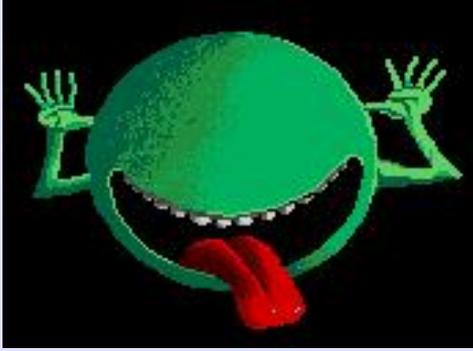


Measuring RPKI Repositories

sidr Interim / Vancouver

2012.07.27

Randy Bush <randy@psg.com>

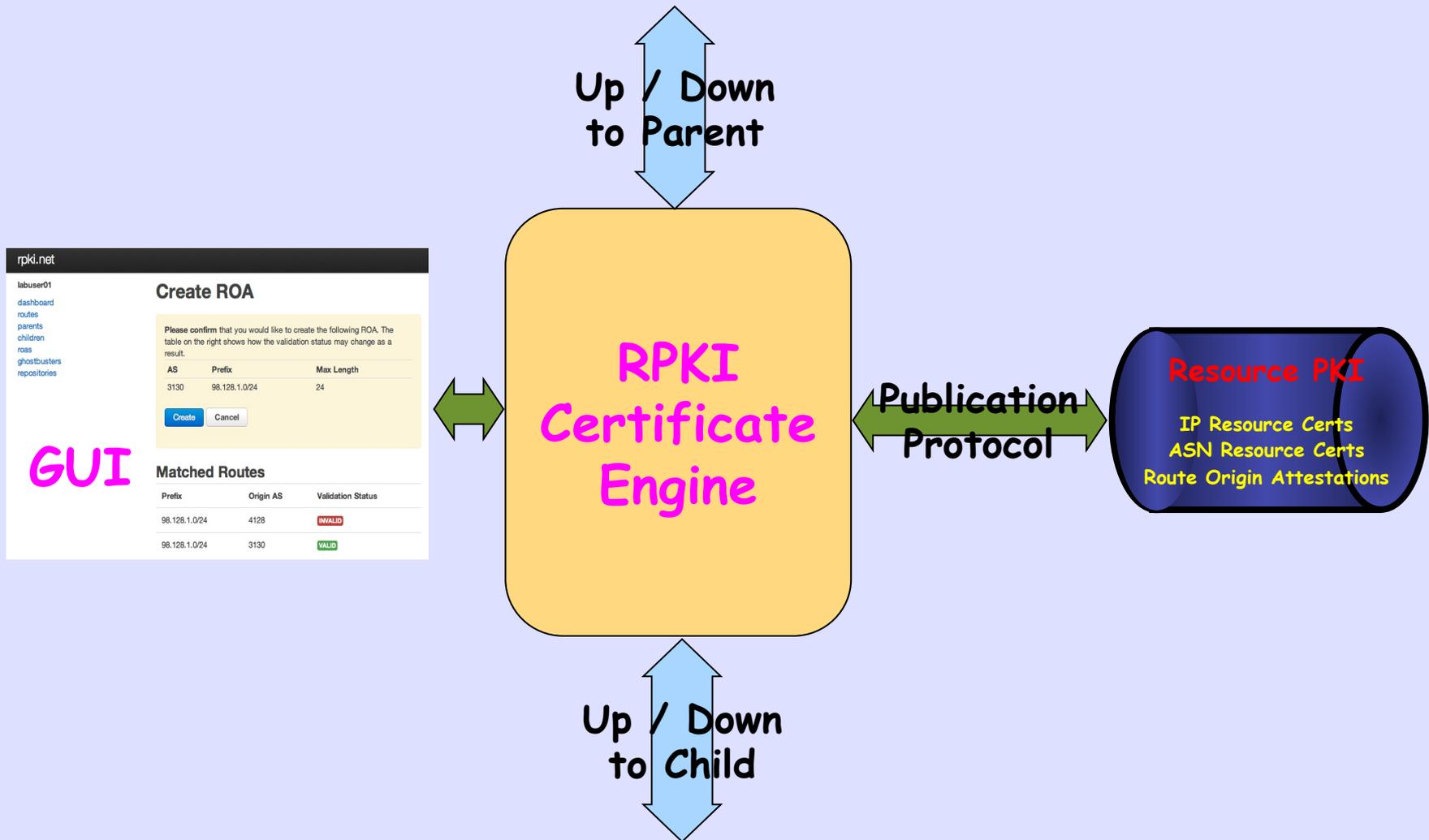


Don't Panic

