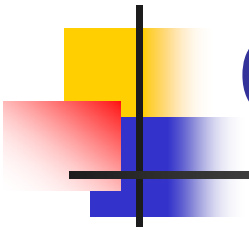
# Update on Resource Certification

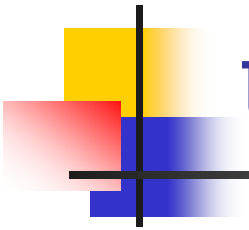
Geoff Huston, APNIC

Mark Kosters, ARIN

SSAC Meeting, March 2008



# On the Internet...



# there are many ways to be bad!

- Enlist a Bot army and mount multi-gigabit DOS attacks
  - Extortion leverage
- Port Scan for known exploits
  - General annoyance
- Spew spam
  - Yes, there are still gullible folk out there!
- Mount a fake web site attack
  - And lure victims
- Mount a routing attack
  - And bring down an entire service / region / country / global network!

cnet NEWS.com

Search:

Today on CNET | Reviews | News | Downloads | Tips & Tricks | CNET TV | Compare Prices

Business Tech | Cutting Edge | Green Tech | Wireless | Security | Media | Markets | Personal

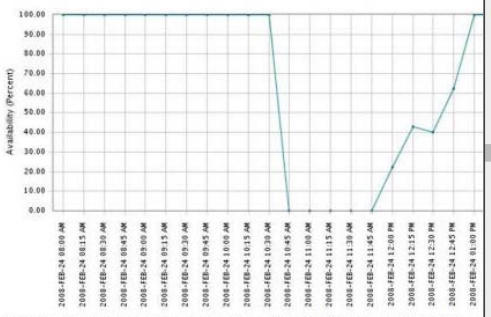
News Blog

Recent posts on technology, trends, and

February 25, 2008 2:30 PM PST

# How Pakistan knocked YouTube offline (and how to make s happens again)

Posted by Declan McCullagh




This graph that network-monitoring firm Keynote Systems provided to us availability of YouTube.com dropping dramatically from 100 percent to 0 hour. It didn't recover completely until two hours had elapsed.

(Credit: Keynote Systems)

A high-profile incident this weekend in which Pakistan's state-owned telecommunications company mar global Web highlights a long-standing security weakness in the way the Internet is managed.

After receiving a censorship order from the telecommunications ministry directing that YouTube.com b went even further. By accident or design, the company broadcast instructions worldwide claiming to be anyone trying to reach YouTube's range of Internet addresses.

The security weakness lies in why those false instructions, which took YouTube offline for two hours o routers around the globe. That's because Hong Kong-based PCCW, which provides the Internet link to the misleading broadcast--which is what most large providers in the United States and Europe do.

This is not a new problem. A network provider in Turkey once pretended to be the entire Internet, snarli Web sites unreachable. Con Edison accidentally hijacked the Internet addresses for Panix customers Omnimedia and the *New York Daily News*. Problems with errant broadcasts go back as far as 1997.

It's also not an infrequent problem. An automatically-updated list of suspicious broadcasts created by New Mexico shows apparent mischief--in the form of dubious claims to be the true destination for certs

bbc.co.uk

Home | TV | Radio | Talk | Where I Live | A-Z Index | Search

UK version | International version | About the versions | Low graphics | Accessibility help

BBC NEWS

WATCH LIVE BBC News 24

News services
Your news when you want it

News Front Page
World
UK
England
Northern Ireland
Scotland
Wales
Business
Politics
Health
Education
Science/Nature
Technology
Entertainment
Also in the news

Video and Audio

Have Your Say
Magazine
In Pictures
Country Profiles
Special Reports

RELATED BBC SITES
SPORT
WEATHER
CBBC NEWSROUND
ON THIS DAY
EDITORS' BLOG

Last Updated: Tuesday, 26 February 2008, 13:43 GMT

E-mail this to a friend | Printable version

# Pakistan lifts the ban on YouTube

**Pakistan's telecoms regulator has lifted the restrictions it imposed on video-sharing website YouTube.**

The Pakistan Telecommunications Authority has told internet service providers (ISPs) to restore access to the site, according to a spokeswoman.

Google, the owner of YouTube, confirmed service had been restored in Pakistan.

The attempt to block the site, reportedly because of a "blasphemous" video clip, caused a near global blackout of the site on Sunday.

A spokesman for YouTube told the BBC News website: "We are pleased to confirm that YouTube is again accessible in Pakistan."

It is reported that a trailer for a forthcoming film by Dutch lawmaker Geert Wilders, which portrays Islam in a negative light, was behind the restrictions.

Turkey and Thailand have in the past also banned access to the site

VIDEO AND AUDIO NEWS
How the YouTube block caused waves around the world
WATCH

SEE ALSO
- Pakistan blocks YouTube website 24 Feb 08 | South Asia
- Should governments block websites? 25 Feb 08 | Middle East
- Thai ban on YouTube website ends 31 Aug 07 | Asia-Pacific
- YouTube site 'blocked' in Morocco 29 May 07 | Africa
- Turkish court bans YouTube access 07 Mar 07 | Europe

RELATED INTERNET LINKS
- YouTube

The BBC is not responsible for the content of external internet sites

TOP TECHNOLOGY STORIES
- Wiki boss 'edited for donation'

The ban wa
Pakistan on
the BBC Ne
technology
Waters, sai
citizens fror
it was belie
"hijacked" t
address of
site.

Those detai
on to the cc
Pakistan at
a different

But the det
internet by
YouTube wa

The block o
lifted once
of the issue
engineers.

The block on the servers was lifted once PCCW had been told of the issue by YouTube engineers.

A statement from Google said that the problems lasted for "about two hours".

"Traffic to YouTube was routed according to erroneous internet protocols, and many users around the world could not access our site," it said.

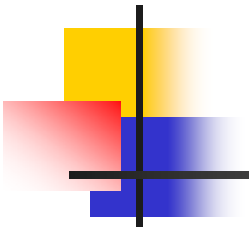
A leading net professional told BBC News: "This was probably a simple mistake by an engineer at Pakistan Telecom. There's nothing to suggest this was malicious."

IP hijacking [illegible] site's unique address by corrupting the internet's routing tables, which direct the flow of data around the world.

