Gott ist tot

George and I are Friends

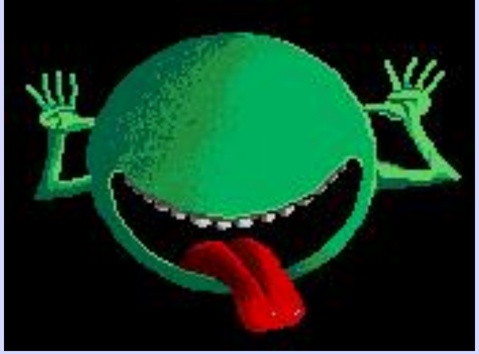
Well, maybe more like brothers; we fight

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!

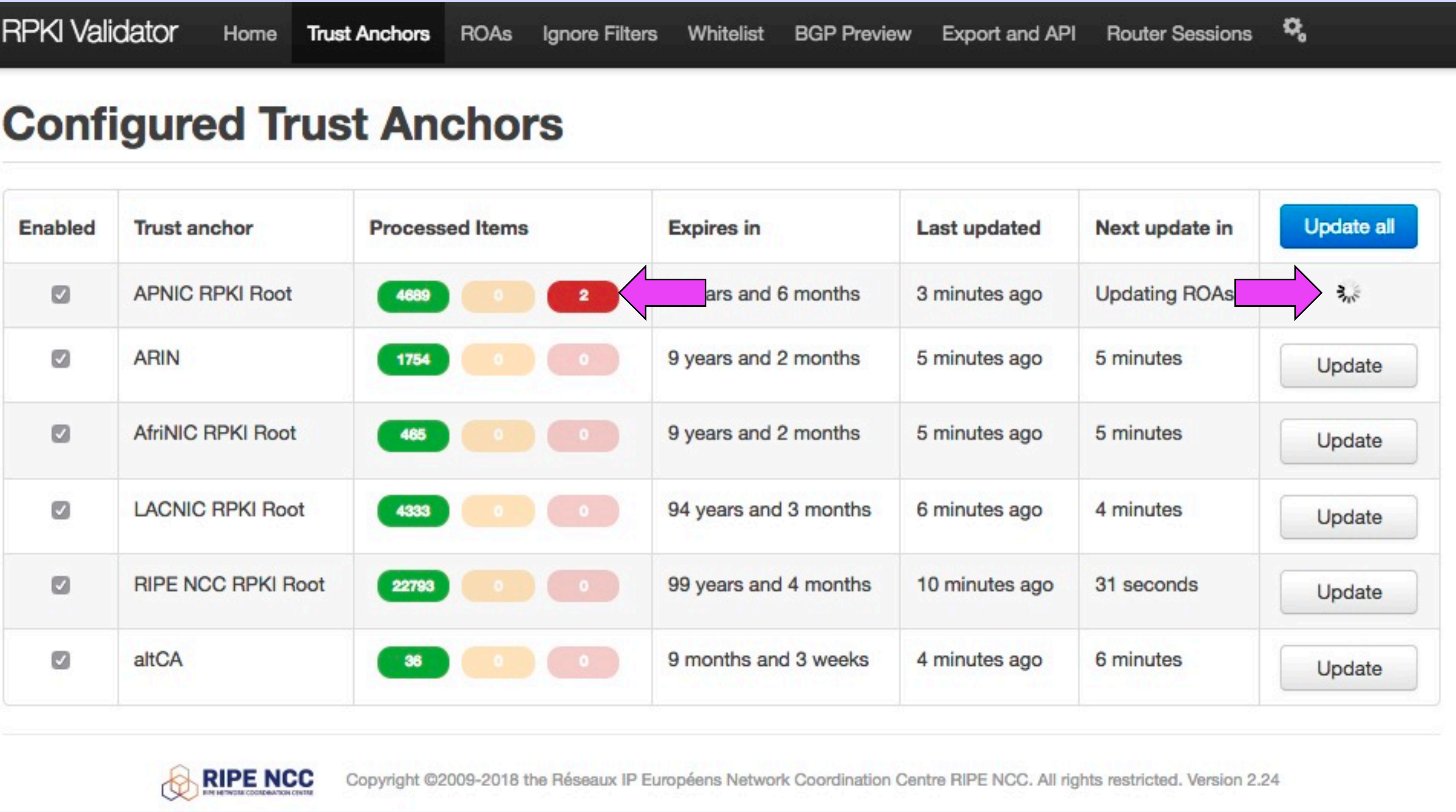
- If my routing relies on the RPKI, then I care a lot about publication reliability
- Of course, good relying party software will expect failures, so this is not a killer
- But when we look at current publication, much is not operational quality
- This has to be fixed

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?'