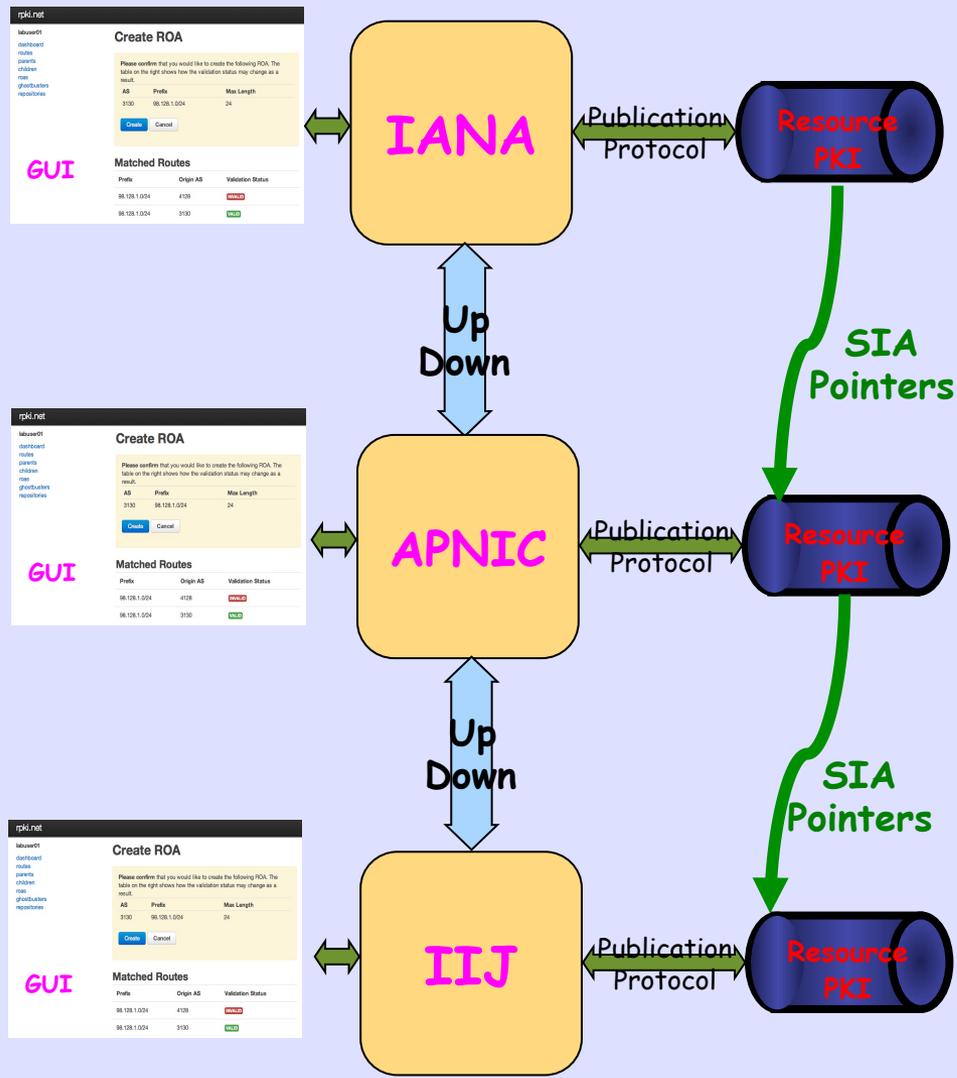
- I am an Engineer, we always think about the problems
- I am a Researcher, we are only interested in the problems
- The RPKI is going really well
- But I want to talk about the problems