**"The fact YouTube is back in action makes me revise my thoughts on the clash between governments and freedom of speech"**

Rory Cellan-Jones

Read Rory's blog



# If I were bad (and greedy)…

I’d attack the routing system

- Through routing I’d attack the DNS
- Through the DNS I’d lure traffic through an interceptor web server
- And be able to quietly collect user’s details

# If I were really bad (and evil)…

I'd attack the routing system

- Through routing I'd attack:
  - the route registry server system
  - the DNS root system
  - trust anchors for TLS and browser certificates
  - isolate critical public servers and resources
  - overwhelm the routing system with spurious information
  - generate a massive routing overload situation to bring down entire regional routing domains
- And see if I could bring the network to a complete chaotic halt

# What's the base problem here?

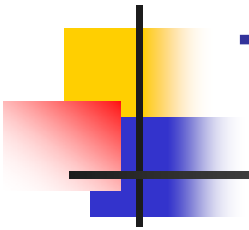
- Routing is built on sloppy mutual trust models
- Routing auditing is a low value activity that noone can perform with any level of thoroughness
- We have grown used to lousy solutions and institutionalized lying in the routing system

- It's a tragedy of the commons situation:
  - Nobody can single-handedly apply rigorous tests on the routing system
  - And the lowest common denominator approach is to apply no integrity tests at all
  - All trust and no defence

# So we need routing security

like we need motherhood, clean air and clean water

- But what does this “need” mean beyond various mantras, noble intentions and vague generalities about public safety and benefit?
  - Who wants to pay for decent security?
  - What’s the business drivers for effective security?
  - How do you avoid diversions into security pantomimes and functionless veneers?
- Can you make decent security and also support “better, faster and cheaper” networked services?



# Threat Model

Understanding routing threats:

- What might happen?
- What are the likely consequences?
- What's my liability here?
- How can the consequences be mitigated?
- What's the set of cost tradeoffs?
- Does the threat and its consequences justify the cost of implementing a specific security response?

# Threat Response

- Collective vs unilateral responses to security threats
  - Should I trust noone else and solve this myself?
  - How much duplication of effort is entailed?
  - Is the threat a shared assessment?
  - Can we pool our resources and work together on a common threat model?
  - What tools do we need?
  - Are there beneficial externalities that are also generated?
  - Who wants to work with me?
  - What's the framework for collective action?

When will you stop asking all these bloody annoying questions and just tell me what to do!

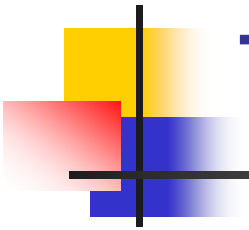
# Routing Security

Protecting **routing protocols** and their operation

- Threat model:
  - Compromise the topology discovery / reachability operation of the routing protocol
  - Disrupt the operation of the routing protocol

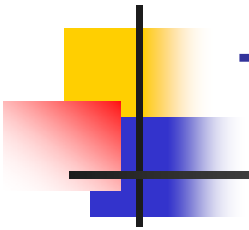
Protecting the **protocol payload**

- Threat model:
  - Insert corrupted address information into your network's routing tables
  - Insert corrupt reachability information into your network's forwarding tables



# Threats

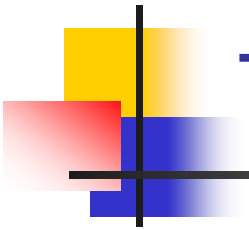
- Corrupting the routers' forwarding tables can result in:
  - Misdirecting traffic (subversion, denial of service, third party inspection, passing off)
  - Dropping traffic (denial of service, compound attacks)
  - Adding false addresses into the routing system (support compound attacks)
  - Isolating or removing the router from the network



# The Current State of Routing Security

What we have had for many years is a relatively insecure inter-domain routing system based on mutual trust that is vulnerable to various forms of disruption and subversion

And it appears that the operational practice of bogon filters and piecemeal use of routing policy databases are not entirely robust forms of defense against these vulnerabilities

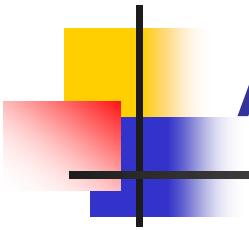


# The Current State of Routing Security

Is pretty bad

- This is a commodity industry that is not really coping with today's level of abuse and attack
  - Incomplete understanding
  - Inadequate resources and tools
  - Inadequate information
  - Inadequate expertise and experience

Can we do better?

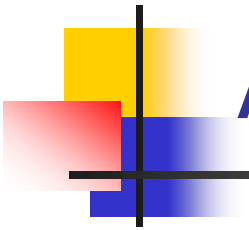


# Address and Routing Security

The basic routing payload security questions that need to be answered are:

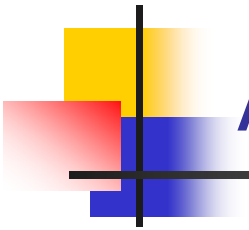
- Is this a **valid address prefix**?
- **Who** injected this address prefix into the network?
- Did they have the necessary **credentials** to inject this address prefix?
- Is the forwarding path to reach this address prefix an **acceptable representation** of the network's forwarding state?

Can these questions be answered reliably, cheaply and quickly?



# A Foundation for Routing Security

- The use of authenticatable attestations to allow automated validation of:
  - the authenticity of the route object being advertised
  - authenticity of the origin AS
  - the binding of the origin AS to the route object
- Such attestations used to provide a cost effective method of validating routing requests
  - as compared to the today's state of the art based on techniques of vague trust and random whois data mining



# A Starting Point for Routing Security

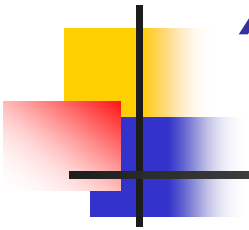
Adoption of some basic security functions into the Internet's routing domain:

- Injection of reliable trustable data
  - A Resource PKI as the base of validation of network data
- Explicit verifiable mechanisms for integrity of data distribution
  - Adoption of some form of certified authorization mechanism to support validation of credentials associated with address and routing information

# A Starting Point

- Certification of the “Right-of-Use” of IP Addresses and AS numbers as a linked attribute of the Internet’s number resource allocation and distribution framework

# X.509 Extensions for IP Addresses



- RFC3779 defines extension to the X.509 certificate format for IP addresses & AS number
- The extension binds a list of IP address blocks and AS numbers to the subject of a certificate
- These extensions may be used to convey the issuer's authorization of the subject for exclusive use of the IP addresses and autonomous system identifiers contained in the certificate extension
- The extension is defined as a critical extension
  - Validation includes the requirement that the Issuer's certificate extension **must** encompass the resource block described in the extension of the certificated being validated

# What is being Certified

For example:

