sync time (seconds): 3.14
Average connection count: 1.00
Average object count: 3.00

An RIR

repository.lacnic.net last week

Sync time (seconds)

Objects (Count)

Average sync time (seconds): 945.96
Average connection count: 63.62
Average object count: 234.00

Creative Commons: Attribution & Share Alike
They do not monitor and have no real NOC
They do not work weekends
I had to write a friend in the RIR’s Engineering
An RIR, OK but Ugly
Something Rotten in AMS
Cause

• This was an NFS problem (NFS is Evil!)
• It went on for months
• DRL logs had full detail showing “NFS”
• But “Nothing Can Be Wrong at the RIR”
• Many weeks later it was fixed, but small problems remained as they kept using NFS
Just Weird

And we wrote to them multiple times and received only snarky responses
RFC 7115 Sec 3

The RPKI repository design [RFC6481] anticipated a hierarchic organization of repositories, as this seriously improves the performance of relying parties gathering data over a non-hierarchic organization. Publishing parties MUST implement hierarchic directory structures.
Fetch Time

OOPS!
RIPE & APNIC Very Slow
Deliberately Bad Directory Structure
Violates RFC
RIPE Fixed Theirs

Change from Flat to Hierarchic Publication

Key Roll
APNIC still has not. Is still not hierarchic per 7115
Conservative Software Saves Us

• Of course, good relying party software will expect failures, so this is not a killer
• DRL relying party software uses old data if it can not fetch new
• As RPKI data are fairly stable, this is OK
• But one RIR had an in-addr disaster which lasted five days!
But we have had no major RPKI disasters recently
So We Have to Make Some
Lame Delegation

- APNIC is Publishing a Child Repo which is Unreachable
- It is CNNIC
- Think Great Firewall
- APNIC & CNNIC are working on this issue
- But been going on for many months
- This is the same as DNS Lame Delegation
DNS Root Change

- DNS Root Servers occasionally change IP address
- Multiple notices go out to the world
- 82.378% of relying parties ignore it
- The long tail of access to the old address goes for many years
- But the DNS protocol is designed for this; no one notices, and it all works
RPKI Trust Anchor Change

• An RIR wants to change their RPKI trust anchor; and they have done this a lot
• The RIR sends out an email or six
• Most relying parties do not see or understand it
• The protocol was NOT designed for this
• Things break; the RIRs blame the user
Now let's deploy a major change to the core of crypto validation!
Flag Day, Eh?

# zgrep -h rrdp /var/log/apache2/access.log* \  
  | awk '{print $1}' | sort -u | wc -l
319

# zgrep -h rpki /var/log/rsync.log* \  
  | awk '{print $6}' | grep '^[ ]' | sort -u | wc -l
227

It's barely deployed and there are more than 500 out there
It is a Non-Trivial Flag Day and the RIRs Have Not Written the Transition RFC!
If the IANA was the single point of trust, as was expected, at least they seem to know how to deal with rolls
The RIRs are Not Network Operators

They’re PTTs, “There can be no problem”
Conclusions

• RPKI protocols do not have the resilience of the DNS. Oops! Our bad.
• RIRs have publication problems repeatedly
• Validation Reconsidered solves a ‘problem’ that RIRs are not actually having
• And it will make things less predictable and understood
• And it’s a flag day which many users are not actually going to follow
We Will Learn to Love Validation Reconsidered
Stickers I Had Made 15 Years Ago

Don't make me come down there
-- God