



APCERT 2009 - Kaohsiung

# IP ADDRESS AND ASN CERTIFICATION TO IMPROVE ROUTING SECURITY

Sanjaya, APNIC Services Area Manager

# RESOURCE CERTIFICATION

# Resource Certificates



- X.509 certificates with IP Address and AS Number extensions (RFC3779)
- This changes the semantics of a certificate from the conventional notion of an identifying document (such as a passport) into a rights holder (such as a bearer bond)

# A Resource Certificate

- The holder of the corresponding private key has a right-of-use over the resources listed in this certificate
- CA Certificate:
  - The right-of-use holder can issue subordinate certificates (i.e. act as a local number registry and issue right-of-use certificates)
- EE Certificate
  - The right-of-use holder can generate digital signatures but cannot issue subordinate certificates (i.e. end user)

# Validating Resource Certificates

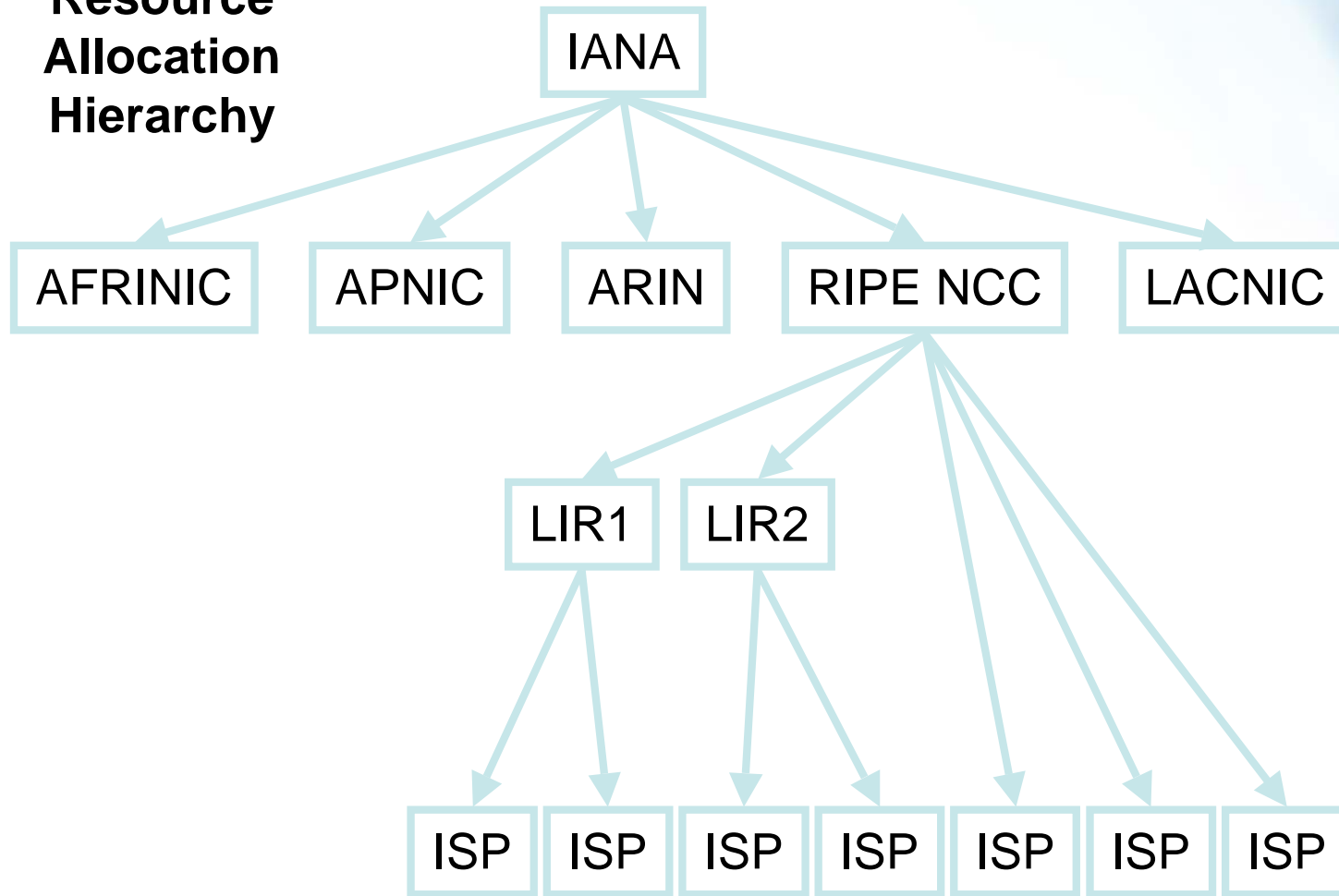
- Same validation task as conventional certificates, with one additional validation check:
  - The resources listed in a certificate must be a subset of the resources listed in the certificate referenced in the certificate's AIA field
- Change in validation semantics
  - From: Is this the key of the entity named "X"
  - To: Is this the key of the entity who holds the current right-of-use for IP address "X"