APNIC (the “Issuer”) certifies that:

the certificate “Subject”

whose public key is contained in the certificate

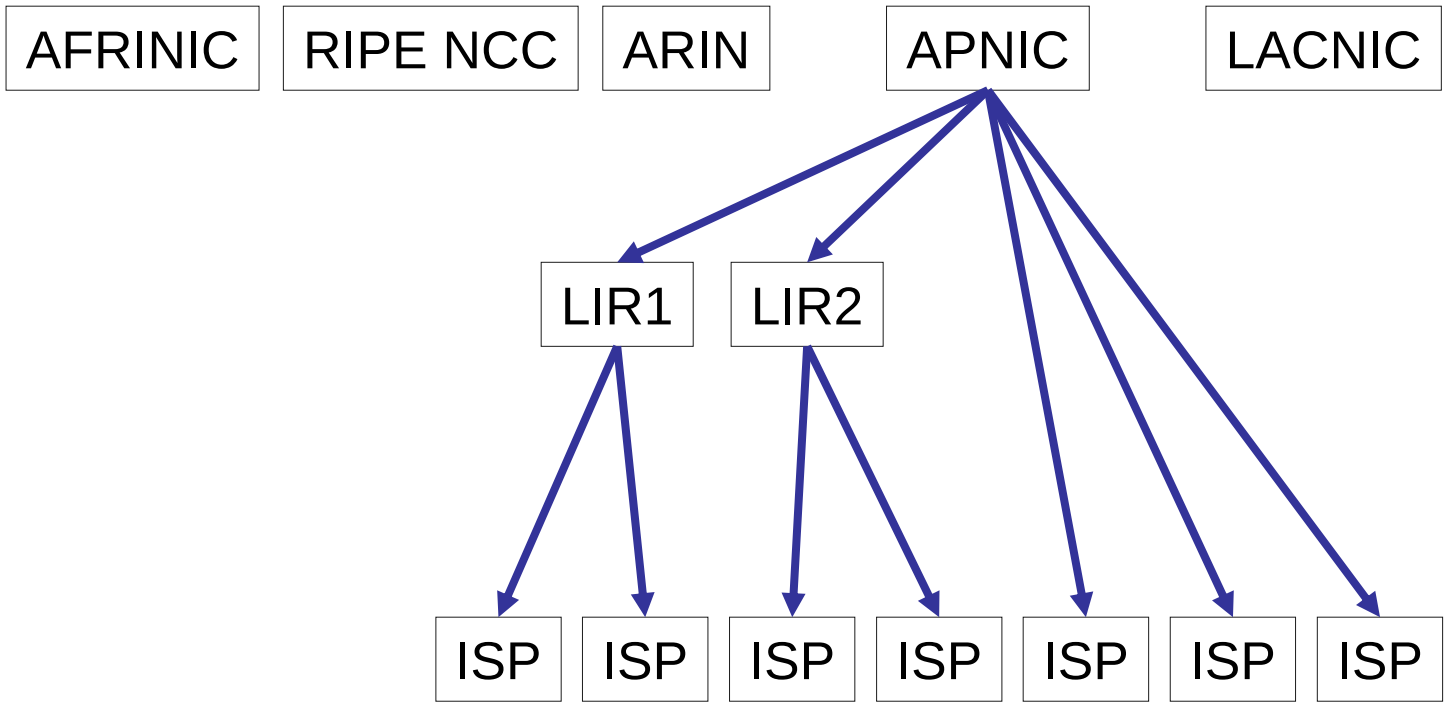
is the current controller of a set of IP address and AS resources

that are listed in the certificate extension

APNIC does NOT certify the identity of the subject, nor their good (or evil) intentions!

