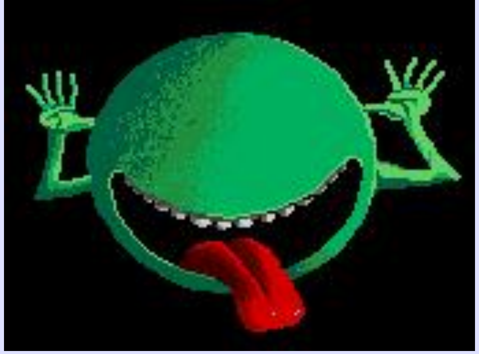
Measuring RPKI Repositories

JaNOG / Kurashiki

2012.05.06

Randy Bush <randy@psg.com>

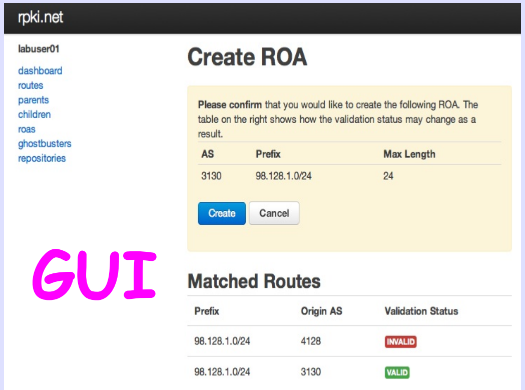


Don't Panic

- 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



rpki.net

labuser01

dashboard
routes
parents
children
roas
ghostbusters
repositories

Create ROA

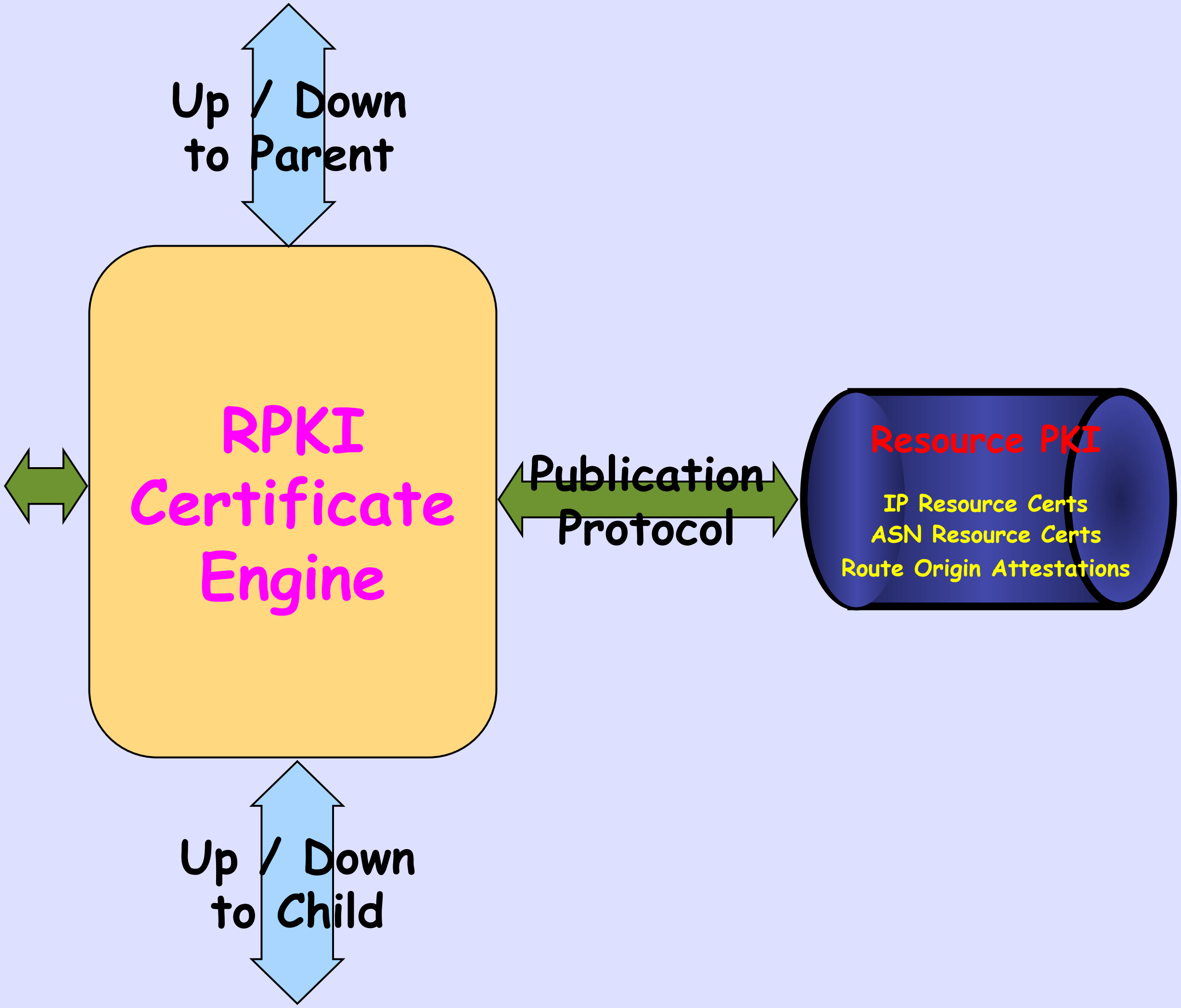
Please confirm that you would like to create the following ROA. The table on the right shows how the validation status may change as a result.

