

The Non-Trivialities of deploying a Public Key Infrastructure




**Harvard, Crypto Class Guest Lecture
November 28, 2010**



How Secure is Routing on the Internet Today? (1)

February 2008 : Pakistan Telecom hijacks Youtube



Corrigendum- Most Urgent

GOVERNMENT OF PAKISTAN
PAKISTAN TELECOMMUNICATION AUTHORITY
ZONAL OFFICE PESHAWAR
Plot-11, Sector A-3, Phase-V, Hayatabad, Peshawar.
Ph: 091-9217279- 5829177 Fax: 091-9217254
www.pta.gov.pk

NWFP-33-16 (BW)/06/PTA February ,2008

Subject: **Blocking of Offensive Website**

Reference: *This office letter of even number dated 22.02.2008.*

I am directed to request all ISPs to immediately block access to the following website

URL: <http://www.youtube.com/watch?v=o3s8jtvvg00>

IPs: 208.65.153.238, 208.65.153.253, 208.65.153.251

Compliance report should reach this office through return fax or at email peshawar@pta.gov.pk today please.

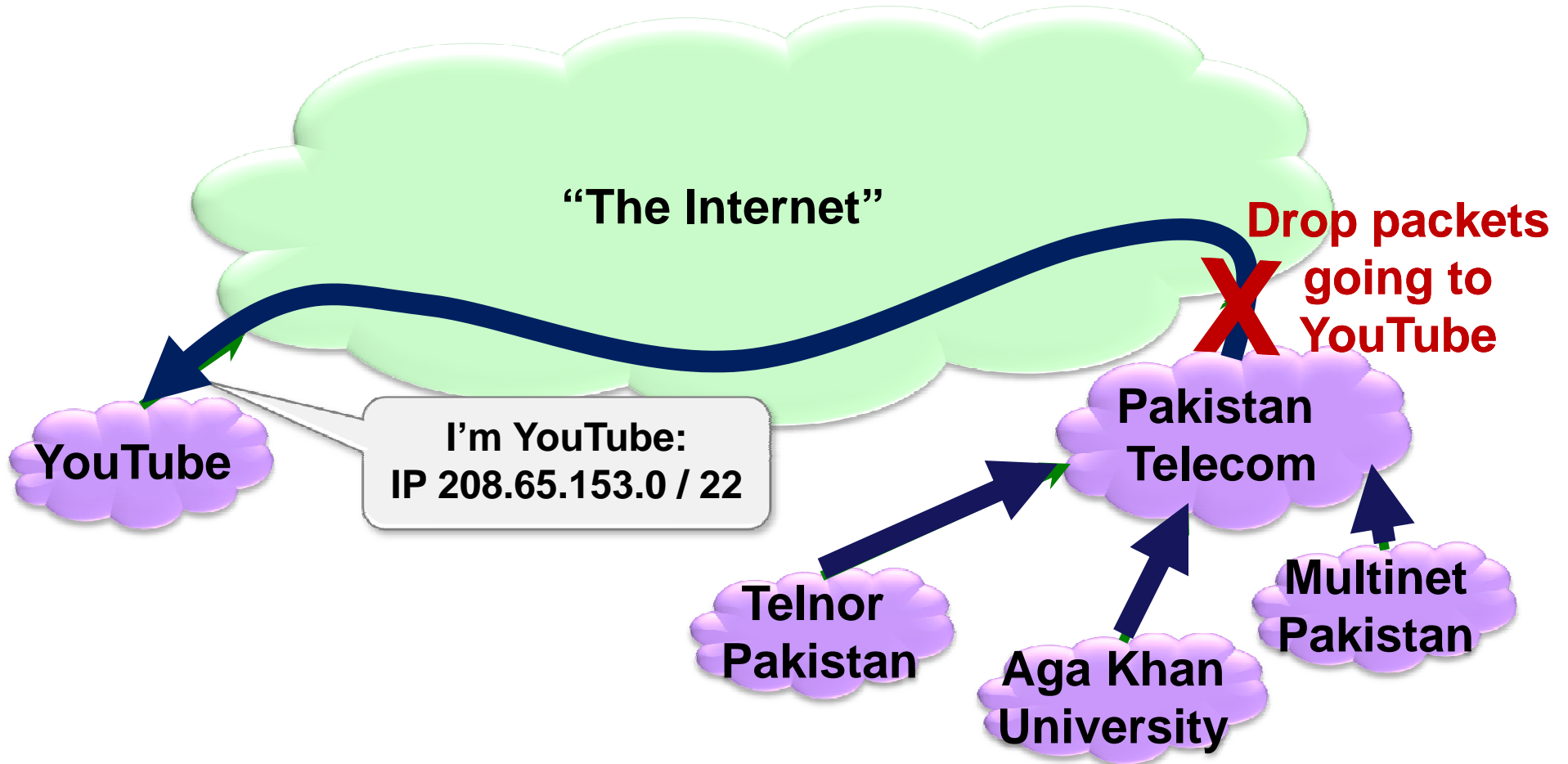
YouTube

an
om
Multinet
Pakistan



How Secure is Routing on the Internet Today? (2)

Here's what should have happened....