Review of RPKI Structure

Publishing / Issuing Party

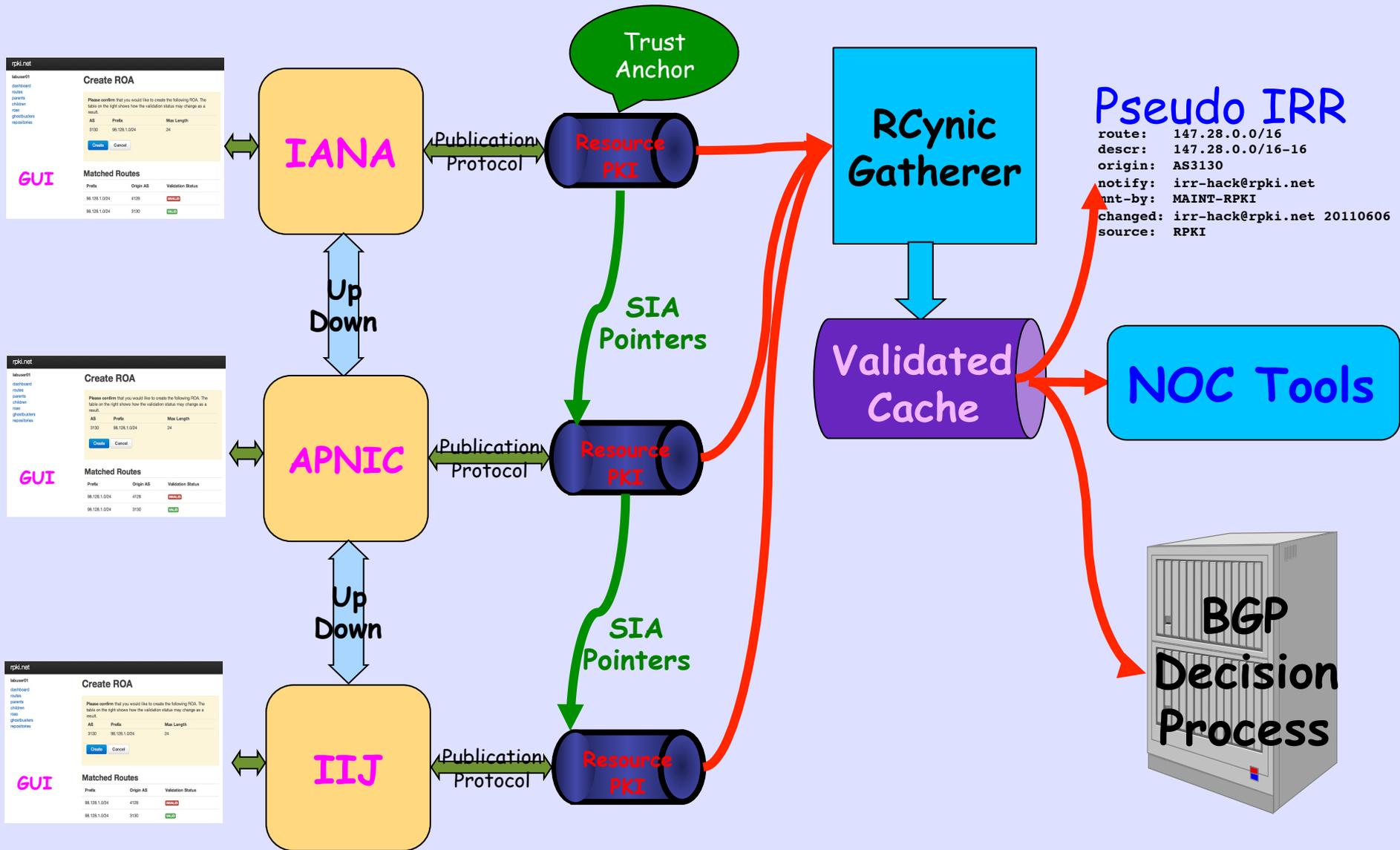


Issuing Parties



Issuing Parties

Relying Parties



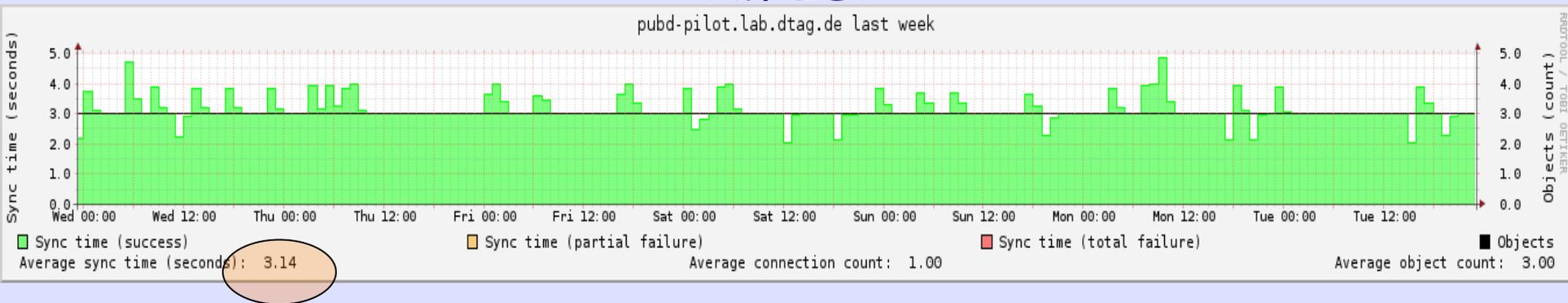
My Routing Relies on It!