AS	Prefix	Max Length
3130	98.128.1.0/24	24

Matched Routes

Prefix	Origin AS	Validation Status
98.128.1.0/24	4128	INVALID
98.128.1.0/24	3130	VALID

GUI



Up / Down to Parent

RPKI Certificate Engine

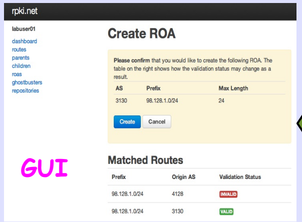
Publication Protocol

Resource PKI

IP Resource Certs
ASN Resource Certs
Route Origin Attestations

Up / Down to Child

Issuing Parties



rpki.net

labuser01

dashboard
routes
parents
children
roas
ghostbusters
repositories

GUI

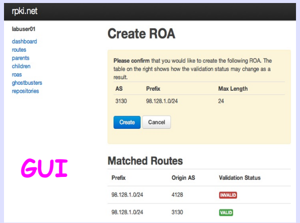
Create ROA

Please confirm that you would like to create the following ROA. The table on the right shows how the validation status may change as a result.

AS	Prefix	Max Length
3130	98.128.1.0/24	24

Matched Routes

Prefix	Origin AS	Validation Status
98.128.1.0/24	4128	INVALID
98.128.1.0/24	3130	VALID



rpki.net

labuser01

dashboard
routes
parents
children
roas
ghostbusters
repositories

GUI

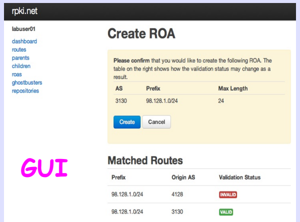
Create ROA

Please confirm that you would like to create the following ROA. The table on the right shows how the validation status may change as a result.

AS	Prefix	Max Length
3130	98.128.1.0/24	24

Matched Routes

Prefix	Origin AS	Validation Status
98.128.1.0/24	4128	INVALID
98.128.1.0/24	3130	VALID



rpki.net

labuser01

dashboard
routes
parents
children
roas
ghostbusters
repositories

GUI

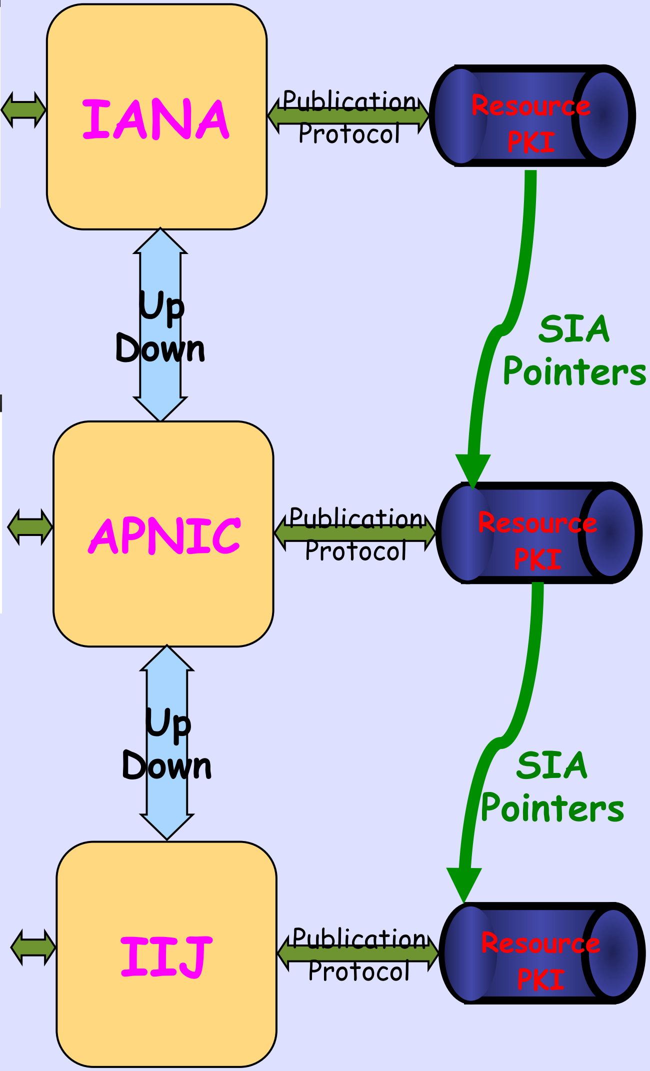
Create ROA

Please confirm that you would like to create the following ROA. The table on the right shows how the validation status may change as a result.