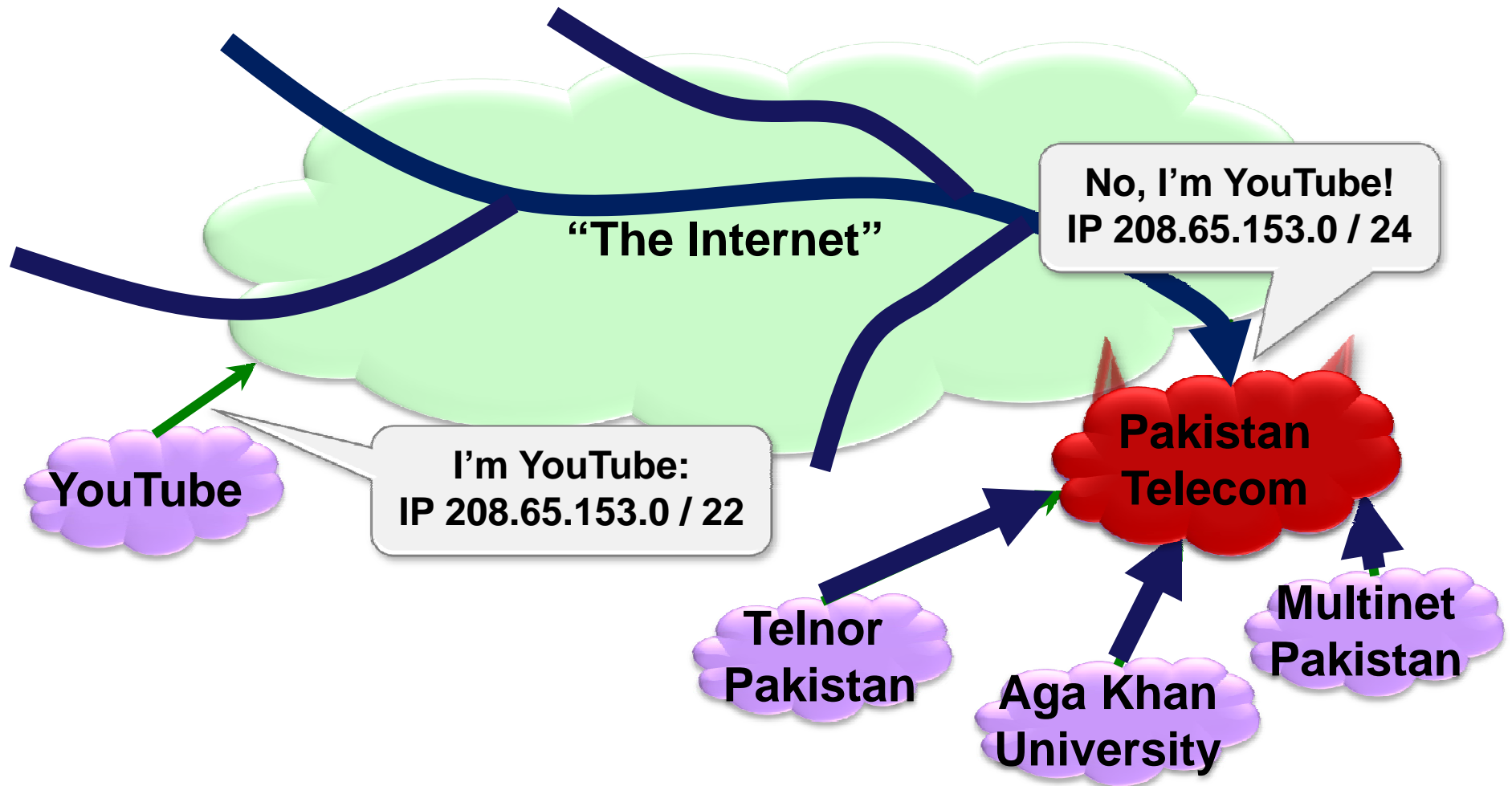


Block your own customers.



How Secure is Routing on the Internet Today? (3)

But here's what Pakistan ended up doing...



Draw traffic from the entire Internet!

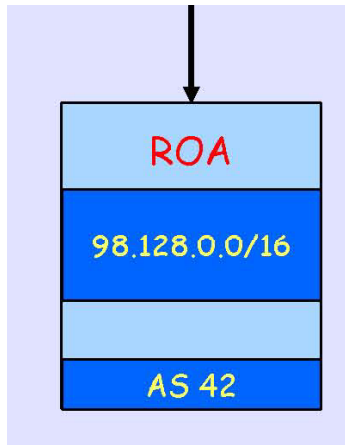


Part 1: Technical Details

Part 2: Political Issues



The ROA and the RPKI



Randy Bush,
NANOG 52

- ROA – Route Origin Attestation
 - Certificate binding IP address block to AS #
 - ... signed by the entity that owns both
 - ... and stamped with an expiration time
-
- The trust anchor for this system is IANA
 - Which delegates IP Address blocks, AS #s
 - And also certifies public keys
-
- The RPKI is the system that does this
 - Chain of trust is a strict hierarchy
 - Implementation is a distributed database



RPKI and IP address / ASN allocation hierarchy

PSGnet /16
Experimental
Allocation
from ARIN

Announces
256 /24s



Too Many EE Certs and ROAs, Yucchhy!