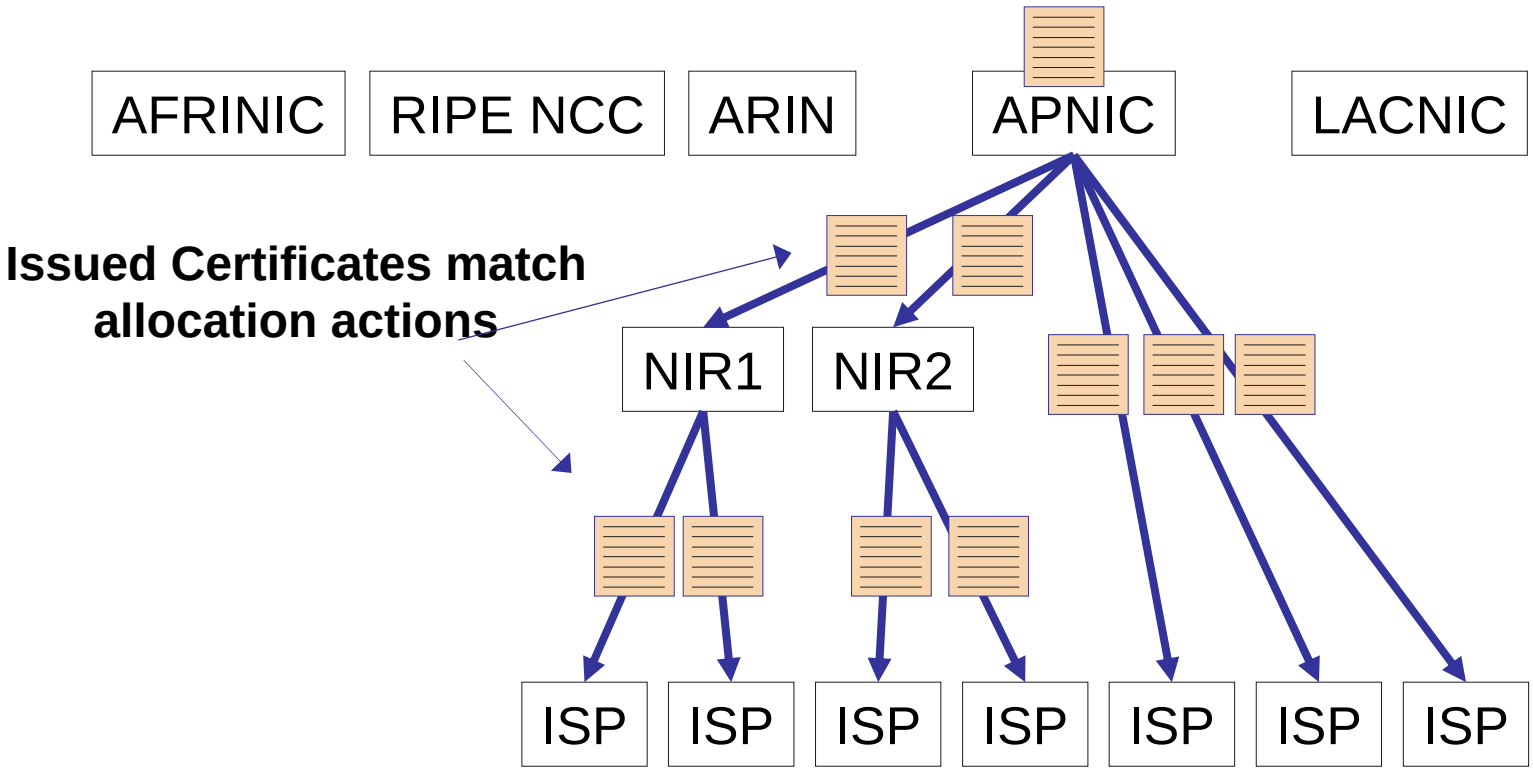
# Resource Certificates

Resource
Allocation
Hierarchy



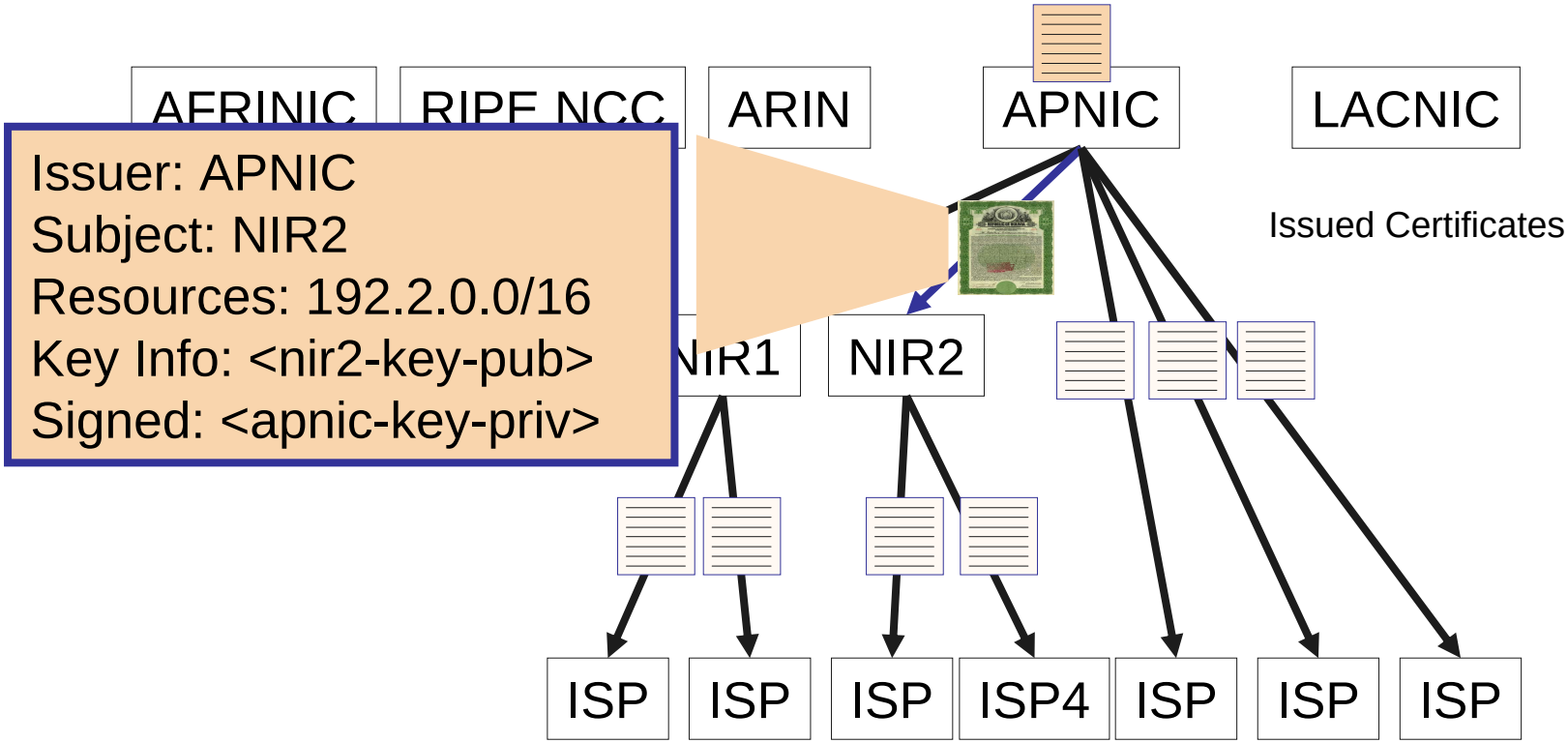
# Resource Certificates

Resource
Allocation
Hierarchy



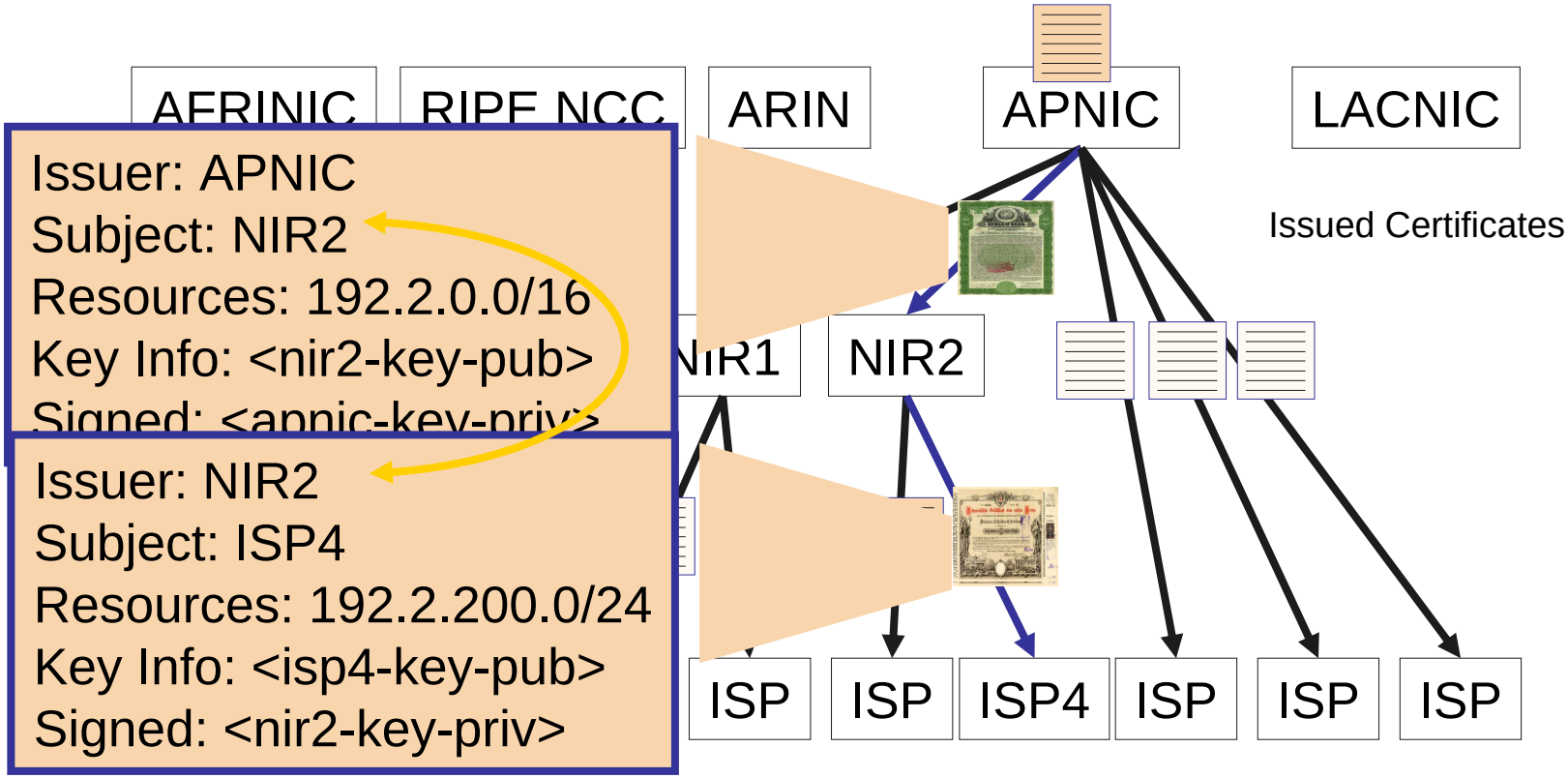
# Resource Certificates

Resource
Allocation
Hierarchy



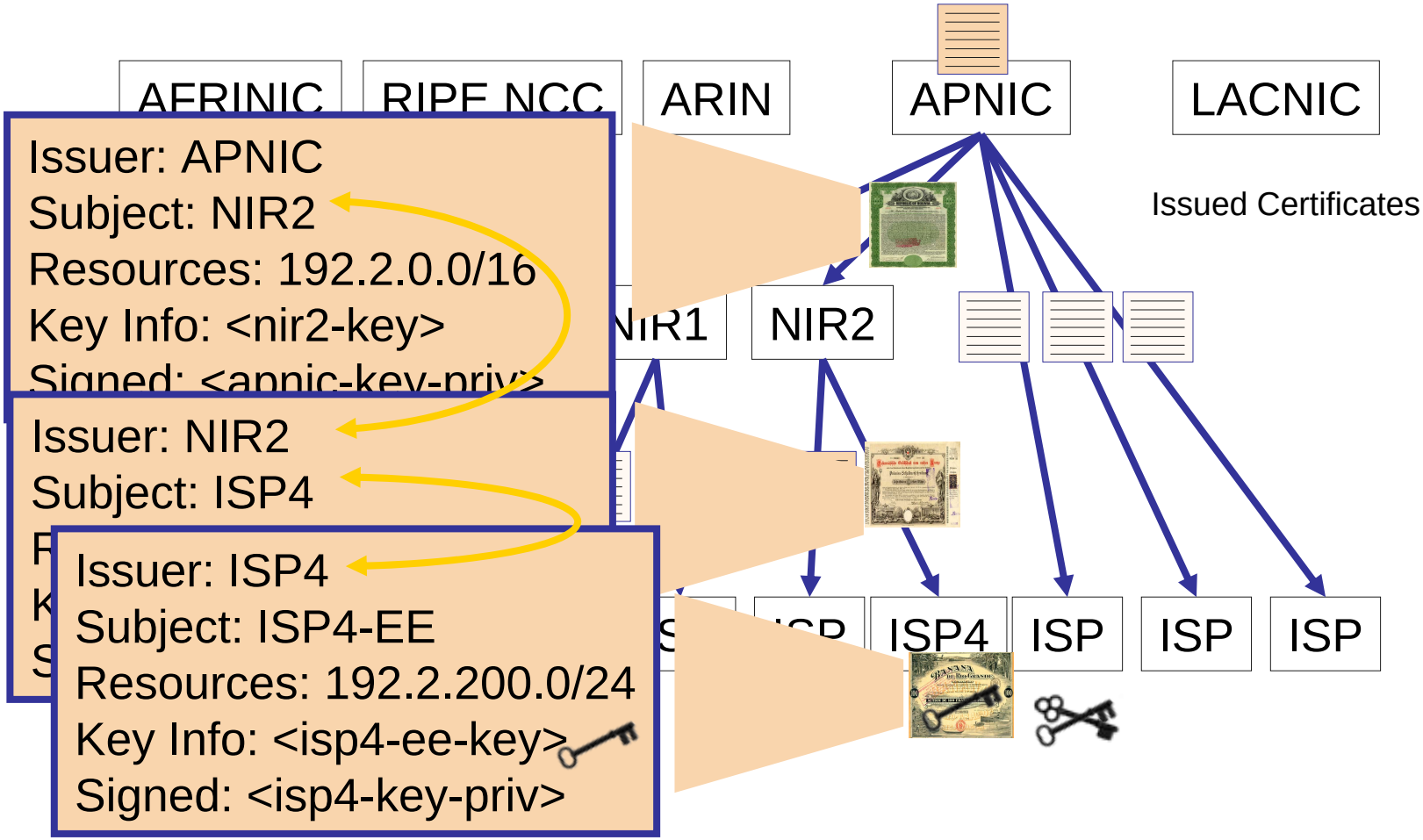