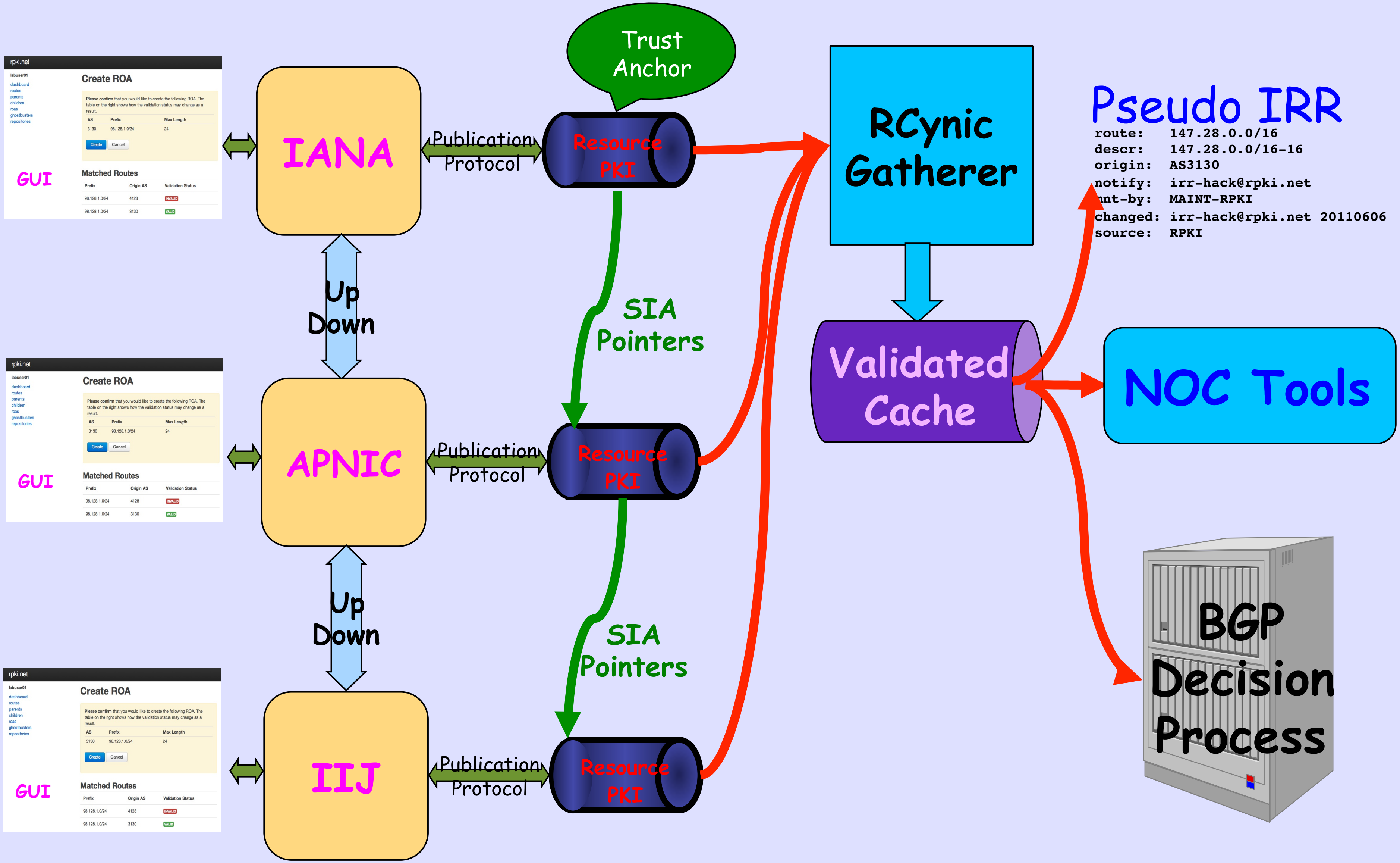
AS	Prefix	Max Length
3130	98.128.1.0/24	24

Matched Routes

Prefix	Origin AS	Validation Status
98.128.1.0/24	4128	INVALID
98.128.1.0/24	3130	VALID



Issuing Parties   Relying Parties



rpki.net

labuser01

dashboard
routes
parents
children
roas
ghostbusters
repositories

Create ROA

Please confirm that you would like to create the following ROA. The table on the right shows how the validation status may change as a result.

AS	Prefix	Max Length
3130	98.128.1.0/24	24

Create | Cancel

Matched Routes

Prefix	Origin AS	Validation Status
98.128.1.0/24	4128	INVALID
98.128.1.0/24	3130	VALID

rpki.net

labuser01

dashboard
routes
parents
children
roas
ghostbusters
repositories

Create ROA

Please confirm that you would like to create the following ROA. The table on the right shows how the validation status may change as a result.

AS	Prefix	Max Length
3130	98.128.1.0/24	24

Create | Cancel

Matched Routes

Prefix	Origin AS	Validation Status
98.128.1.0/24	4128	INVALID
98.128.1.0/24	3130	VALID

rpki.net

labuser01

dashboard
routes
parents
children
roas
ghostbusters
repositories

Create ROA

Please confirm that you would like to create the following ROA. The table on the right shows how the validation status may change as a result.

AS	Prefix	Max Length
3130	98.128.1.0/24	24

Create | Cancel

Matched Routes

Prefix	Origin AS	Validation Status
98.128.1.0/24	4128	INVALID
98.128.1.0/24	3130	VALID

```
route:    147.28.0.0/16
descr:    147.28.0.0/16-16
origin:   AS3130
notify:   irr-hack@rpki.net
mnt-by:   MAINT-RPKI
changed:  irr-hack@rpki.net 20110606
source:   RPKI
```

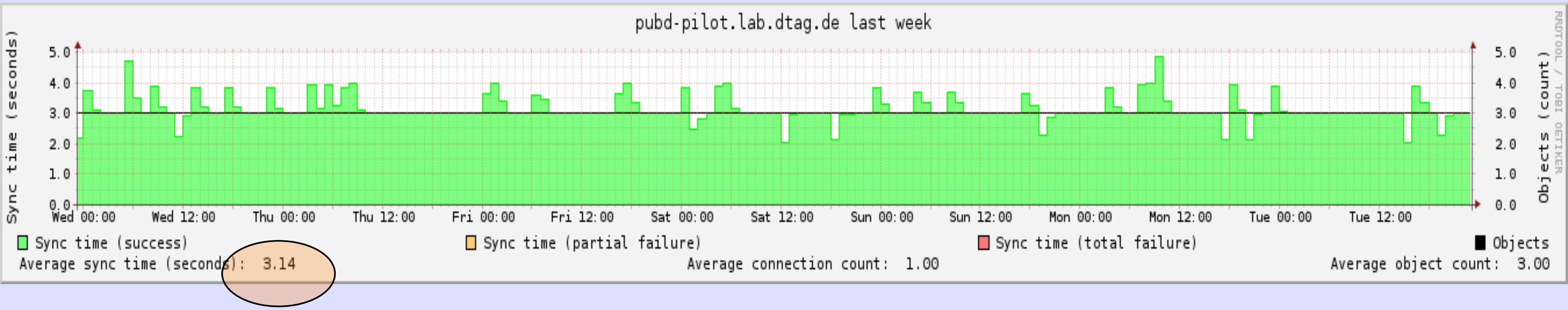
My Routing Relies on It!