Ephemeral public keys and attestations

Route Origin Authorization (ROA)

Long-term Certificate



Certificate for an ephemeral key



End Entity Cert
can not sign certs.
can sign other things
e.g. ROAs



This is not a Cert
It is a signed blob



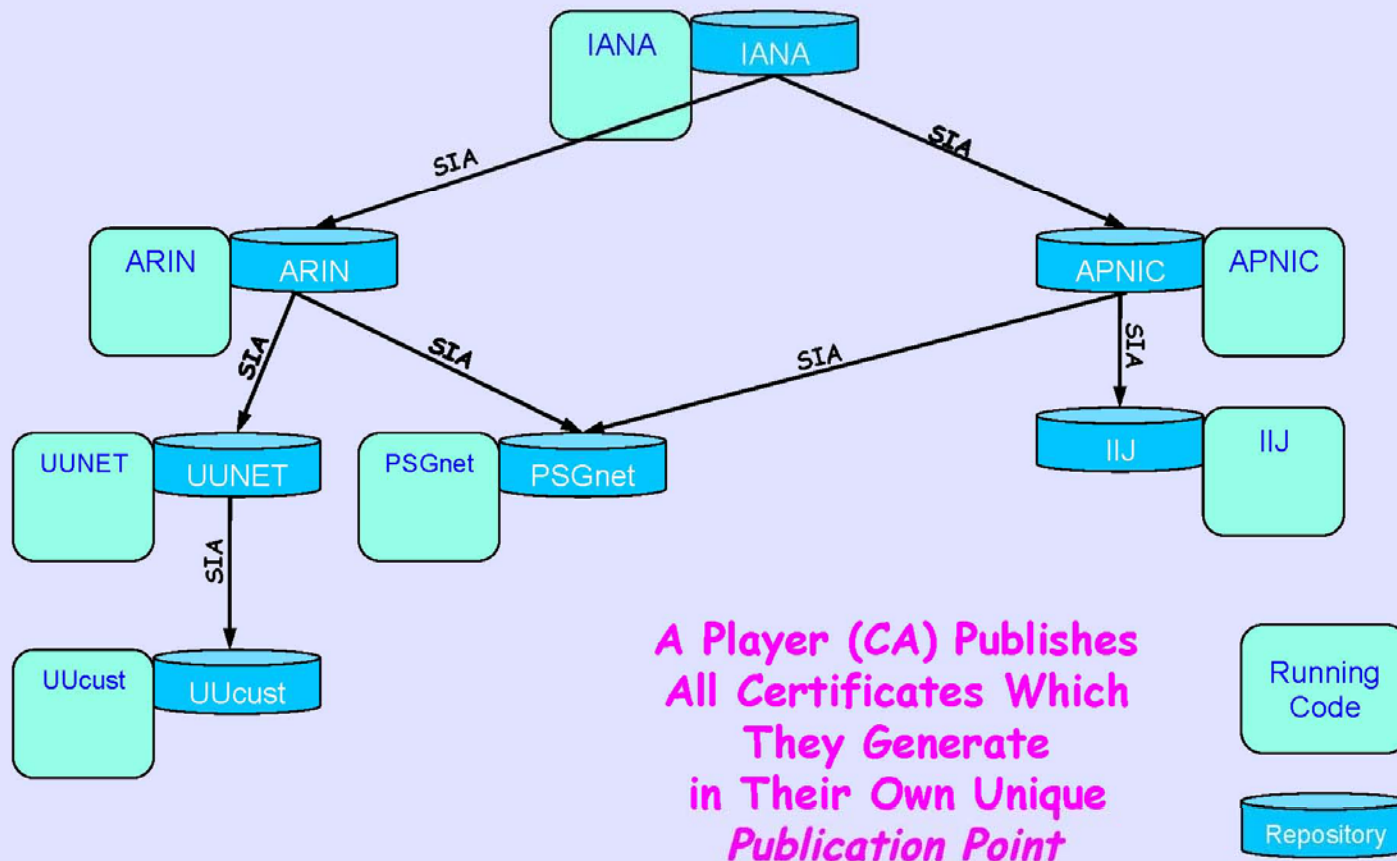
Revocation & Expiration

- Two ways to “invalidate” a certificate
 1. Expiration (it expires, or one of it’s parent certs expires)
 2. Revocation
 - Uses a CRL - certificate revocation list
 - CRL is issued by the authority that issued the cert
 - Either query based “Is this cert ok?”, or a full list is published.
 - Complicates things! Introduces latency. People may not bother.
- A CA certificate may be revoked by due to
 - key rollover (compromised, or just to keep it fresh)
 - change in the allocated resource set (IP addresses, AS numbers)
- To invalidate a ROA, the CA revokes the EE certificate.
 - EE Certs typically used just once, for a single ROA!