# Resource Certificate PKI

- Intended for Public Use IP resources
- Hierarchical PKI
- Precisely follows the resource allocation framework
  - Each registry in the allocation hierarchy is a CA
  - Each resource allocation is described in a Resource Certificate
- Trust Anchor is under discussion
  - Relying party to choose

# Resource Certificates

**Resource  
Allocation  
Hierarchy**



# Potential Uses of Resource Certificates



- Securing Whois objects
- Securing Internet Routing Registry objects
- Secure Routing
- Facilitating Resource Transfer functions
- Source address validation mechanism

# HOW CAN RESOURCE CERTIFICATES BE USED TO SECURE ROUTING?

Six worst Internet routing attacks - Network World - Internet Explorer provided by Dell

http://www.networkworld.com/news/2009/011509-bgp-attacks.html

Google

Six worst Internet routing attacks - Network World

Take a minute to **save millions in vendor lock-in costs.**  
 Watch our *Choice & Flexibility* video now →

**Juniper**  
 NETWORKS

**NETWORKWORLD** News | Blogs & Columns | Subscriptions | Videos | Events | More

Search

Security | LANs & WANs | VoIP | Infrastructure Mgmt | Wireless | Software | Data Center | SMB | Careers | Toolshed | Communities

Anti-Malware | Compliance & Regulation | Desktop Firewall / Host IPS | Enterprise Firewall / UTM | IDS / IPS | NAC | Security Management | Whitepapers | Webcasts

## Six worst Internet routing attacks

How YouTube, Yahoo and others fell prey to router incidents and accidents

By Carolyn Duffy Marsan, Network World, 01/15/2009

Share/Email | Buzz up! | 1 Comment | Print | Toolshed - IT A&A

Here's our list of the biggest security incidents involving the Internet's core routing protocol, the Border Gateway Protocol. Some of these incidents were attacks; others were accidental misconfigurations. But all of them disrupted traffic to Web sites or entire networks because of incorrect routing messages being propagated across the Internet through BGP. (Read the latest on [U.S. government efforts to secure BGP](#), and about [four open source BGP tools](#).)

### Pakistan Telecom blocks YouTube

In February 2008, [Pakistan Telecom](#) inadvertently [brought down](#) the entire [YouTube](#) site worldwide for two hours as it was attempting to restrict local access to the site. When Pakistan Telecom tried to filter access to YouTube, it sent new routing information via BGP to PCCW, an ISP in Hong Kong that propagated the false routing information across the Internet.

### ICANN puts root server at risk

The Internet Corporation for Assigned Names and Numbers (ICANN) [screwed up](#) in November 2007 when it renumbered the DNS root server "I" that it

File Integrity Monitoring: Secure Your Virtual and Physical IT Environments : Download now

Advertisement

Think you're protected?  
**THINK AGAIN.**

Get the *Outthink the Threat* eBook now ▶

SEE WHERE MALWARE IS MAKING HEADLINES

**TREND MICRO**  
 Securing Your Web World

### Most Read

- 40% of geeks surveyed really work fewer than ... say what?
- Juniper's answer to Cisco in the data center: Stratus Project
- Gmail chat invaded by phishing scam
- Microsoft has big growth plans even as economy limps
- Five fantastic open source tools for Windows admins

Internet | Protected Mode: On | 100%

## The Problem

- How do you check that use of Internet resources is legitimate?
  - “I’m multi-homed. Please advertise my /24”
  - “A spammer has hijacked 123.456.100.0/23. Please null route them.”
  - “That’s funny, I didn’t think that YouTube was based in Pakistan... Should AS123 be allowed to advertise their prefix?”
  - ...

# Address and Routing Security



- The (very) basic routing security questions that need to be answered are:
  - Is this a **valid** address prefix?