SW Installed as Shipped



Configured Trust Anchors

Enabled	Trust anchor	Processed Items	Expires in	Last updated	Next update in	Update all
☑	APNIC RPKI Root	4689 0 2	ars and 6 months	3 minutes ago	Updating ROAs	
☑	ARIN	1754 0 0	9 years and 2 months	5 minutes ago	5 minutes	Update
☑	AfriNIC RPKI Root	465 0 0	9 years and 2 months	5 minutes ago	5 minutes	Update
☑	LACNIC RPKI Root	4333 0 0	94 years and 3 months	6 minutes ago	4 minutes	Update
☑	RIPE NCC RPKI Root	22793 0 0	99 years and 4 months	10 minutes ago	31 seconds	Update
☑	altCA	36 0 0	9 months and 3 weeks	4 minutes ago	6 minutes	Update

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).

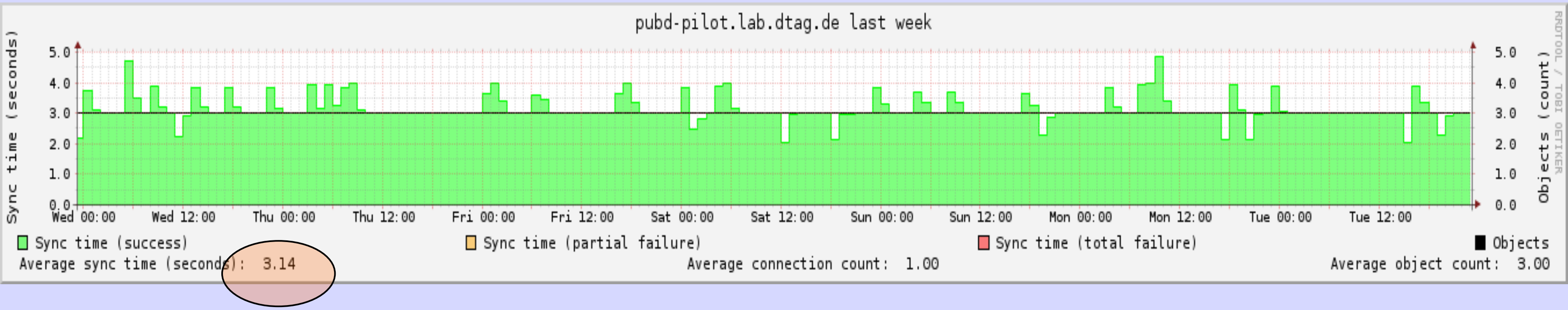
For years now I've been trying to get the attention of the RIRs on this issue, but their implementers keep telling me that they believe that having a relatively short manifest EE certificate lifetime is important to protect them from something, not really clear what when I press them on this point, but 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