# Resource Certificates

Resource
Allocation
Hierarchy



# Resource Certificates

Resource
Allocation
Hierarchy

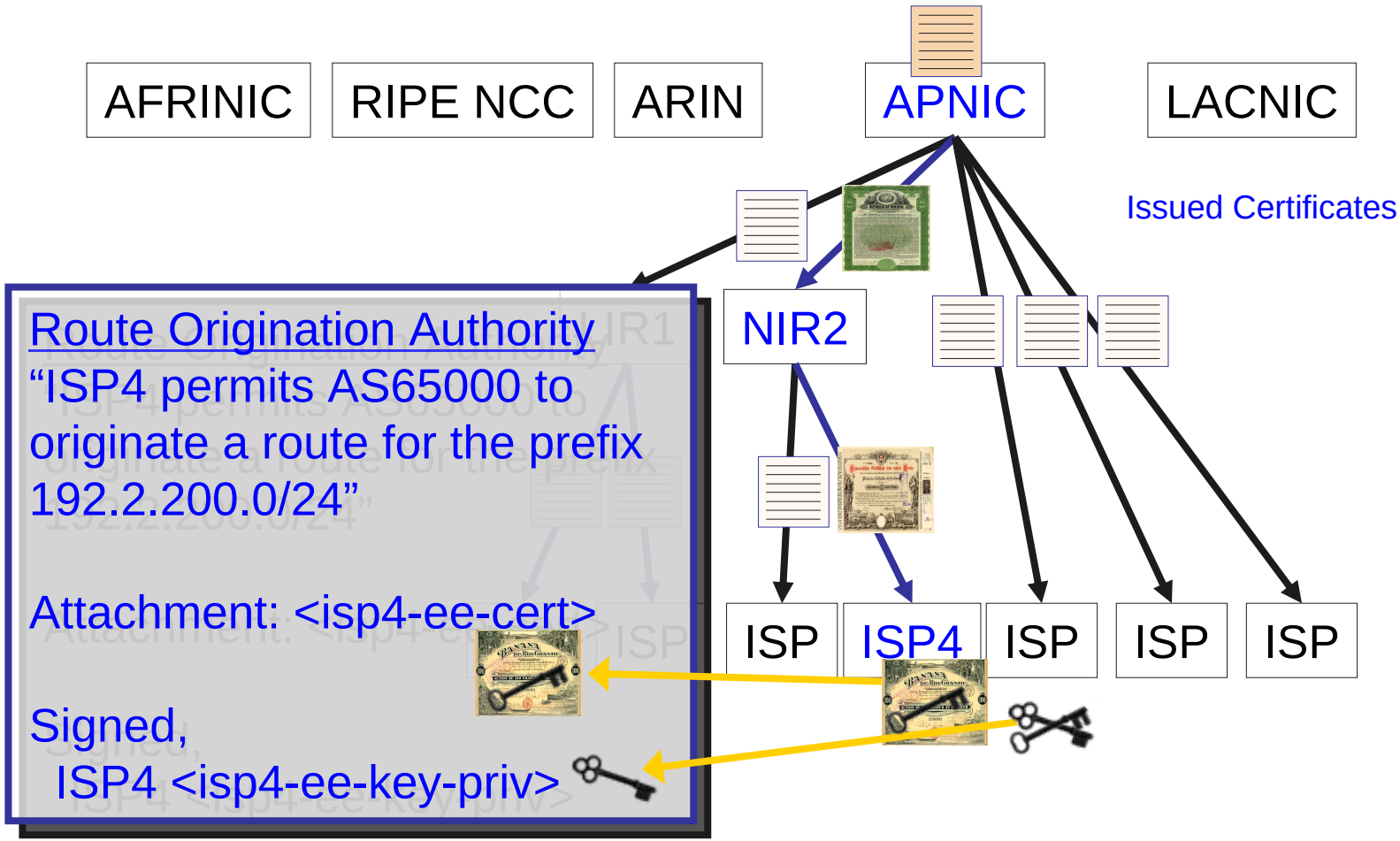


# What could you do with Resource Certificates?

- You could sign routing origination authorities or routing requests with your private key, providing an authority for an AS to originate a route for the named prefix. A Relying Party can validate this authority in the RPKI
- You could use the private key to sign routing information in an Internet Route Registry
- You could attach a digital signature to a protocol element in a routing protocol
- You could issue signed derivative certificates for any sub-allocations of resources