- 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

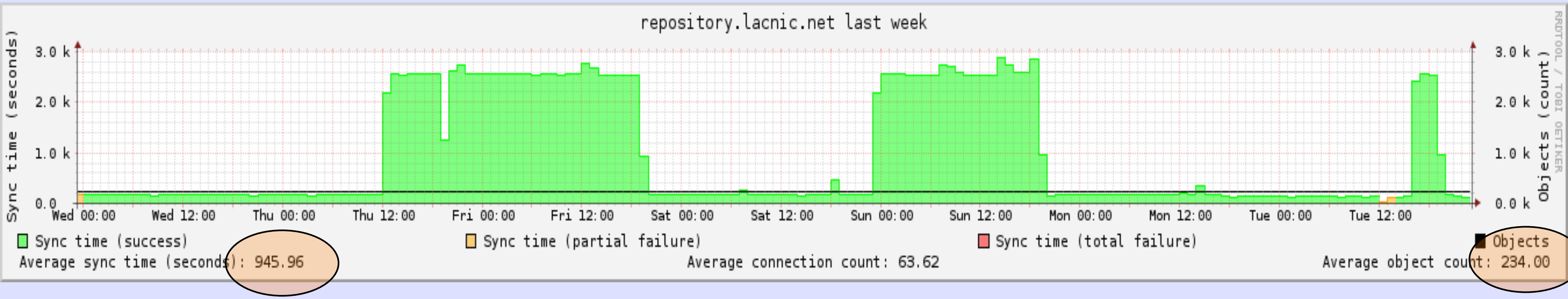
These Graphs are from rpki.net's Relying Party Software Web Page it Makes for You