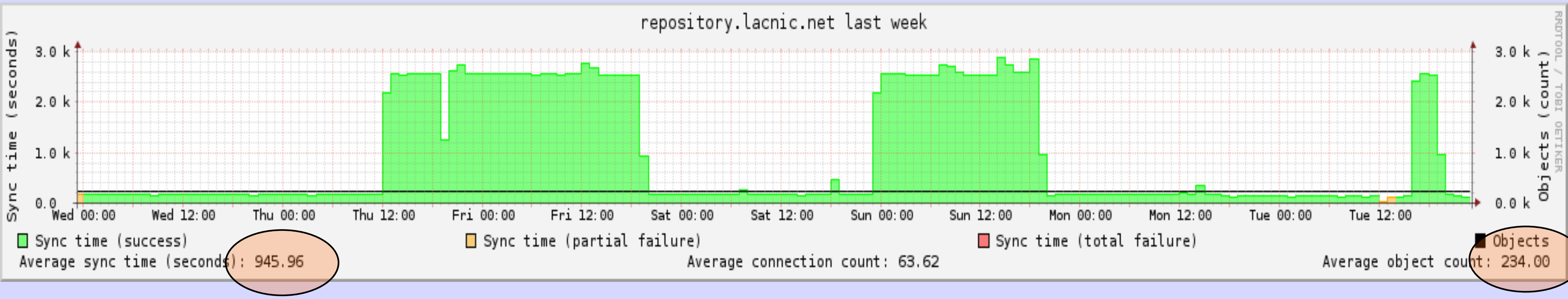
Many are old

Not Bad

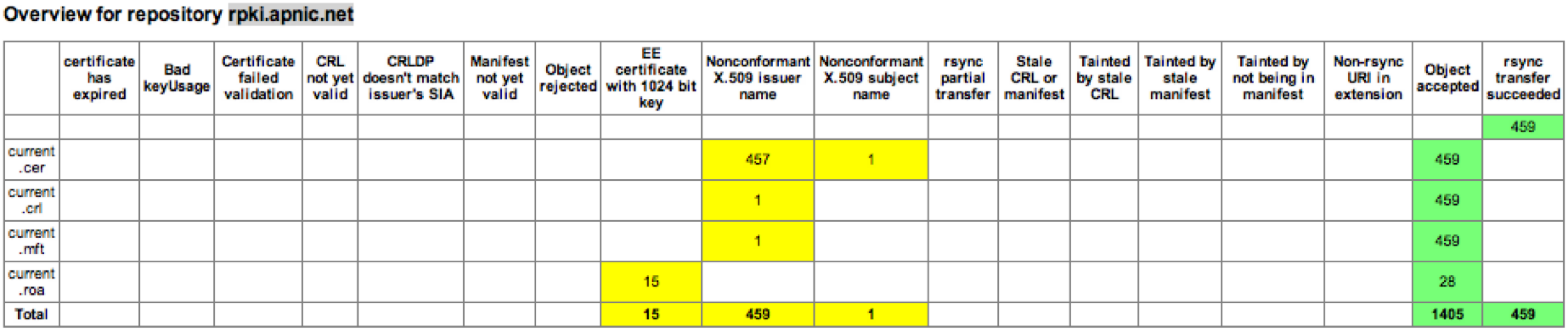
An ISP



An RIR

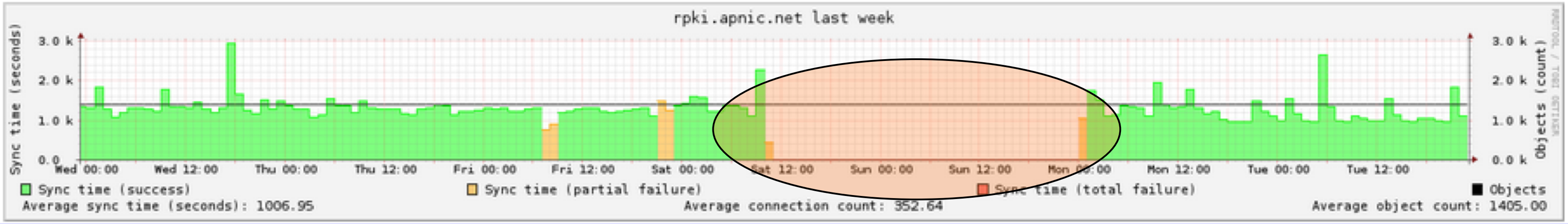


Very Bad



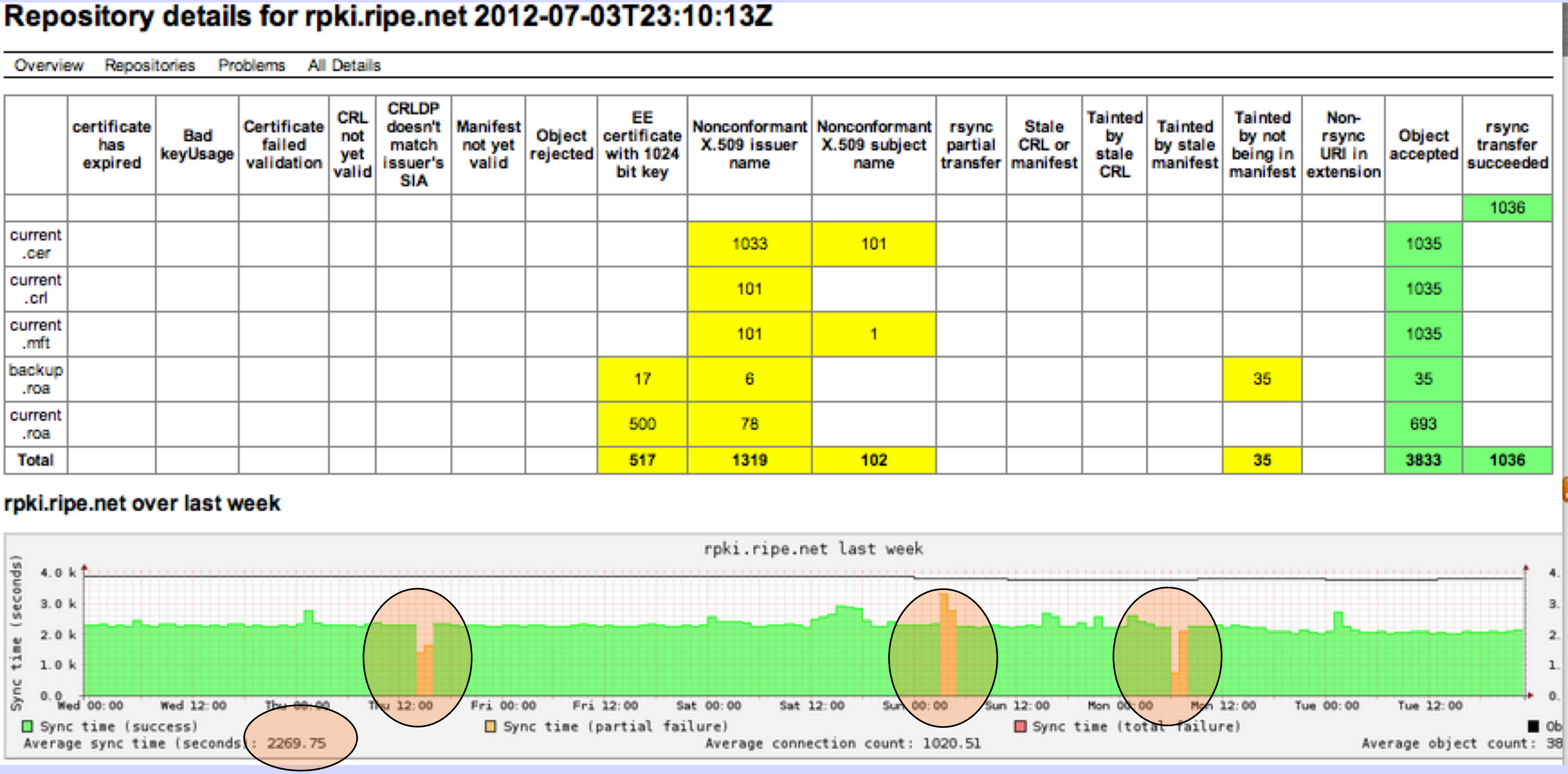
Overview for repository rpki.apnic.net

	certificate has expired	Bad keyUsage	Certificate failed validation	CRL not yet valid	CRLDP doesn't