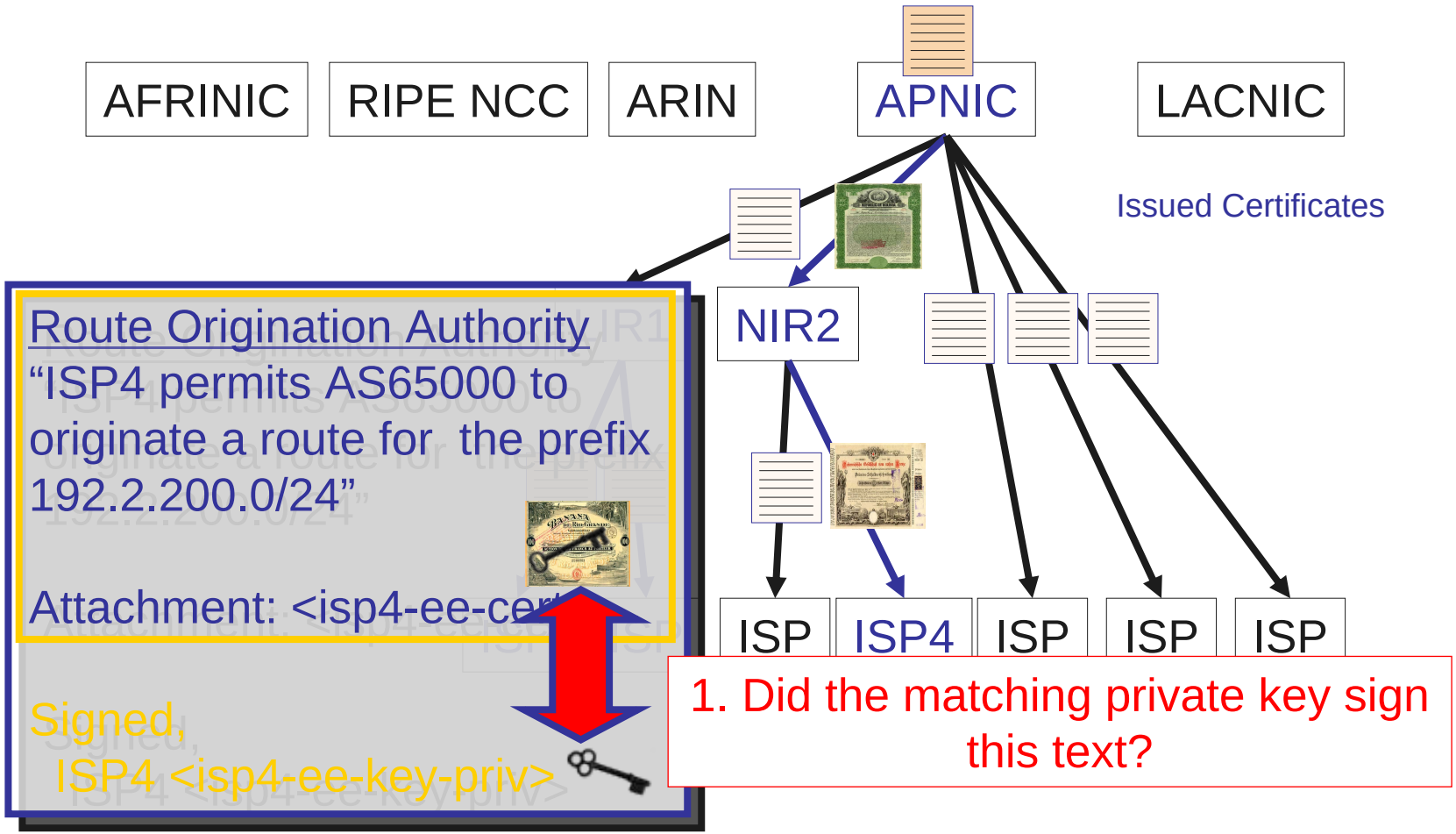
# Signed Objects

Resource
Allocation
Hierarchy



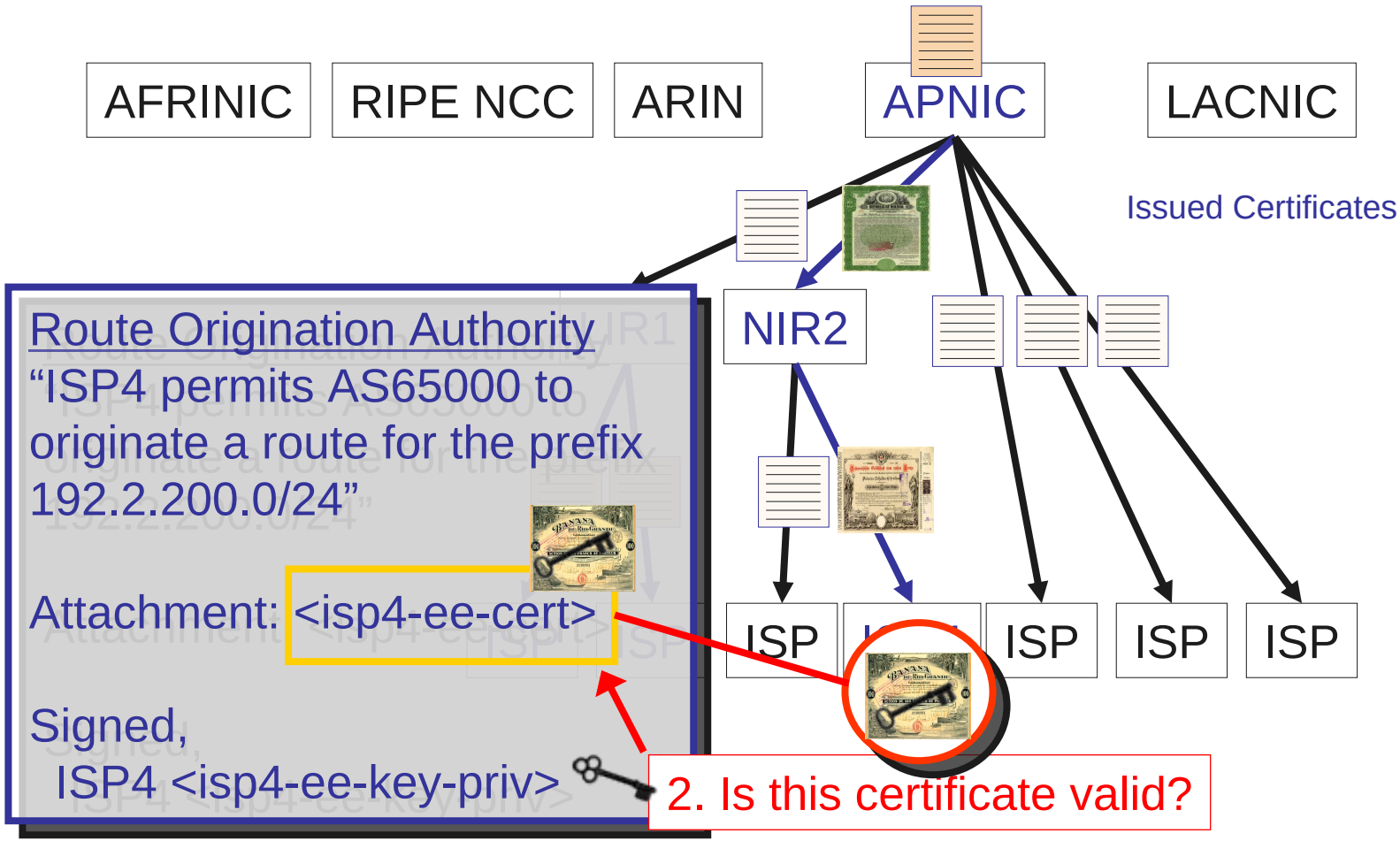
# Signed Object Validation

Resource
Allocation
Hierarchy



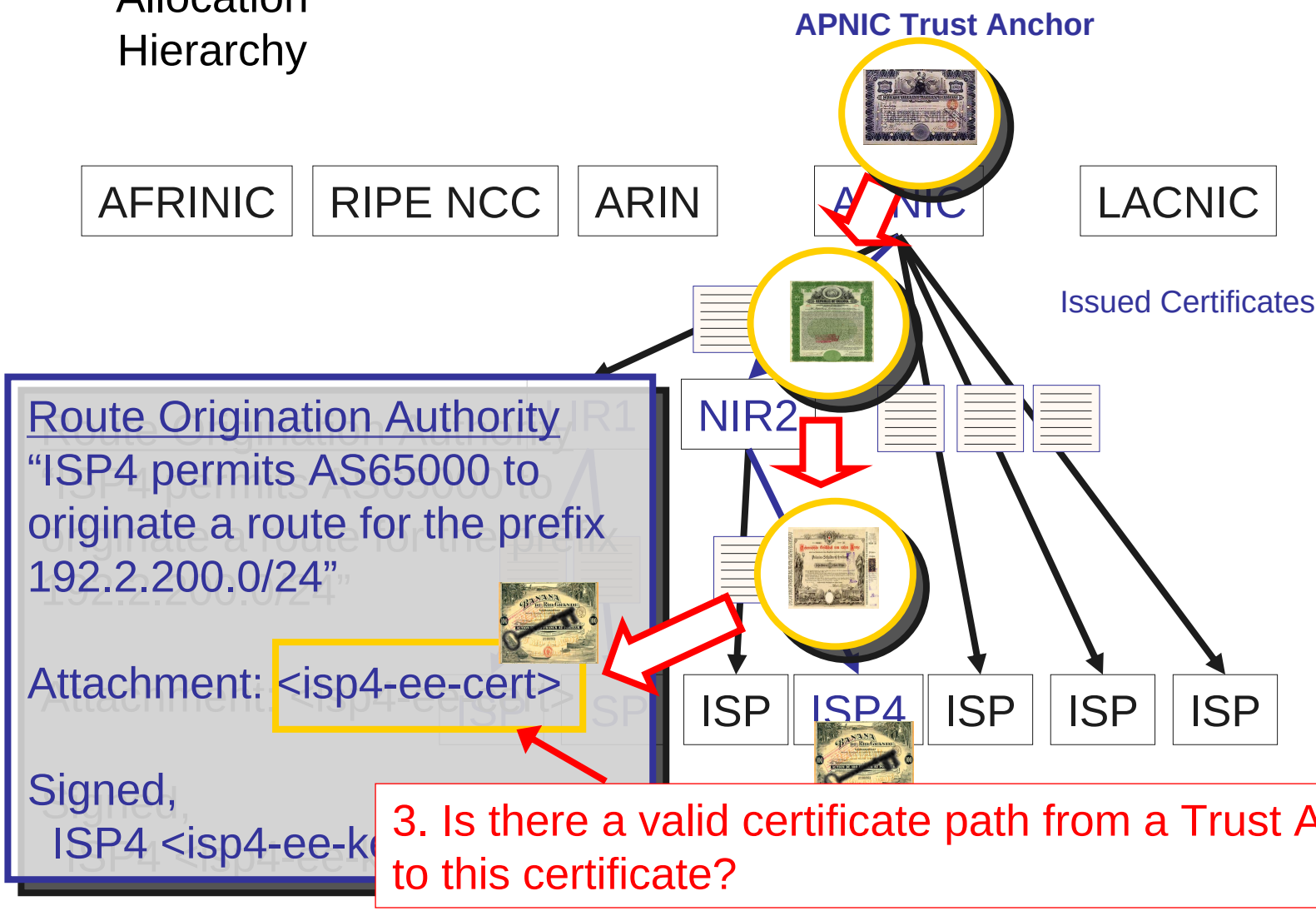
# Signed Object Validation

Resource
Allocation
Hierarchy



# Signed Object Validation

Resource Allocation Hierarchy



# Signed Object Validation

Resource
Allocation
Hierarchy

AFRINIC | RIPE NCC | A

Route Origination Authority

"ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24"

Attachment: <isp4-ee-cert>

Signed,
ISP4 <isp4-ee-key-priv>

Validation Outcomes

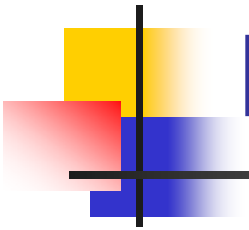
1. ISP4 authorized this Authority document
2. 192.2.200.0/24 is a **valid** address, derived from an APNIC allocation
3. ISP4 holds a current right-of-use of 192.2 200.0/24
4. A route object, where AS65000 originates an advertisement for the address prefix 192.2.200.0/24, has the explicit authority of ISP4, who is the current holder of this address prefix

# Managing Resource Certificates

- Resource Holders ‘enroll’ for certificates using existing trusted relationship between issuer and holder
- Exchange of credentials to establish a secure path between issuer and subject
- Subject and Issuer each operate instances of an “RPKI Engine” to manage certificate issuance actions
- Certificate Issuance reflects the current state of the issuer’s allocation database

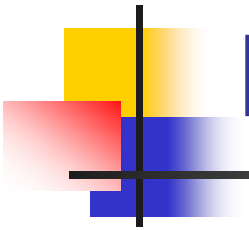
# Managing Resource Certificates

- Certificate management is an automated process driven by the issuer's allocation database state
- Uses a distributed publication repository system to allow:
  - CA's to publish certificates and CRLs
  - EE's to publish signed objects
- Relying Parties could maintain a local cache of the publication repository framework to allow local validation operations to be performed efficiently



# Progress

- Specifications submitted to the SIDR WG of the IETF:
  - Specification of a profile for Resource certificates
  - Specification of the distributed publication repository framework
  - Specification of the architecture of the RPKI
  - Specification of profiles for Route Origination Authorization objects (ROAs) and Bogon Origination Attestation objects (BOAs)
  - Specification of the Issuer / Subject resource certificate provisioning protocol



# Progress

- Implementation Progress
  - Four independent implementation efforts for various aspects of the RPKI are underway at present
  - Tools for Resource Certificate management