## **Valid:**

That the prefix has been allocated through the address distribution framework, and that this allocation sequence can be demonstrated and validated

# Address and Routing Security



- The (very) basic routing security questions that need to be answered are:
  - Is this a **valid** address prefix?
  - **Who** advertised this address prefix into the network?

## **Who:**

The route originator, identified by the origin AS of the corresponding route object. The originating AS also should be **valid.**

# Address and Routing Security



- The (very) basic routing security questions that need to be answered are:
  - Is this a **valid** address prefix?
  - **Who** advertised this address prefix into the network?
  - Did they have the necessary **credentials** to advertise this address prefix?

## **Credentials:**

Can a link be established between the address holder and the route originator such that the address holder has explicitly authorized the originating AS?

# Address and Routing Security



- The (very) basic routing security questions that need to be answered are:
  - Is this a **valid** address prefix?
  - **Who** advertised this address prefix into the network?
  - Did they have the necessary **credentials** to advertise this address prefix?
  - Is the advertised **path authentic**?

## An **authentic path**:

A sequence of valid ASs that represents a transit path from the current location to the prefix **and/or** A sequence of valid ASs that represents the path of the routing update message

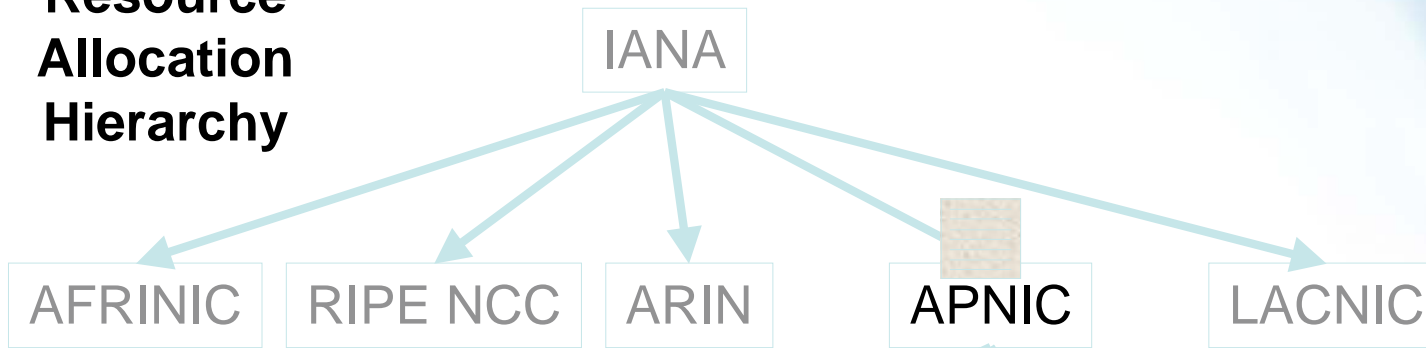
# Signed Attestations Examples



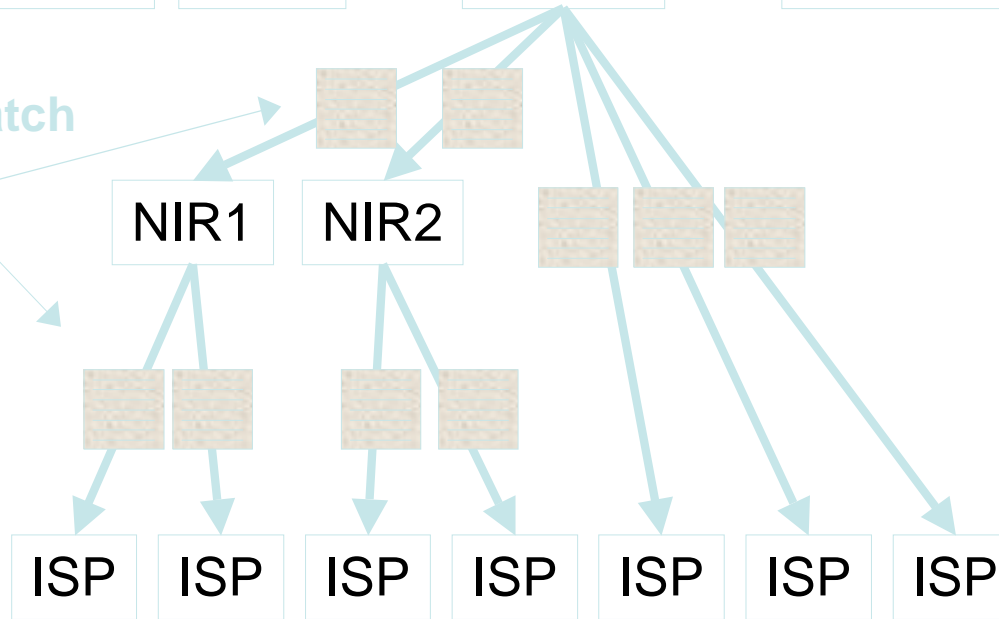
- Route Origin Authorizations (ROA)
  - “I allow AS123 to announce prefix 10.0.0.0/8”, signed the holder of 10.0.0.0/8
- Bogon Origin Attestation (BOA)
  - “I attest that 10.10.10.0/24 and AS456 should never be announced”, signed the holder of 10.10.10.0/24 and AS456
- AS Adjacency Attestation Objects (AAO)
  - “I attest that AS456 is adjacent to AS123 and AS789”, signed the holder of AS456
- Other signed data