match issuer's SIA	Manifest not yet valid	Object rejected	EE certificate with 1024 bit key	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	rsync partial transfer	Stale CRL or manifest	Tainted by stale CRL	Tainted by stale manifest	Tainted by not being in manifest	Non-rsync URI in extension	Object accepted	rsync transfer succeeded
																		459
current .cer									457	1							459	
current .crl									1								459	
current .mft									1								459	
current .roa								15									28	
Total								**15**	**459**	**1**							**1405**	**459**



- 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



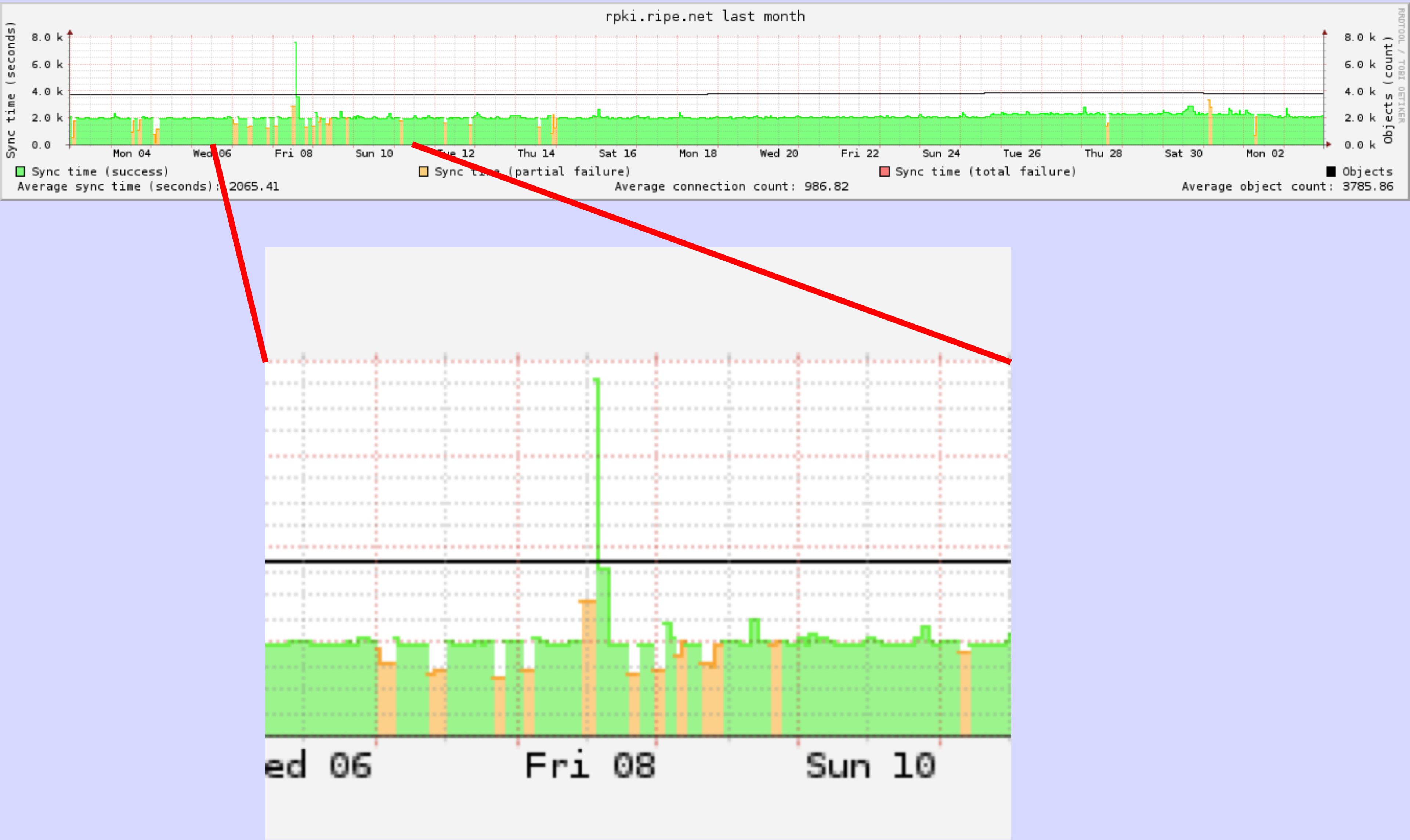
Repository details for rpki.ripe.net 2012-07-03T23:10:13Z