Not Bad

An ISP

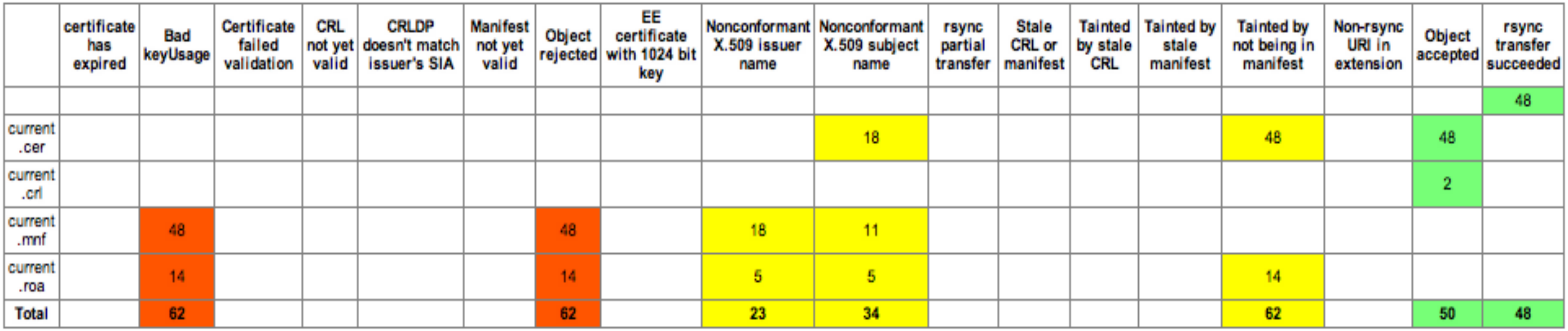


An RIR

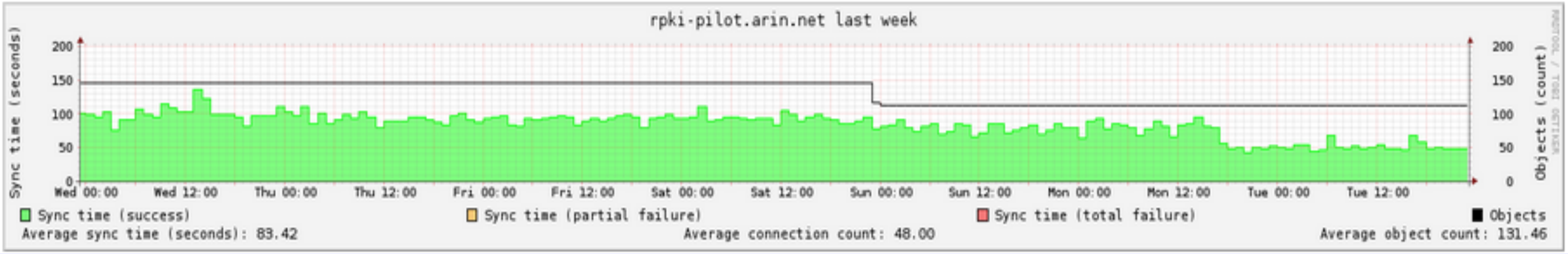


Not So Good

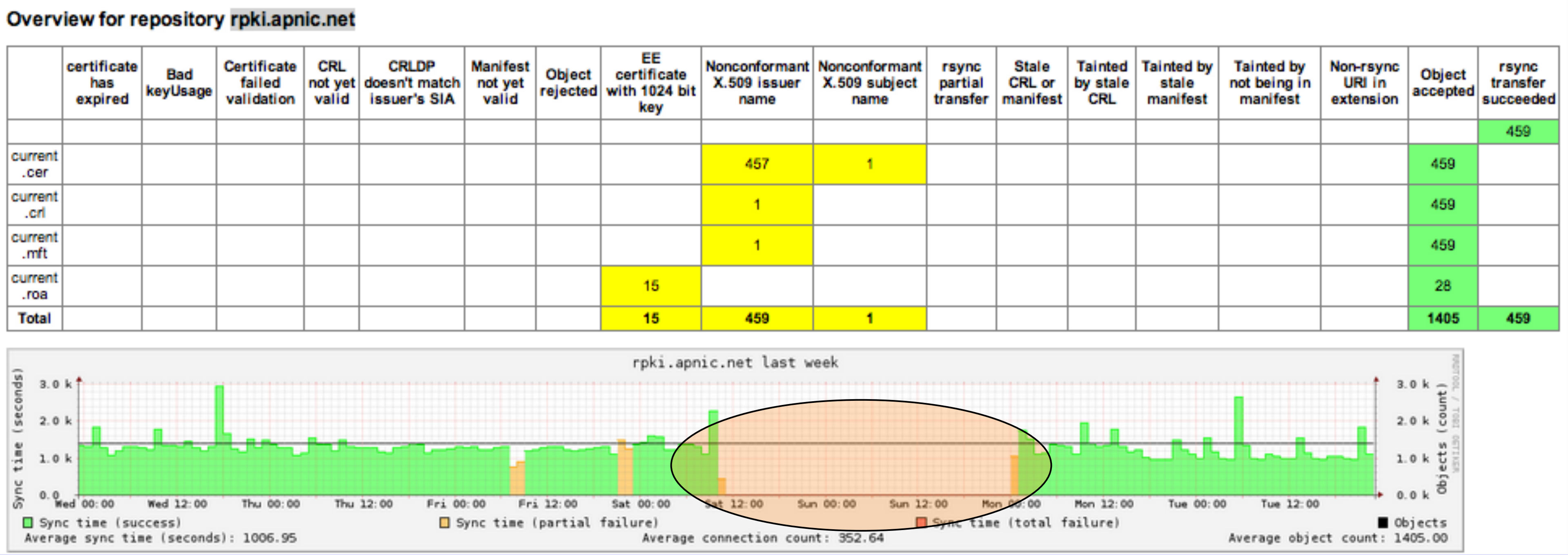
Overview for repository rpki-pilot.arin.net