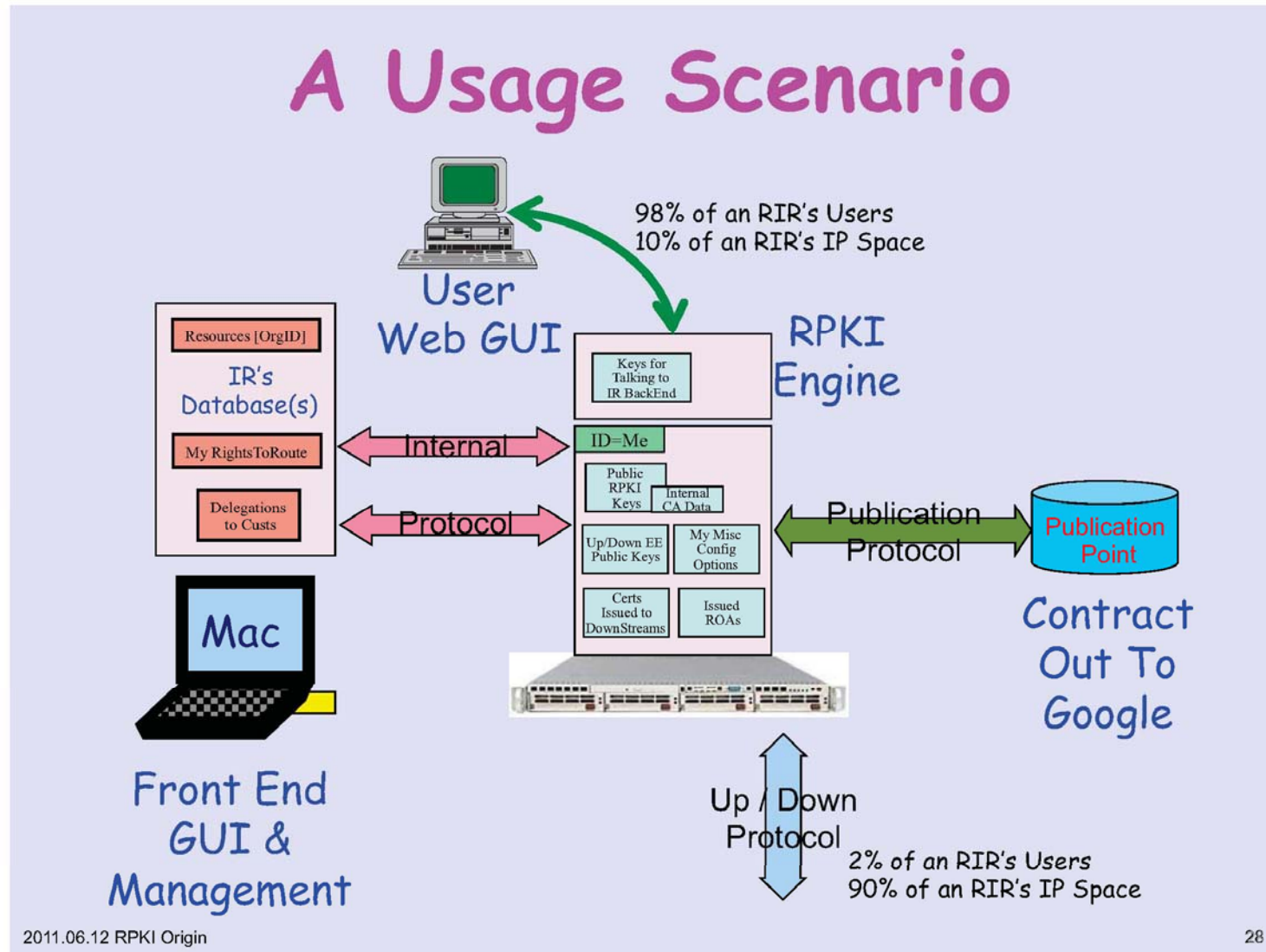
Implementation as a distributed database (1)