- 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

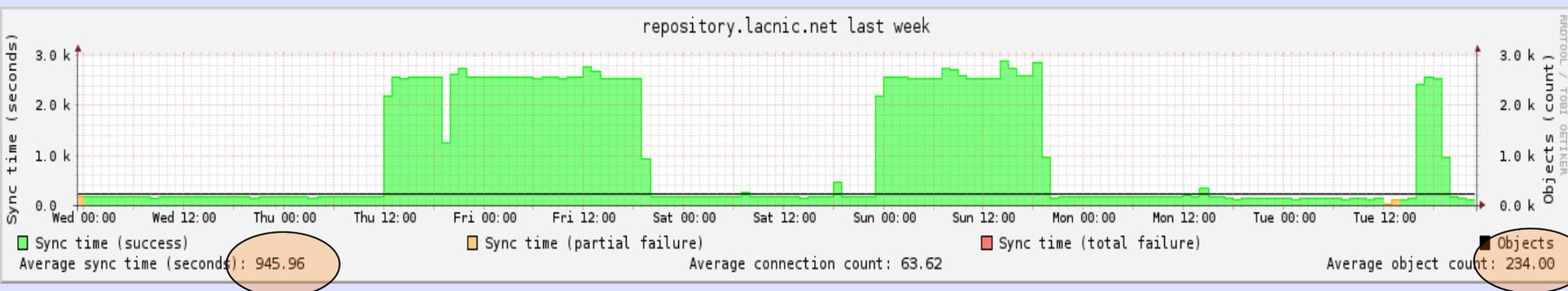
These Graphs are
from rпки.net's
Relying Party
Software Web Page
it Makes for You

Not Bad

An ISP



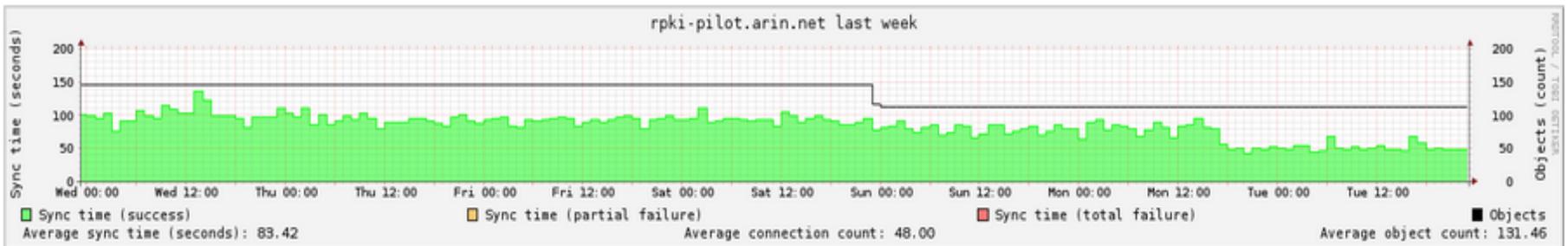
An RIR



Not So Good

Overview for repository `rpki-pilot.arin.net`

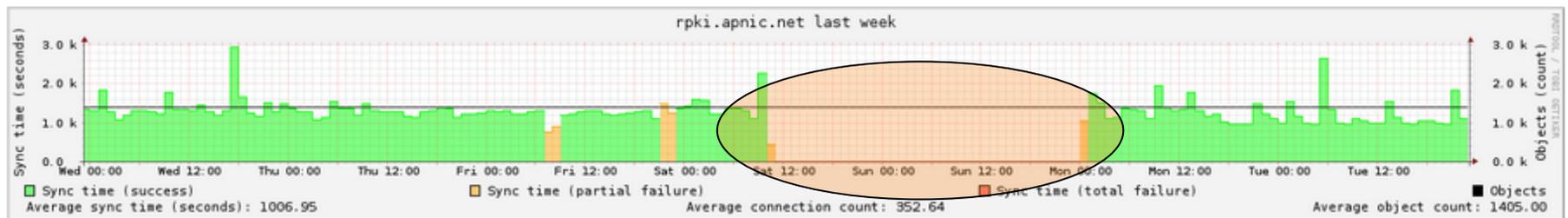
	certificate has expired	Bad keyUsage	Certificate failed validation	CRL not yet valid	CRLDP doesn't match issuer's SIA	Manifest not yet valid	Object rejected	EE certificate with 1024 bit key	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	rsync partial transfer	Stale CRL or manifest	Tainted by stale CRL	Tainted by stale manifest	Tainted by not being in manifest	Non-rsync URI in extension	Object accepted	rsync transfer succeeded
																		48
current .cer										18					48		48	
current .crl																	2	
current .mnf		48					48		18	11								
current .roa		14					14		5	5					14			
Total		62					62		23	34					62		50	48



Very Bad

Overview for repository rpkg.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 APNIC Engineering