	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

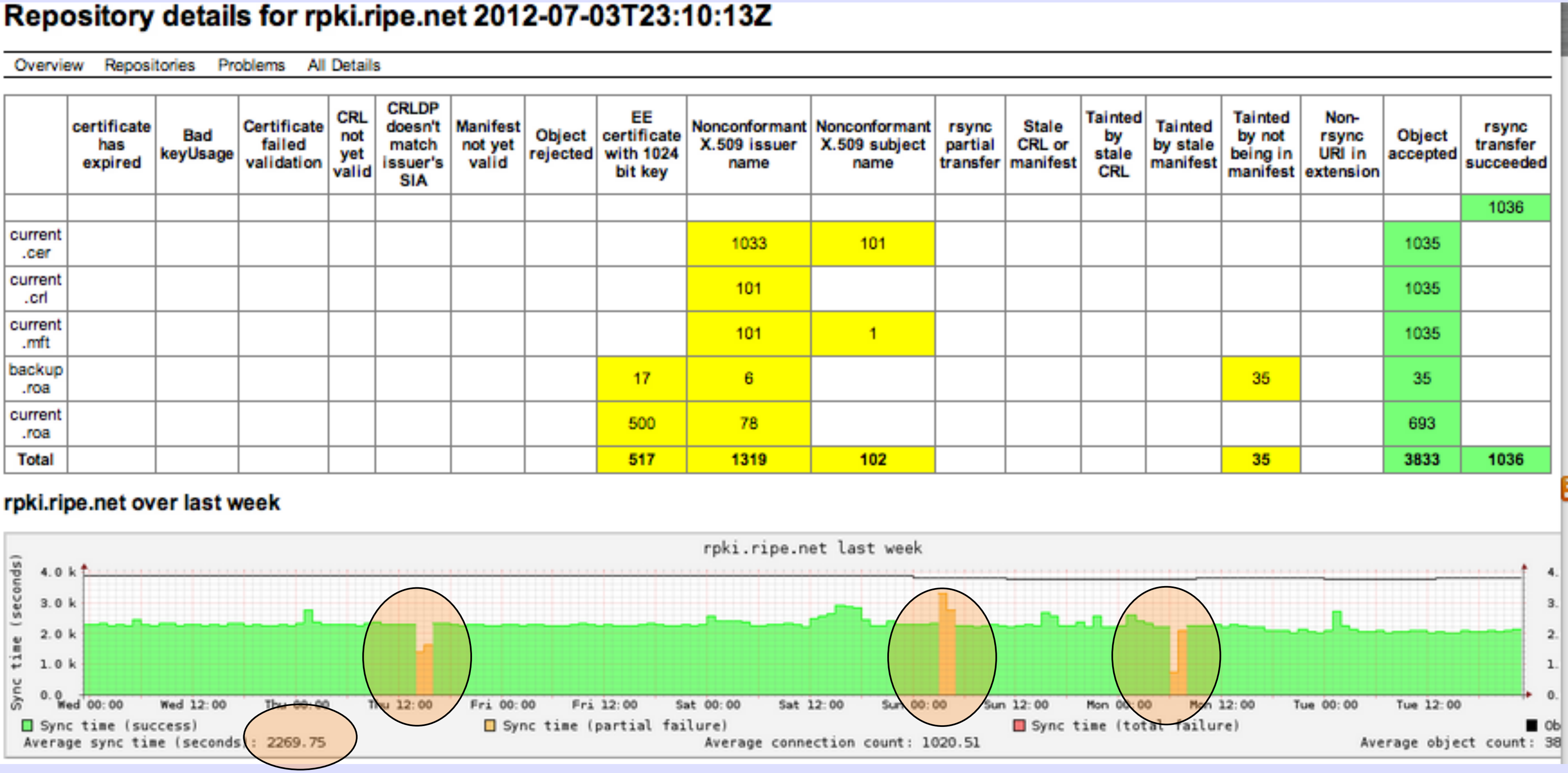


Overview for repository rpki.apnic.net

	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 APNIC Engineering

RIPE Stayed Up



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

Overview Repositories Problems All Details

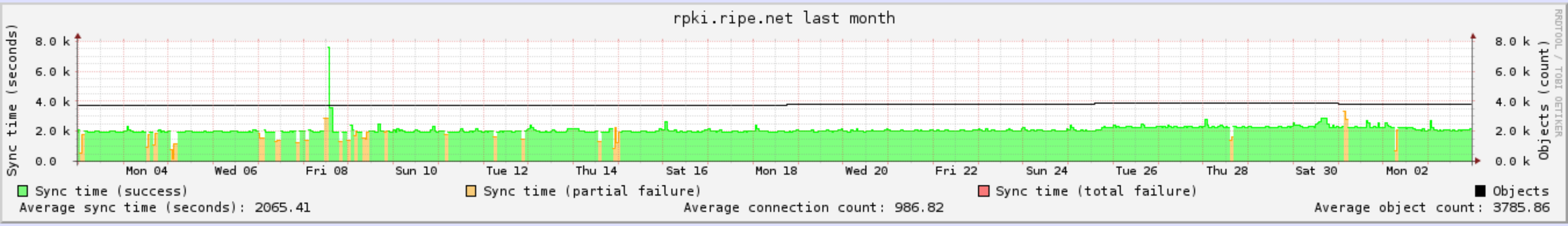
	certificate has expired	Bad keyUsage	Certificate failed validation	CRL not yet valid	CRLDP doesn't match issuer's SIA	Manifest not yet valid	Object rejected	EE certificate with 1024 bit key	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	rsync partial transfer	Stale CRL or manifest	Tainted 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

🟩 Sync time (success) 🟧 Sync time (partial failure) 🟥 Sync time (total failure) ■ Ob

Average sync time (seconds): 2269.75 Average connection count: 1020.51 Average object count: 38