Distributed RPKI DataBase



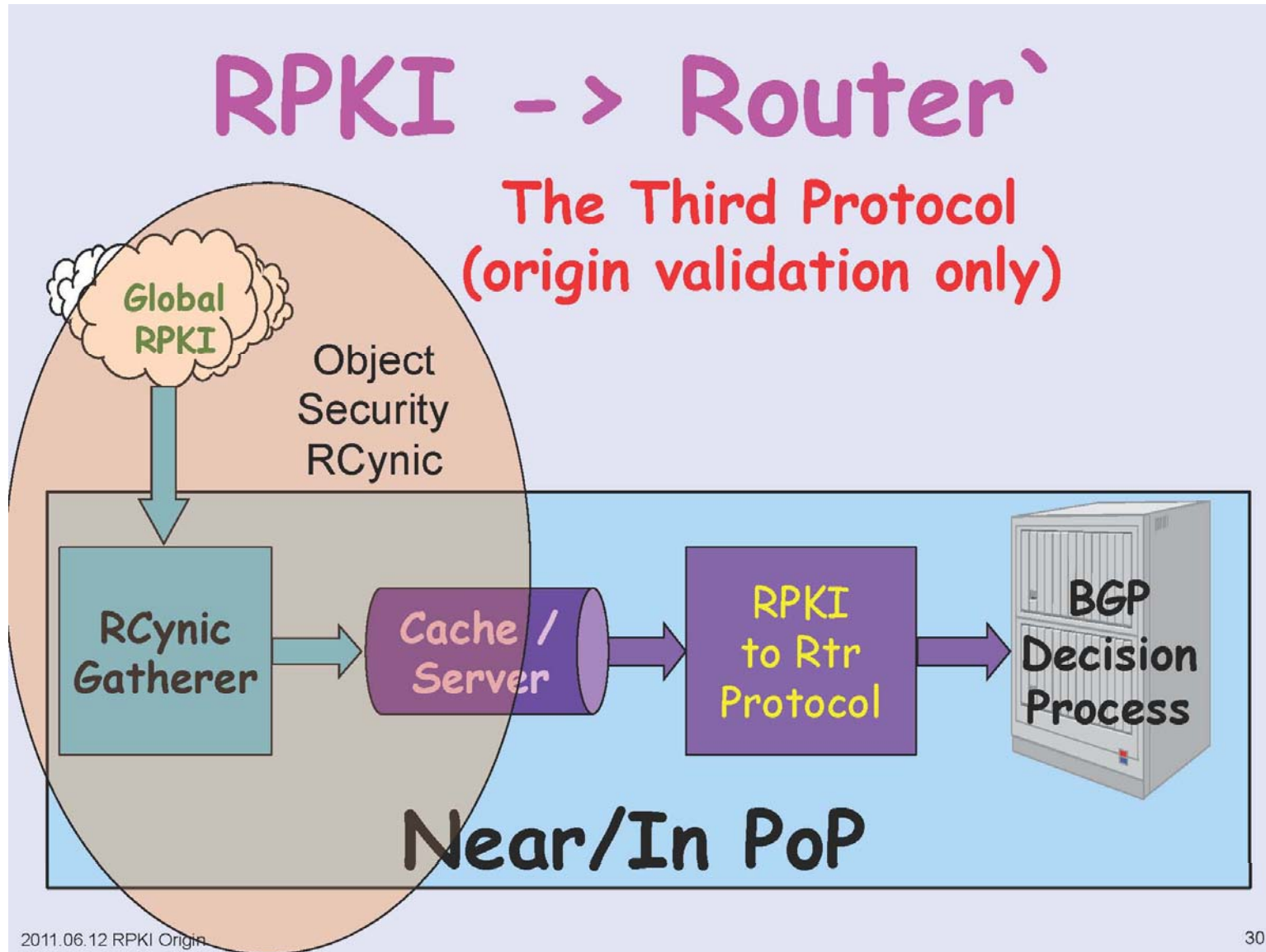


Implementation as a distributed database (2)





Implementation as a distributed database (3)





Does an invalid/missing cert mean I can't route? (1)

Result of Check

- **Valid** - A matching/covering ROA was found with a matching AS number
- **Invalid** - A matching or covering ROA was found, but AS number did not match, and there was no valid one
- **Not Found** - No matching or covering ROA was found



Does an invalid/missing cert mean I can't route? (2)

Policy Override Knobs

- Disable Validity Check Completely
- Disable Validity Check for a Peer
- Disable Validity Check for Prefixes

When check is disabled, the result is "Not Found," i.e. as if there was no ROA

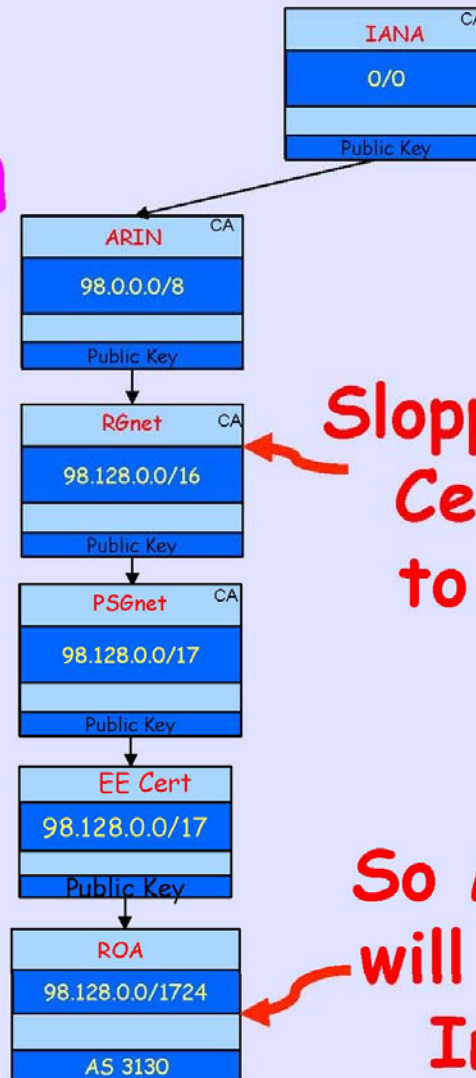


Does an invalid/missing cert mean I can't route? (3)

Up-Chain Expiration

BGP routing message will become "not found" not "invalid"

(I think this is a special case to deal with expiring ROAs)



Sloppy Admin,
Cert Soon
to Expire!

So My ROA
will become
Invalid!



What they tell the operators to calm them down.

But in the End, You Control Your Policy

"Announcements with Invalid origins *MAY* be used, but *SHOULD* be less preferred than those with Valid or NotFound."

-- draft-ietf-sidr-origin-ops

But if I do not reject Invalid, what is all this for?