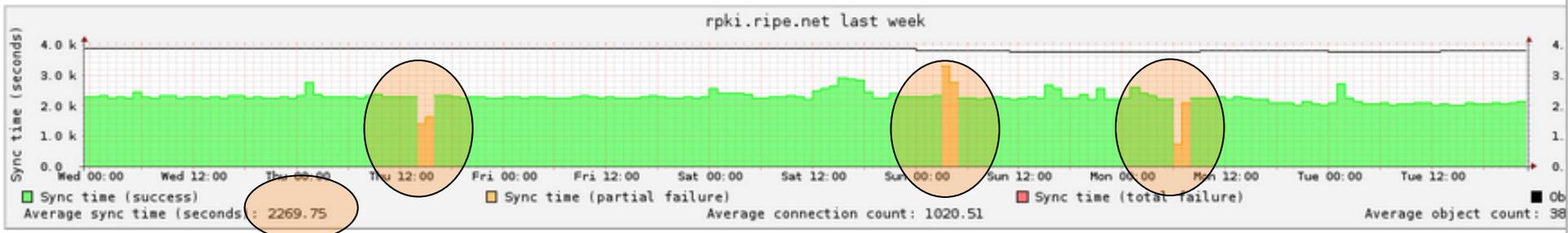
RIPE Stayed Up

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

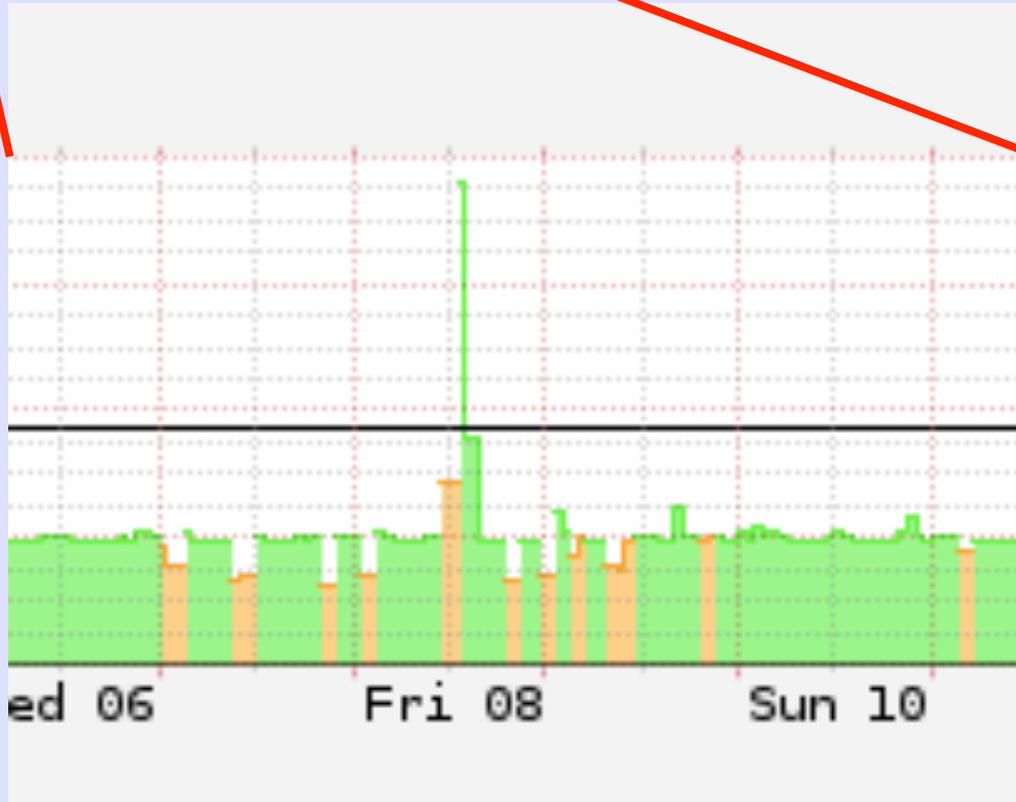
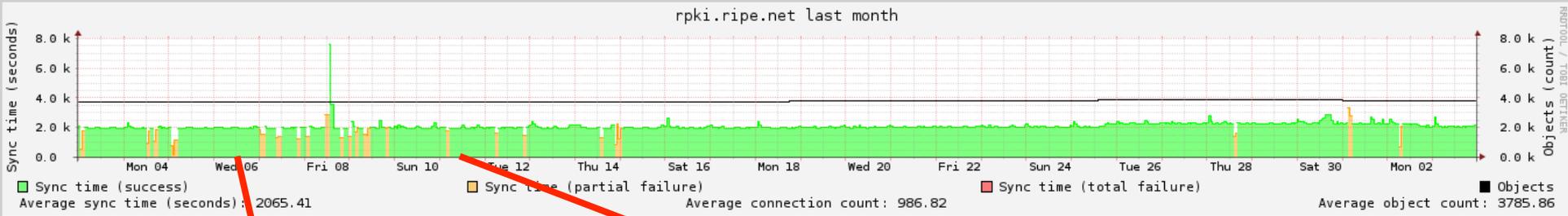
Overview Repositories Problems All Details