Overview Repositories Problems All Details

	certificate has expired	Bad keyUsage	Certificate failed validation	CRL not yet valid	CRLDP doesn't match issuer's SIA	Manifest not yet valid	Object rejected	EE certificate with 1024 bit key	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	rsync partial transfer	Stale CRL or manifest	Tainted by stale CRL	Tainted by stale manifest	Tainted by not being in manifest	Non-rsync URI in extension	Object accepted	rsync transfer succeeded
																		1036
current .cer									1033	101							1035	
current .crl									101								1035	
current .mft									101	1							1035	
backup .roa								17	6						35		35	
current .roa								500	78								693	
Total								**517**	**1319**	**102**					**35**		**3833**	**1036**

rpki.ripe.net over last week

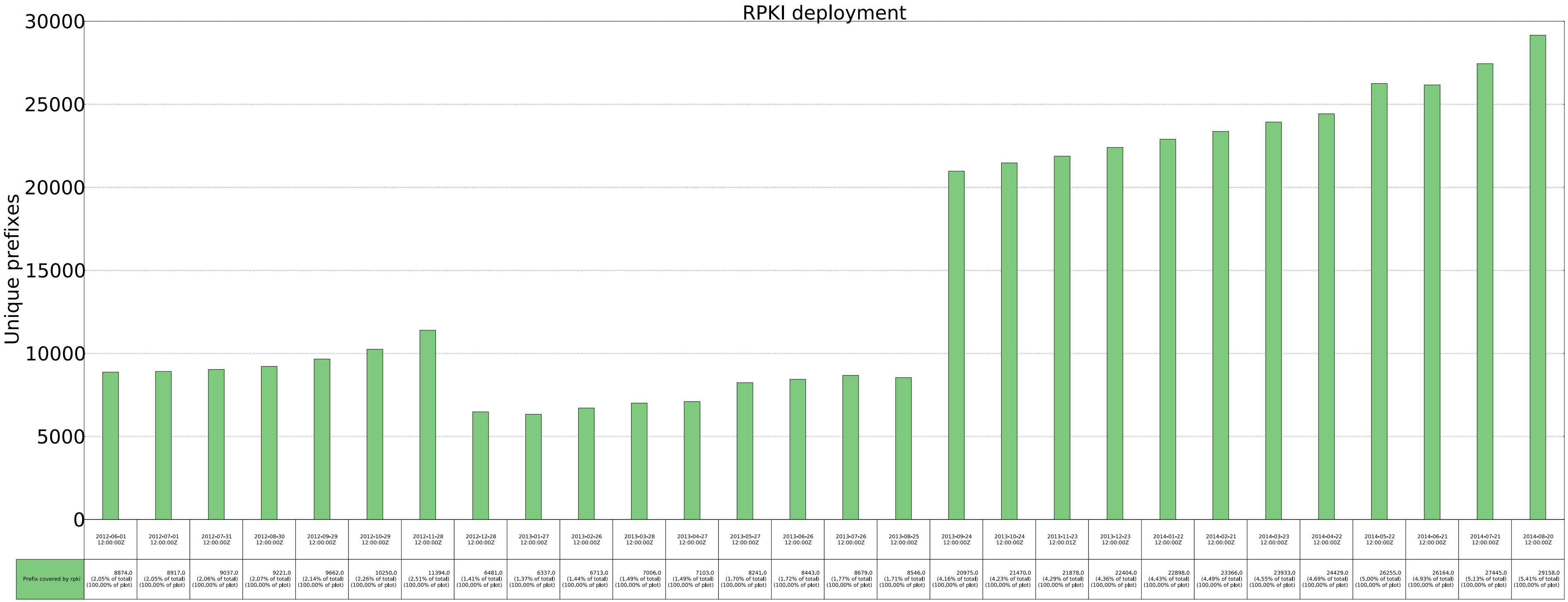
Something Rotten in AMS



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

LACNIC TA Expired



	2012-06-01 12:00:00Z	2012-07-01 12:00:00Z	2012-07-31 12:00:00Z	2012-08-30 12:00:00Z	2012-09-29 12:00:00Z	2012-10-29 12:00:00Z	2012-11-28 12:00:00Z	2012-12-28 12:00:00Z	2013-01-27 12:00:00Z	2013-02-26 12:00:00Z	2013-03-28 12:00:00Z	2013-04-27 12:00:00Z	2013-05-27 12:00:00Z	2013-06-26 12:00:00Z
Prefix covered by rpki	8874.0 (2.05% of total) (100.00% of plot)	8917.0 (2.05% of total) (100.00% of plot)	9037.0 (2.06% of total) (100.00% of plot)	9221.0 (2.07% of total) (100.00% of plot)	9662.0 (2.14% of total) (100.00% of plot)	10250.0 (2.26% of total) (100.00% of plot)	11394.0 (2.51% of total) (100.00% of plot)	6481.0 (1.41% of total) (100.00% of plot)	6337.0 (1.37% of total) (100.00% of plot)	6713.0 (1.44% of total) (100.00% of plot)	7006.0 (1.49% of total) (100.00% of plot)	7103.0 (1.49% of total) (100.00% of plot)	8241.0 (1.70% of total) (100.00% of plot)	8443.0 (1.72% of total) (100.00% of plot)

	2013-07-26 12:00:00Z	2013-08-25 12:00:00Z	2013-09-24 12:00:00Z	2013-10-24 12:00:00Z	2013-11-23 12:00:01Z	2013-12-23 12:00:00Z	2014-01-22 12:00:00Z	2014-02-21 12:00:00Z	2014-03-23 12:00:00Z	2014-04-22 12:00:00Z	2014-05-22 12:00:00Z	2014-06-21 12:00:00Z	2014-07-21 12:00:00Z	2014-08-20 12:00:00Z
Prefix covered by rpki	8679.0 (1.77% of total) (100.00% of plot)	8546.0 (1.71% of total) (100.00% of plot)	20975.0 (4.16% of total) (100.00% of plot)	21470.0 (4.23% of total) (100.00% of plot)	21878.0 (4.29% of total) (100.00% of plot)	22404.0 (4.36% of total) (100.00% of plot)	22898.0 (4.43% of total) (100.00% of plot)	23366.0 (4.49% of total) (100.00% of plot)	23933.0 (4.55% of total) (100.00% of plot)	24429.0 (4.69% of total) (100.00% of plot)	26255.0 (5.00% of total) (100.00% of plot)	26164.0 (4.93% of total) (100.00% of plot)	27445.0 (5.13% of total) (100.00% of plot)	29158.0 (5.41% of total) (100.00% of plot)