Slide: Randy Bush, NANOG 52

2011.06.12 RPKI Origin

- This is only partly true!
- The routing system is a graph.
- I may be influenced by other nodes. If someone wrongly rejects a route due to "not found" or "invalid" I may not get the route.



Part 1: Technical Details

Part 2: Political Issues



Who paid for this thing?

Work Supported By

- **US Government**

THIS PROJECT IS SPONSORED BY THE DEPARTMENT OF HOMELAND SECURITY UNDER AN INTERAGENCY AGREEMENT WITH THE AIR FORCE RESEARCH LABORATORY (AFRL). [0]

[0] - they Take your Scissors Away and we turn them into plowshares

- **ARIN**

- **Internet Initiative Japan & ISC**

- **Cisco, Juniper, Google, NTT, Equinix**

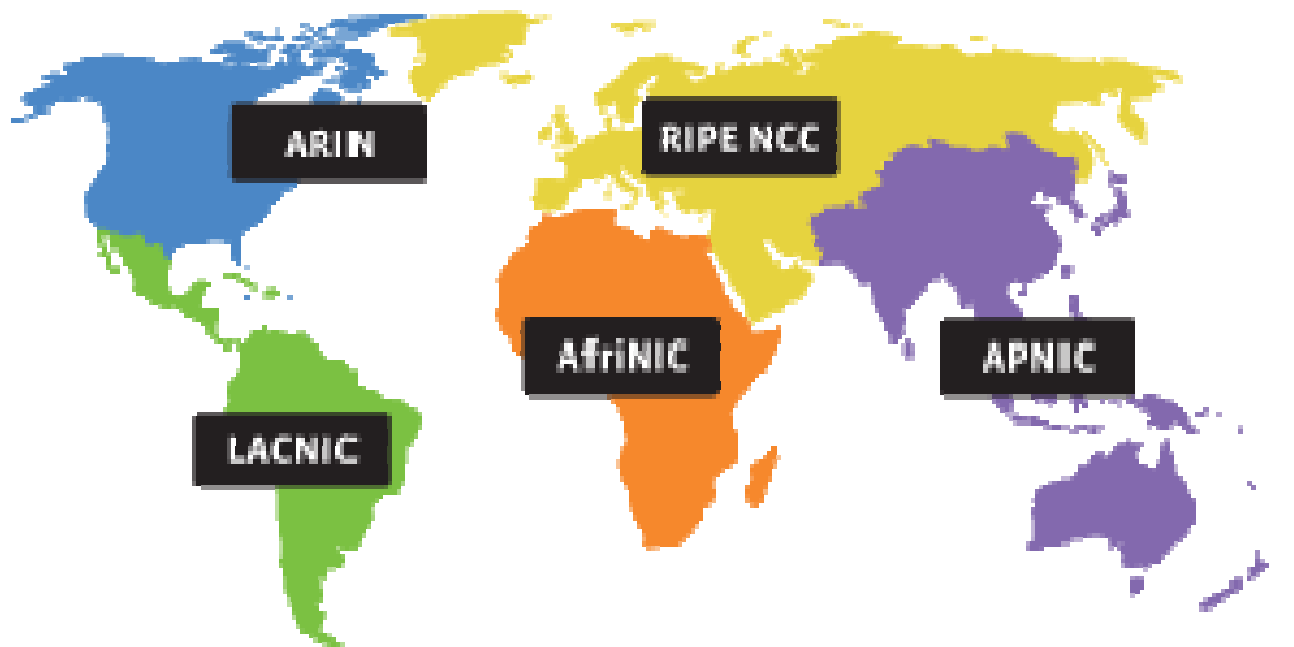


Who owns the root of trust? (1)