	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-sync 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



RIPE has Bad History



Cause

- This was an NFS problem (NFS is Evil!)
- It went on for months
- RPKI.NET logs had full detail showing "NFS"
- But "Nothing Can Be Wrong at the RIR"
- Finally it was fixed, but small problems remain

Just Weird

```
871553 -rw-r--r-x 4 rcynic rcynic 1969 Feb 17 13:26:29 2012 /  
usr/home/rpki/rcynic/data/authenticated.2012-07-11T00:00:00Z/  
rpki.afrinic.net/member_repository/  
F3634D22/92EF8890119911E0A59EB577833A7E19/79FBE550468F11E19086CAB  
E31FFE8A0.roa
```

```
871602 -rw-r--r-x 4 rcynic rcynic 2009 Feb 17 13:26:26 2012 /  
usr/home/rpki/rcynic/data/authenticated.2012-07-11T00:00:00Z/  
rpki.afrinic.net/member_repository/  
F3634D22/92EF8890119911E0A59EB577833A7E19/82331D8C6C2011E0890EBAC  
0A0C76497.roa
```

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

The RIRs are Not Network Operators

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

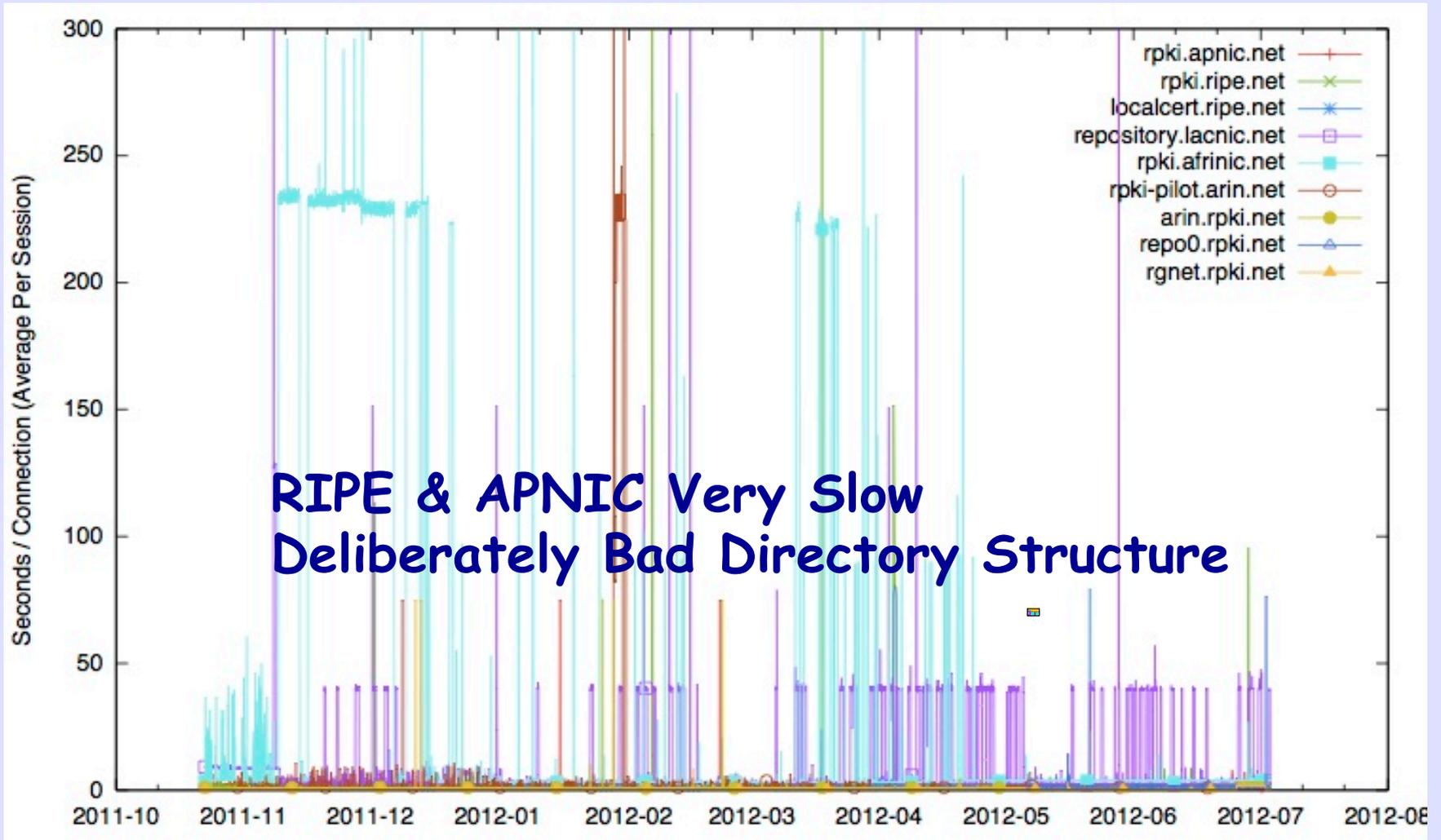
Good Software Will Save US

- Of course, good relying party software will expect failures, so this is not a killer
- rpki.net relying party software uses old data if it can not fetch new
- As RPKI data are fairly stable, this is OK
- But RIPE's in-addr disaster lasted five days!