RIPE has Bad History



- 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

The RIRs are Not Network Operators

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

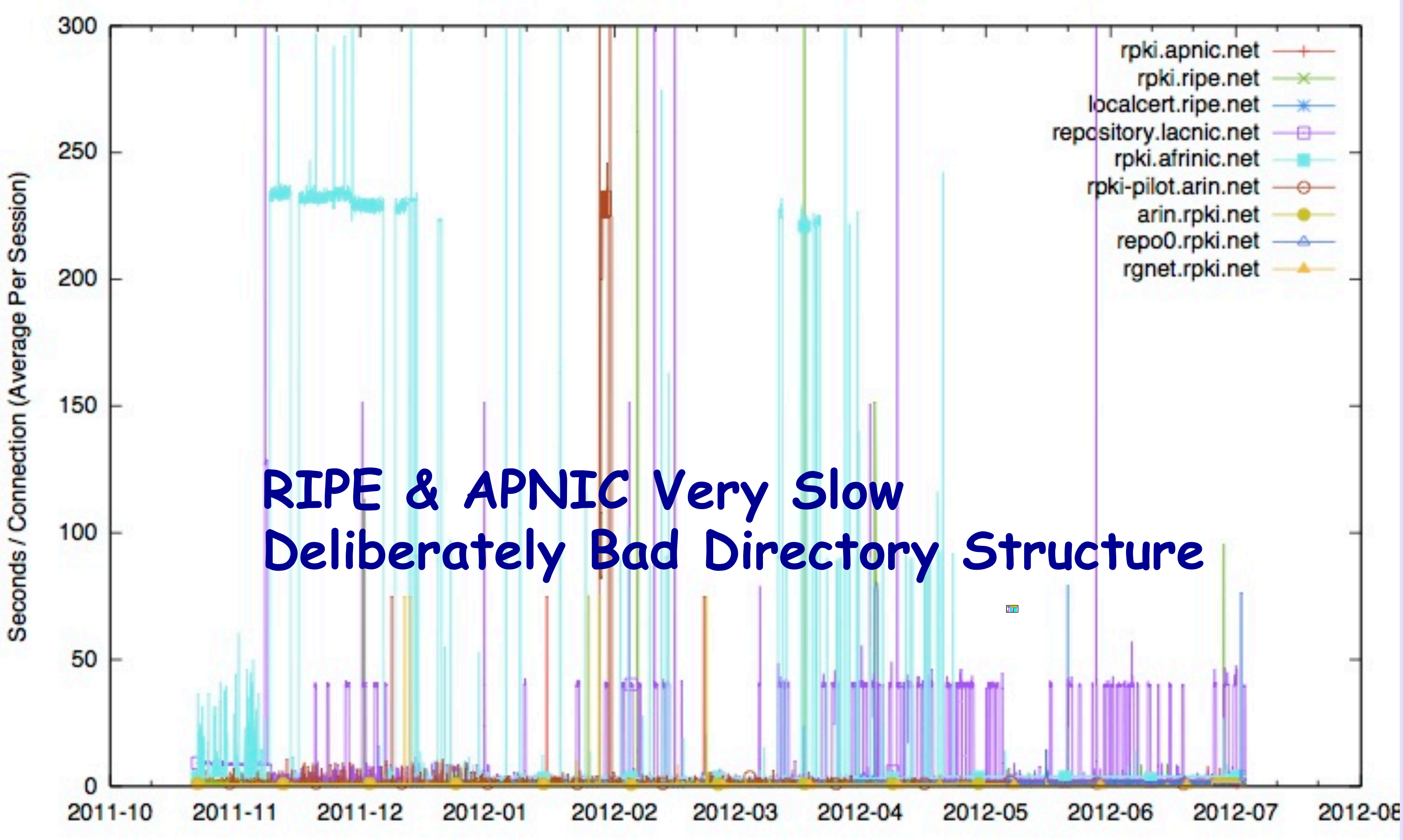
Good Software Will Save US

- 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

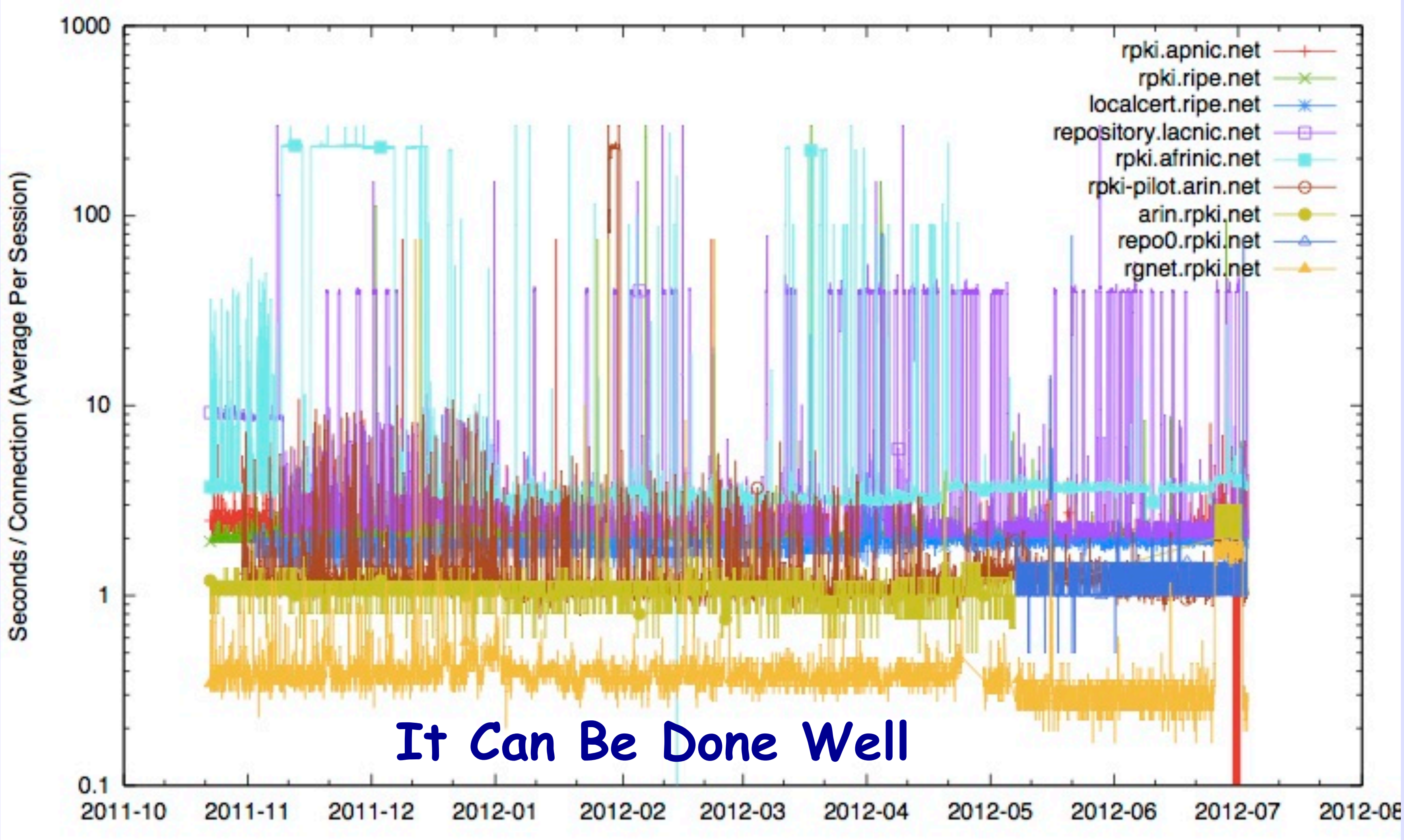
Again, from rpki.net Relying Party Software

Connect Time (linear)



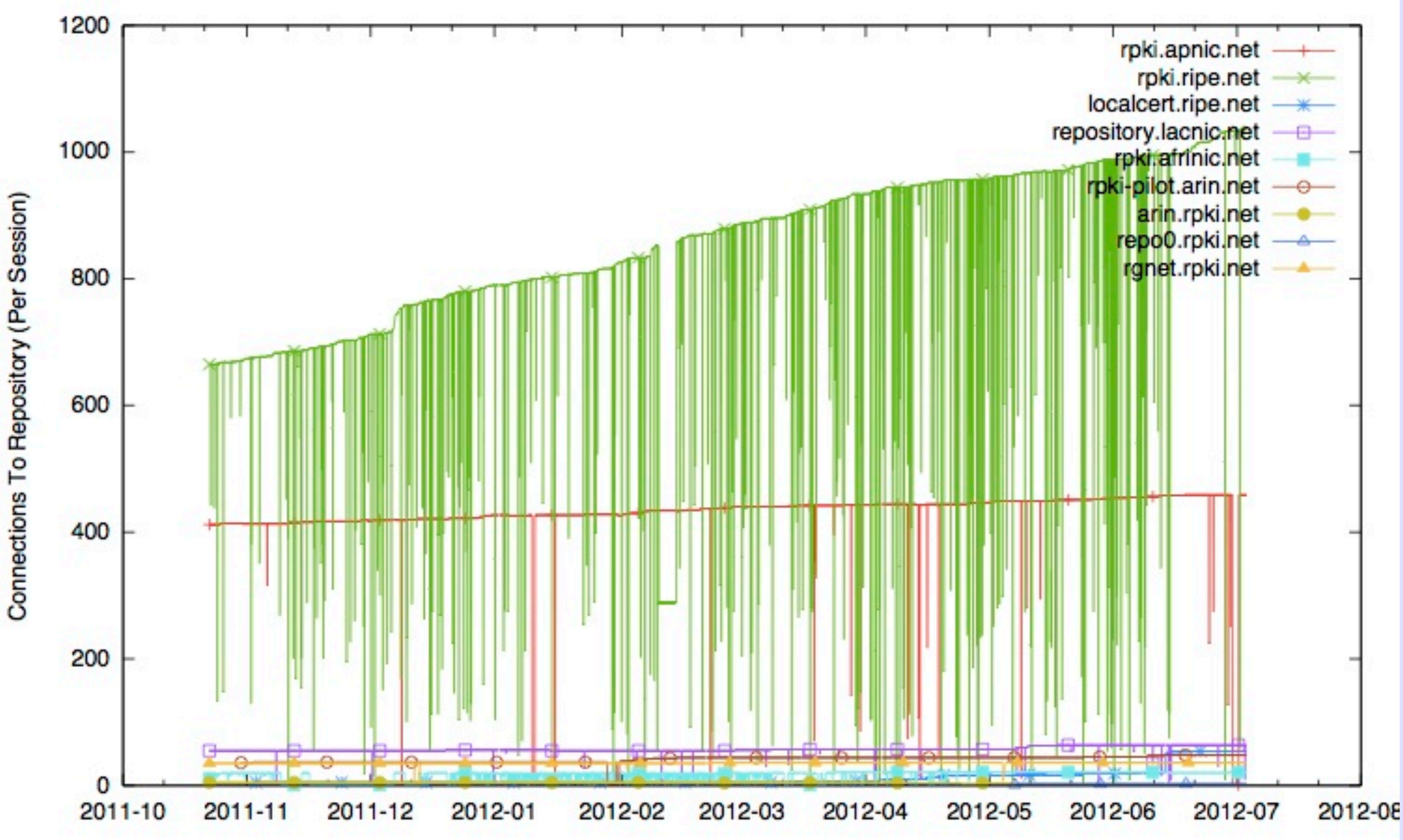
RIPE & APNIC Very Slow
Deliberately Bad Directory Structure