Internet Assigned Numbers Authority

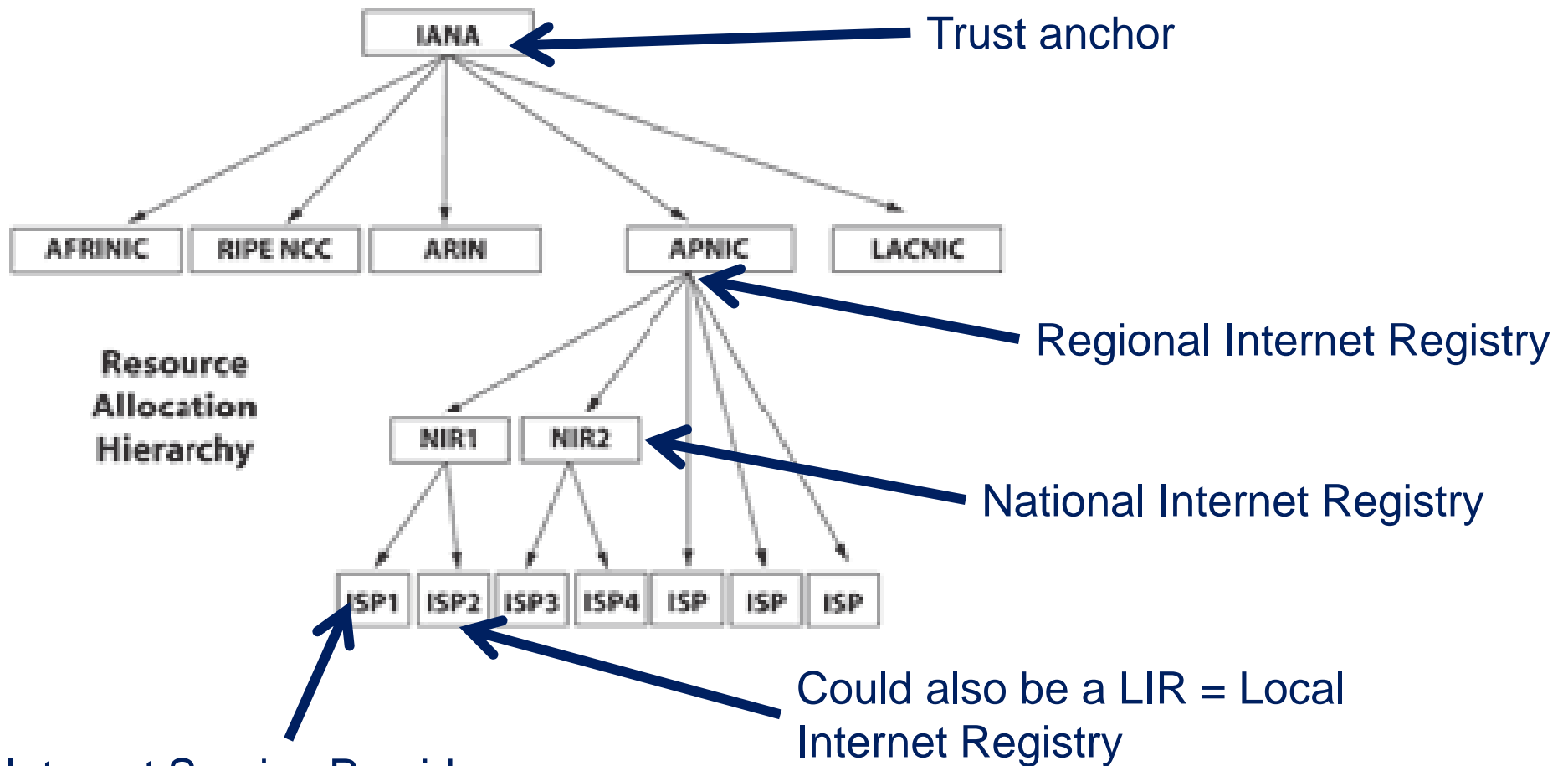
“IANA is responsible for global coordination of the Internet Protocol addressing systems, as well as the Autonomous System Numbers used for routing Internet traffic.”



<http://www.iana.org/numbers>



The entities involved in the certificate hierarchy



Internet Service Provider (e.g. AT&T), which could delegate further to one of its customers (e.g. Princeton)



Network Operators are distrustful of the RIRs

- Are the RIRs just using this as a cash grab?
- What if I (the network operator) forget to pay my RIR?
 - They revoke my certificate. My network is offline!
- What if the RIR is lazy, and has stale data?
 - My certificate expires. My network is offline!
- Before RPKI we had IRR (“internet route registries”)
 - Non-cryptographic way of providing some RPKI functionality
 - This didn’t work at all. The data there is totally stale.
 - Will RPKI be the same?

A history of stale data

The IRRs

- IRRs decentralized - ~55 IRRs currently
 - Operated by RIRs, operators, other, none authoritative
- Perception: data is largely unusable, insecure, stale - Do people ever actually delete IRR objects?
- Customer issues - don't understand or want to use IRRs, ISP's proxy
- Insecure IRR update models (++RIPE)
- Tools to configure based on IRR data, internal database - ISPs should have these functions fully automated
- Inter-IRR communications, which are trustworthy, how is this enumerated in deployed policy
- Timing issues, race conditions
- Full route policy enumeration
- Special case policies (e.g., more-specifics with blackhole communities)
- Use of IRRs cost money\$\$



Central control vs informal social trust model? (1)

“ the introduction of RPKI dramatically changes the existing **decentralized governance model** by linking resource allocation and routing.

And this change shapes the **incentives of the various organizations involved to adopt the technology.**

The issue is who has hierarchical control over whom?”

http://blog.internetgovernance.org/blog/_archives/2011/9/7/4894404.html



Central control vs informal social trust model? (2)

Masataka Ohta of Japan, made a case for ... a looser form of networked governance:

"Your and my ISPs," he claimed, "are loosely connected by a **chain of social trust relationships between adjacent ISPs**, which is why we can exchange packets over the Internet with reasonable security."

"The problem of PKI is that its **security socially depends** on a loose connection of **a chain of adjacent Certificate Authorities**. ...

Socially compromising a Certificate Authority in the network is as easy as socially compromising an ISP."

http://blog.internetgovernance.org/blog/_archives/2010/3/13/4479658.htm
|



Who owns the root of trust? (2)

[New IANA contract solicitation](#), posted November 10, 2011:

“The United States Department of Commerce (DoC), National Telecommunications and Information Administration (NTIA) intends to award a contract to maintain the continuity and stability of services related to certain interdependent Internet technical management functions, known collectively as the Internet Assigned Numbers Authority (IANA).”

A successful bidder ... must be a **wholly U.S. owned** and operated firm or university ... and organized under the laws of one of the 50 U.S. states. ... Any operations and activities can be inspected by U.S. government officials at any time.