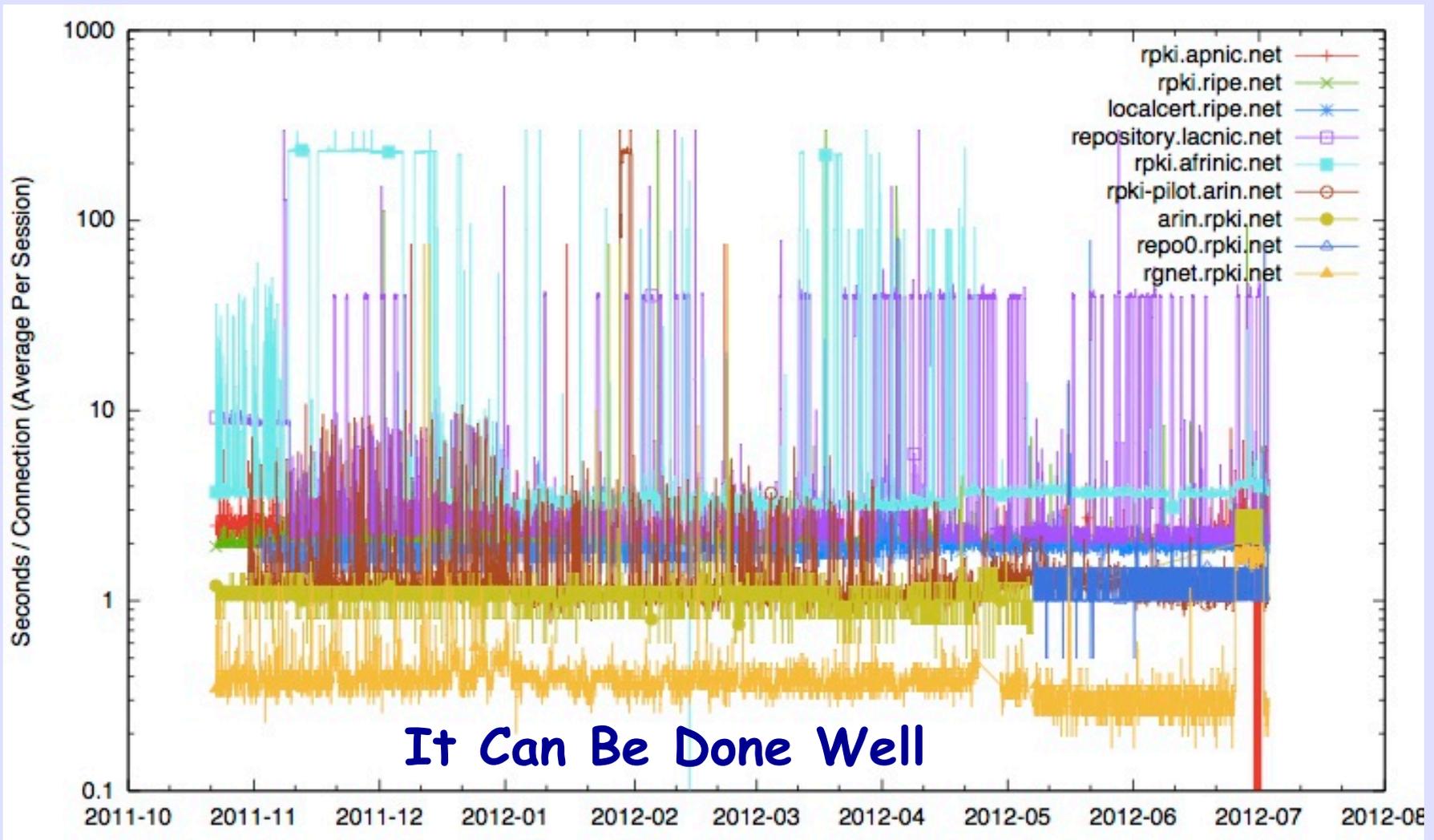
Some Statistics

Again, from rpki.net
Relying Party
Software

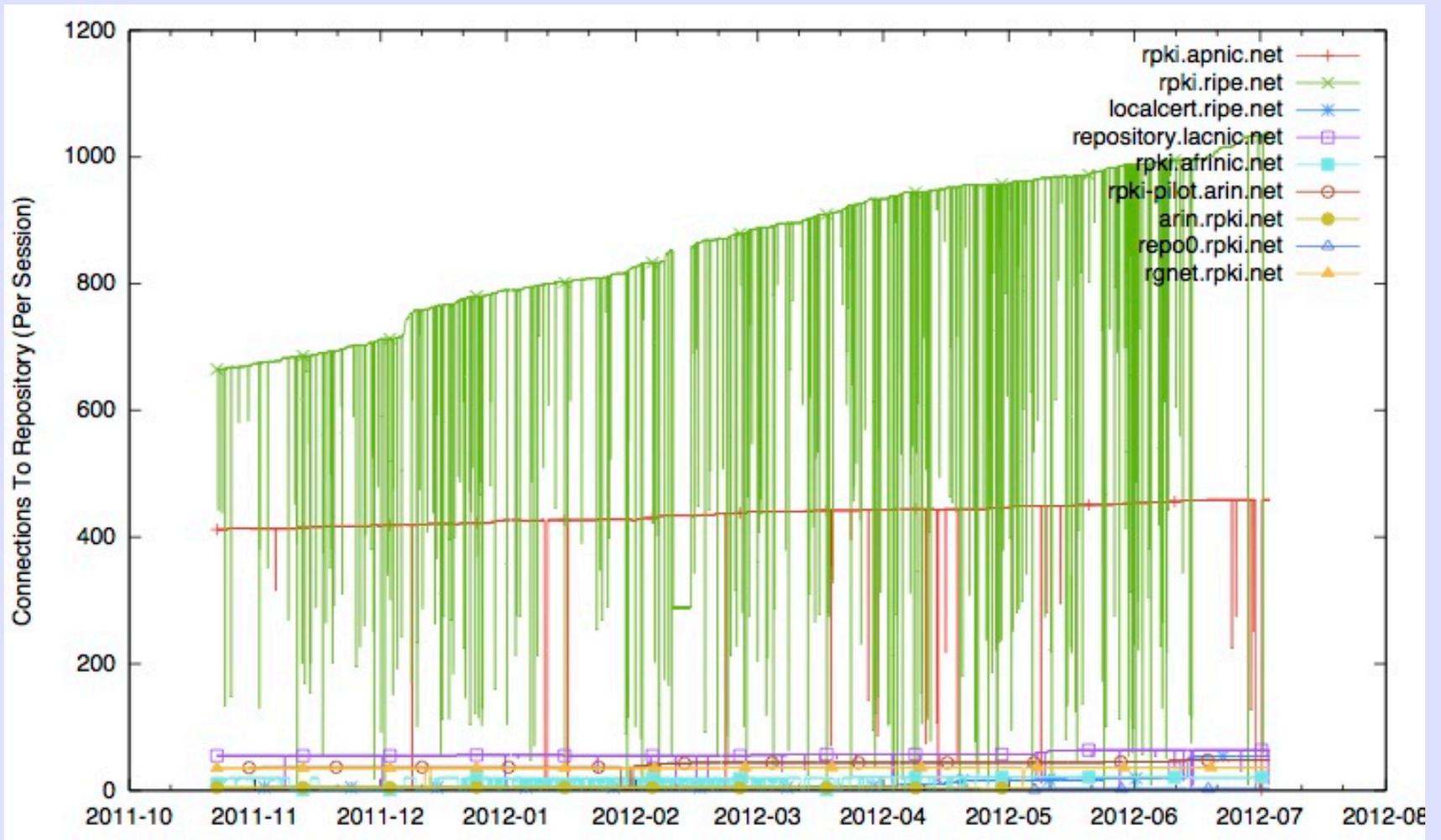
Connect Time (linear)



Connect Time (log)



Connection Counts



Number of Objects



Conclusions

- RPKI Deployment is serious, especially in the RIPE region
- RIRs are not Operator Quality/Reliability
- JPNIC could set an example!
- APNIC & RIPE Publication Structure needs to be fixed
- Relying Party software works around these
- More Measurement and Monitoring