Connect Time (log)

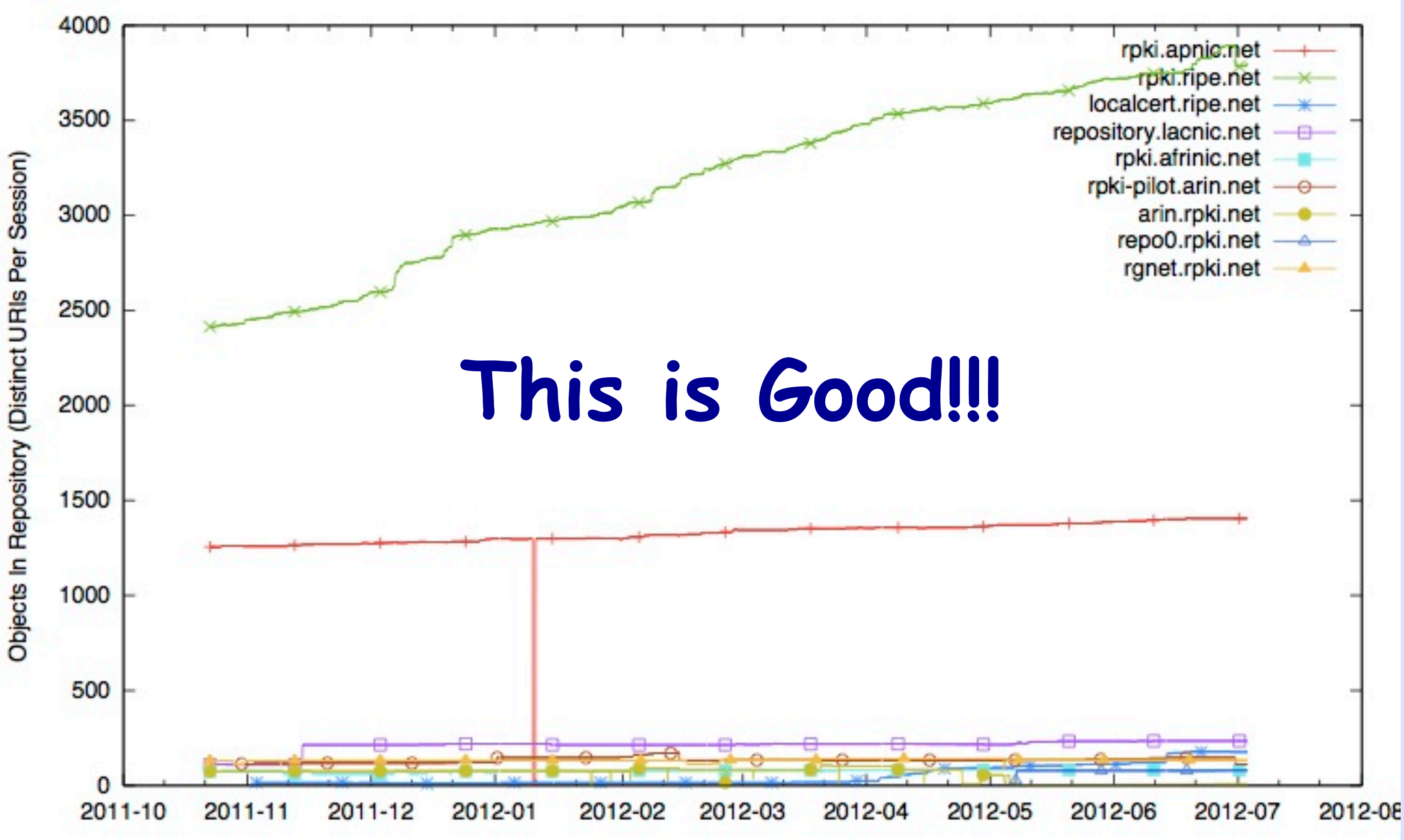


It Can Be Done Well

Connection Counts



Number of Objects



This is Good!!!

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