Just Weird

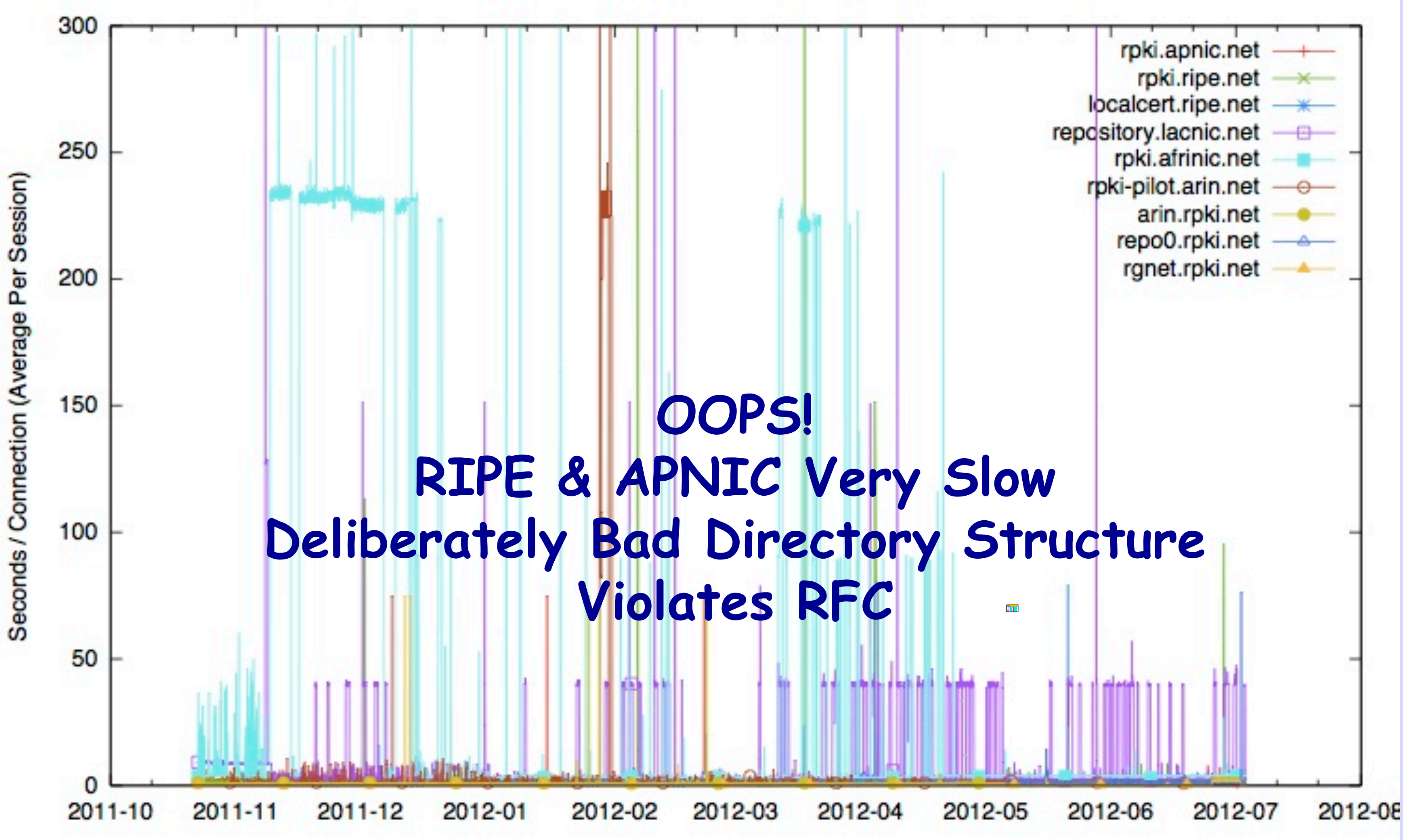
```
871553 -rw-r--r-x  4 rcynic  rcynic  1969 Feb 17 13:26:29
/usr/home/rpki/rcynic/data/authenticated.2012-07-
11T00:00:00Z/rpki.afrinic.net/member_repository/F3634D22/92EF889
0119911E0A59EB577833A7E19/79FBE550468F11E19086CABE31FFE8A0.roa
871602 -rw-r--r-x  4 rcynic  rcynic  2009 Feb 17 13:26:26
/usr/home/rpki/rcynic/data/authenticated.2012-07-
11T00:00:00Z/rpki.afrinic.net/member_repository/F3634D22/92EF889
0119911E0A59EB577833A7E19/82331D8C6C2011E0890EBAC0A0C76497.roa
```