# Resource Certificates

## Resource Allocation Hierarchy

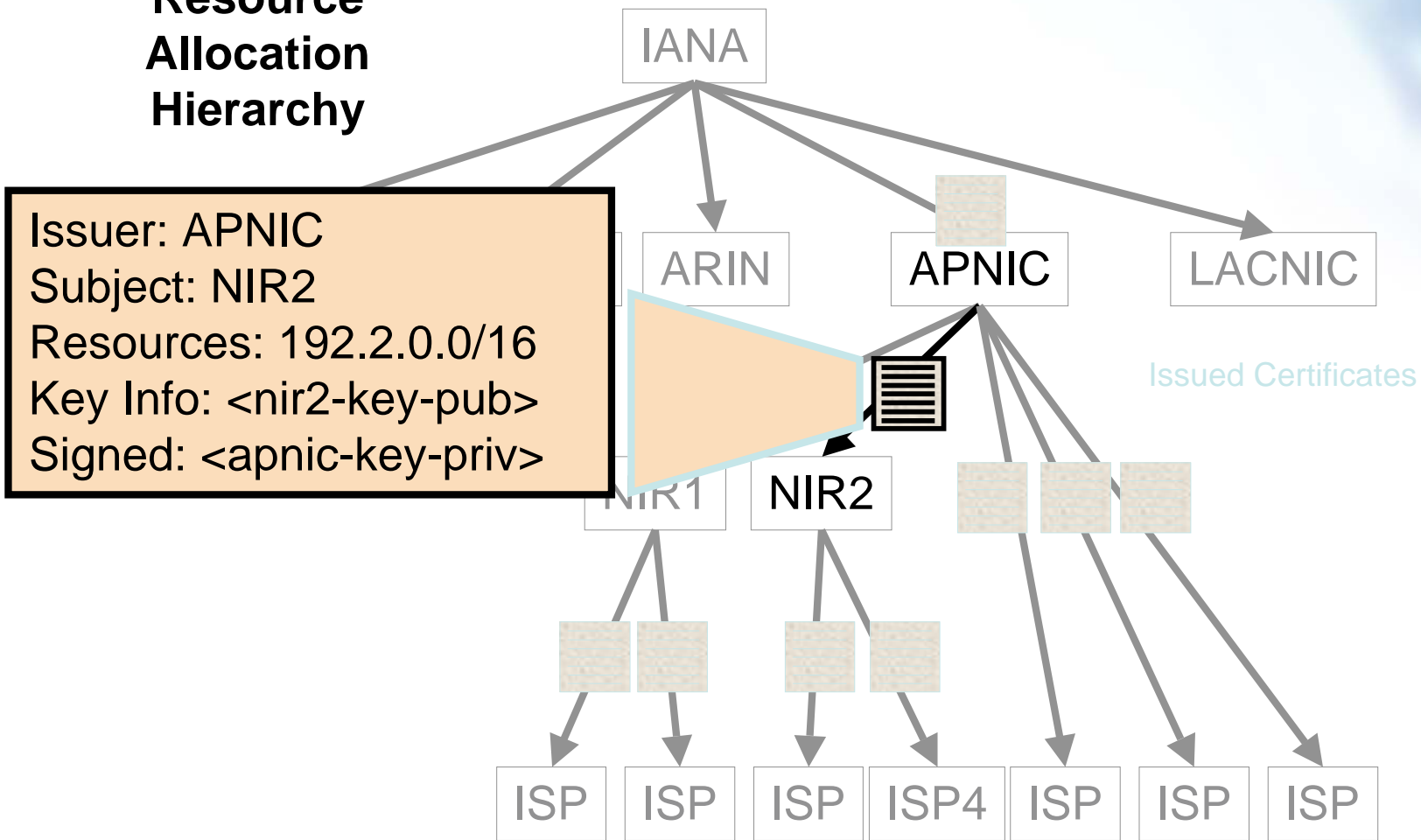


Issued Certificates match allocation actions



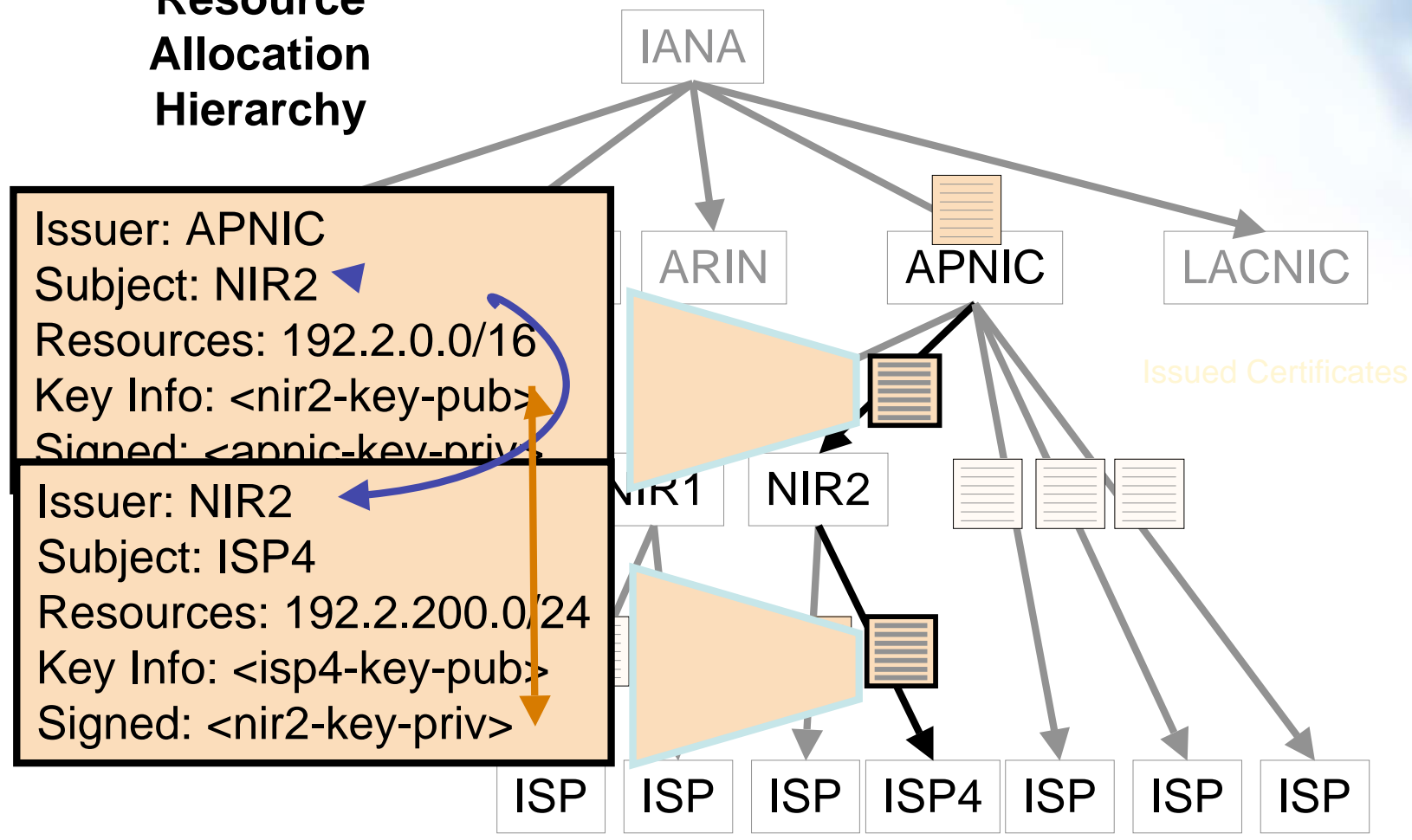