    - Requests, Issuance, Revocation, Validation
  - Issuer / Subject certificate provisioning protocol
  - Functional RPKI Engine instance for an RIR integrated into one RIR's production environment
  - Relying Party local cache management
  - RPKI validation tools

# Intended Objectives

- Create underlying framework for route security measures
- Assist ISP business process accuracy with Peering and Customer Configuration tool support
- Improve the integrity of published data through the signing and verification capability in Whois, IRR and similar

# What this does NOT do

- Compete with sBGP, soBGP, pgBGP, ... proposals
  - It is intended to provide a robust validation framework that supports the operation of such proposals that intend to secure the operation of the BGP protocol
- Insert another critical point of vulnerability into the Internet
  - No intention of defining a framework of certificate-enforced compliance as a precursor to network reachability
  - Interpretation of validation outcomes is a local policy preference outcome

# Current Activity

- ARIN
  - Working through ISC and PSG.NET for code and design work
  - Engine to be placed in the public domain
  - Hope to have pilot service up to test by the end of the year

# Current Activity (cont)

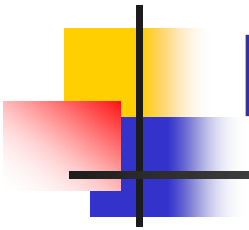
- APNIC
  - Has a working RPKI CA placed into its production platform (Feb 2008)
  - In house development of Perl based implementation of RPKI engine largely complete, with Perl interface to OpenSSL libraries, to be published as an open source software suite
  - Working on RPKI digital signature services for APNIC clients for for mid-2008

# Current Activity (cont)

- BBN
  - Resource certificate validation engine (java implementation)
- RIPE NCC
  - Business Procedure Modelling
  - RPSL Signatures

# Next (Technical) Steps

- Tools for ‘hosted’ RPKI services
  - Allow an ISP or an LIR to outsource Resource Certificate management services to an external agency
- Tools to manage attestation and authority generation and signing for end entities
- Relying Party tools to assist in validation functions
- Tools to support RIR functions
- Addition of digital signatures to IRR objects
- Specification of use of RPKI within the routing system



# References

- IETF SIDR Working Group
  - http://tools.ietf.org/wg/sidr/
- Working project documentation at:
  - http://mirin.apnic.net/resourcecerts/wiki/index.php/Main_Page
- ISC (funded by ARIN) subversion reference at:
  - http://subvert-rpki.hactrn.net/

# Questions?