And we wrote to them multiple times and received only snarky responses

RFC 7115 Sec 3

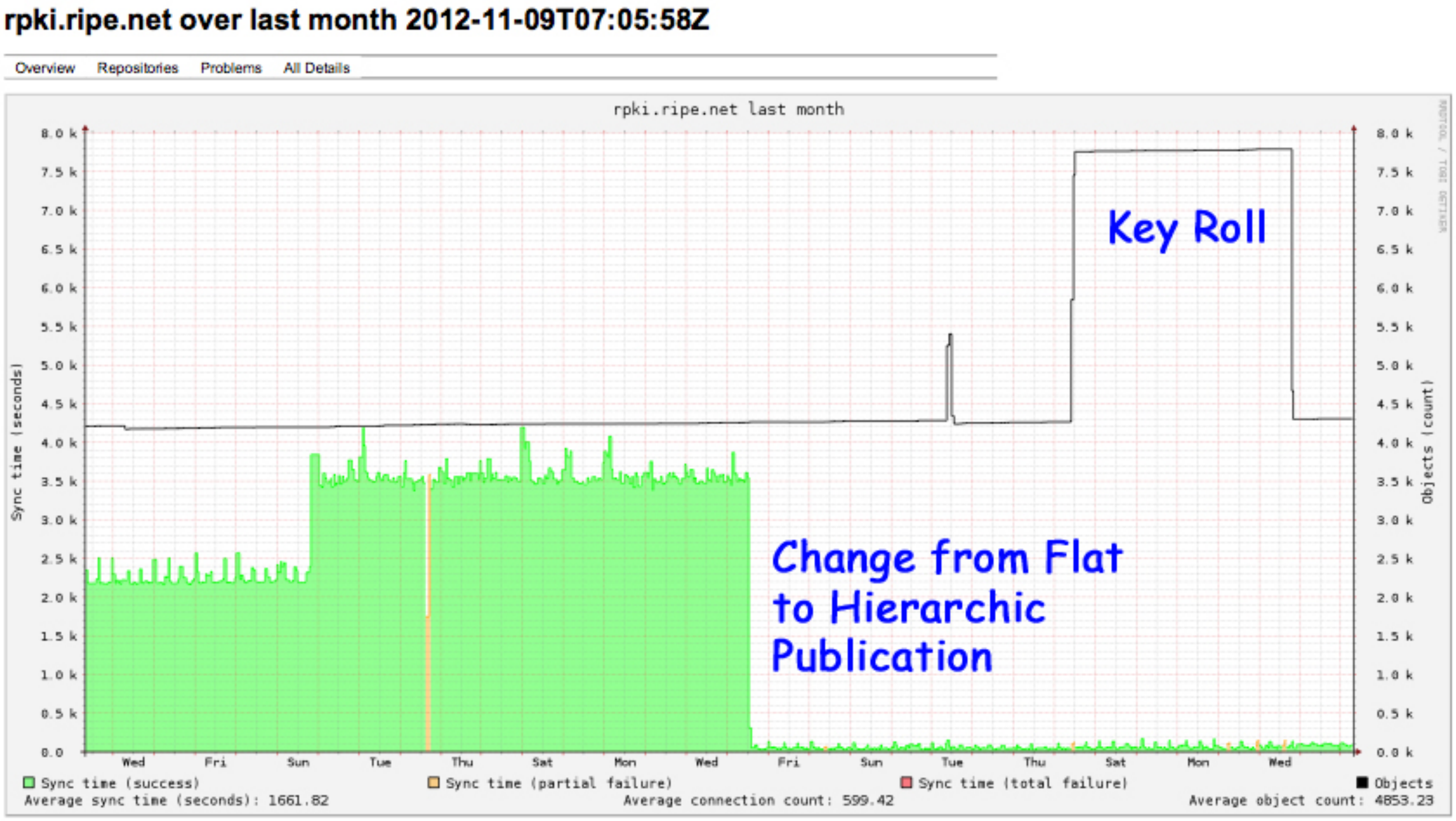
The RPKI repository design [RFC6481] anticipated a hierarchic organization of repositories, as this seriously improves the performance of relying parties gathering data over a non-hierarchic organization. Publishing parties MUST implement hierarchic directory structures.

Fetch Time



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

RIPE Fixed Theirs



rpki.ripe.net over last month 2012-11-09T07:05:58Z

Key Roll

Change from Flat to Hierarchic Publication

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 then 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

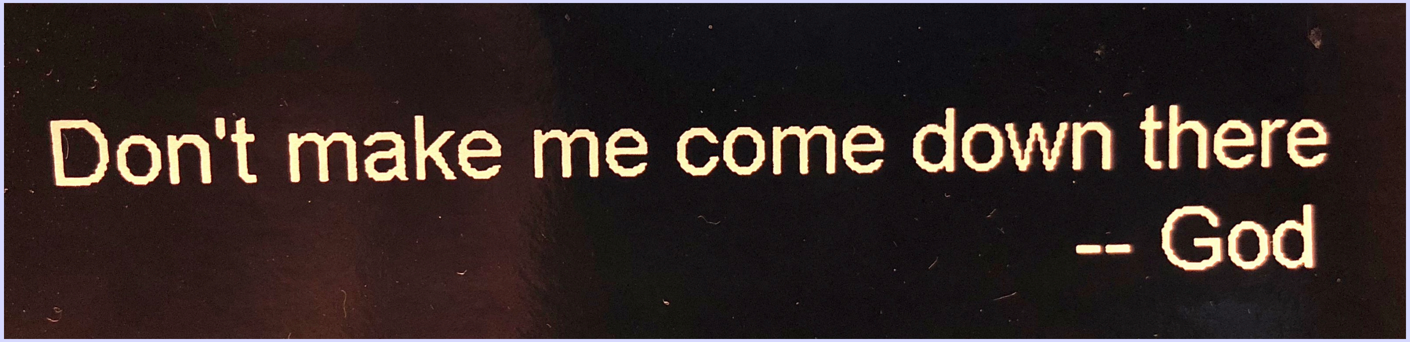
They're PTTs, "There can be no problem"

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