...the "Internet user community" is included as an "interested and affected party" in section C.1.3. This means that the Contractor ... must develop a "close and constructive working relationship" with it, and that Internet users are given standing in regards to commenting ... on certain things...

http://blog.internetgovernance.org/blog/_archives/2011/11/16/4940638.html



Who owns the root of trust? (3)

The Internet Architecture Board supports the notion of a single trust anchor:

"The notion of having a certification hierarchy with multiple equally trusted roots may be appealing from a social and political perspective because of 'fairness' and 'equality' arguments. But that notion allows different organizations to make **inconsistent and conflicting assertions** about to whom a particular address block has been allocated. In the case of conflicting assertions, the conflict would need to be solved by each relying party, requiring each relying party to have their own security policy and the associated increased complexity. Such an approach does not provide any guarantee that the outcome would lead to a globally coherent view of which resources have been allocated to whom."

http://blog.internetgovernance.org/blog/_archives/2010/3/13/4479658.html



Who owns the root of trust? (4)

Multiple roots doesn't always work so well...



March 23, 2011 - 6:08pm | By [Peter Eckersley](#)

**Iranian hackers obtain fraudulent HTTPS certificates:
How close to a Web security meltdown did we get?**

On March 15th, an HTTPS/TLS [Certificate Authority](#) (CA) was tricked into issuing fraudulent certificates that posed a dire risk to Internet security. Based on currently available information, the incident got close to — but was not quite — an Internet-wide security meltdown.

Jake Applebaum: “If the CA cannot provide even a basic level of revocation, it's clearly irresponsible to ship that CA root in a browser. Browsers should give insecure CA keys an Internet Death Sentence rather than expose the users of the browsers to known problems.”

<https://www.eff.org/deeplinks/2011/03/iranian-hackers-obtain-fraudulent-https>



What about the National Internet Registries?

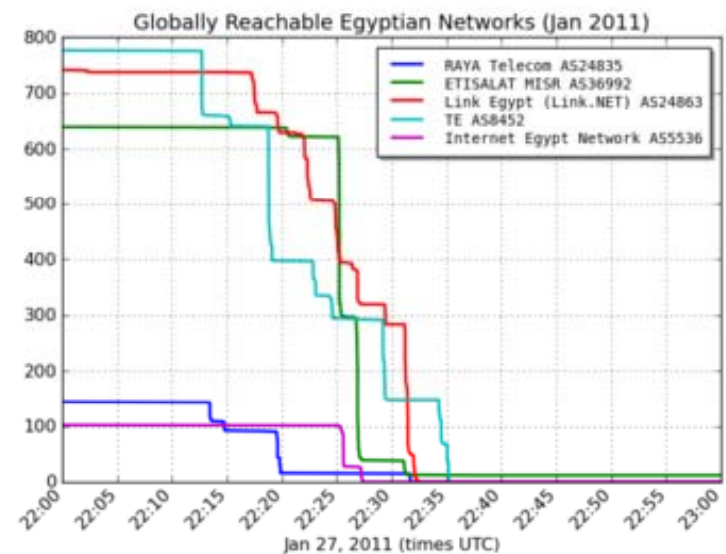
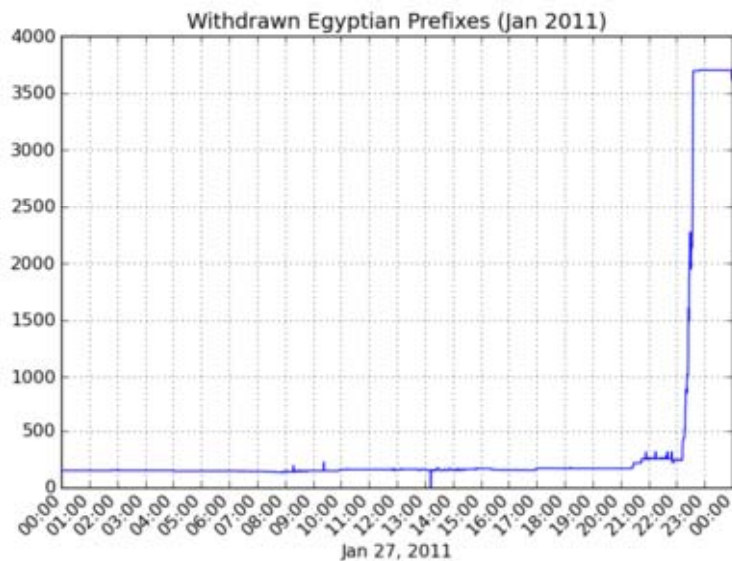
Each country can locally manages it's local certificates.

- What happens if they refuse to issue certs for ASes or IP addresses they don't like?
- Remember what happened in Egypt?

Egypt Leaves the Internet

By James Cowie on January 27, 2011 7:56 PM

<http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml>





Summary: Obstacles to deploying RPKI

Technical challenges?

- Keeping data fresh. Dealing with revocation
- Building a decentralized database.
- Backward compatibility
 - Will it make my network unreachable?
 - Will it make it harder to find good routes?

Political issues?

- Moving from “web-of-trust” to a centralized model?
- Who controls the trust anchor?
- Can nations use this for censorship?