# Resource Certificates

## Resource Allocation Hierarchy



# Resource Certificates

## Resource Allocation Hierarchy



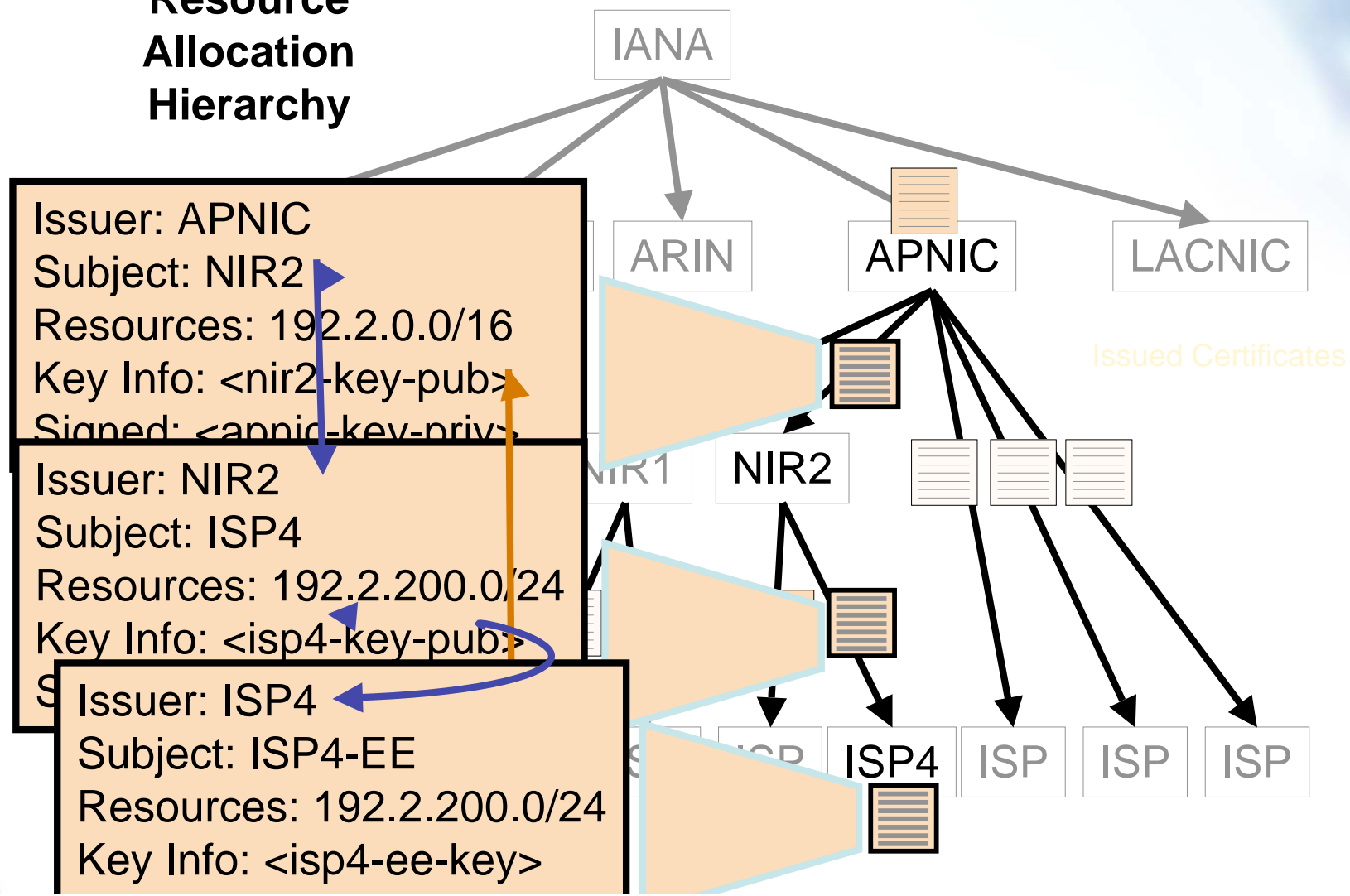
Issuer: APNIC  
 Subject: NIR2  
 Resources: 192.2.0.0/16  
 Key Info: <nir2-key-pub>  
 Signed: <apnic-key-priv>

---

Issuer: NIR2  
 Subject: ISP4  
 Resources: 192.2.200.0/24  
 Key Info: <isp4-key-pub>  
 Signed: <nir2-key-priv>

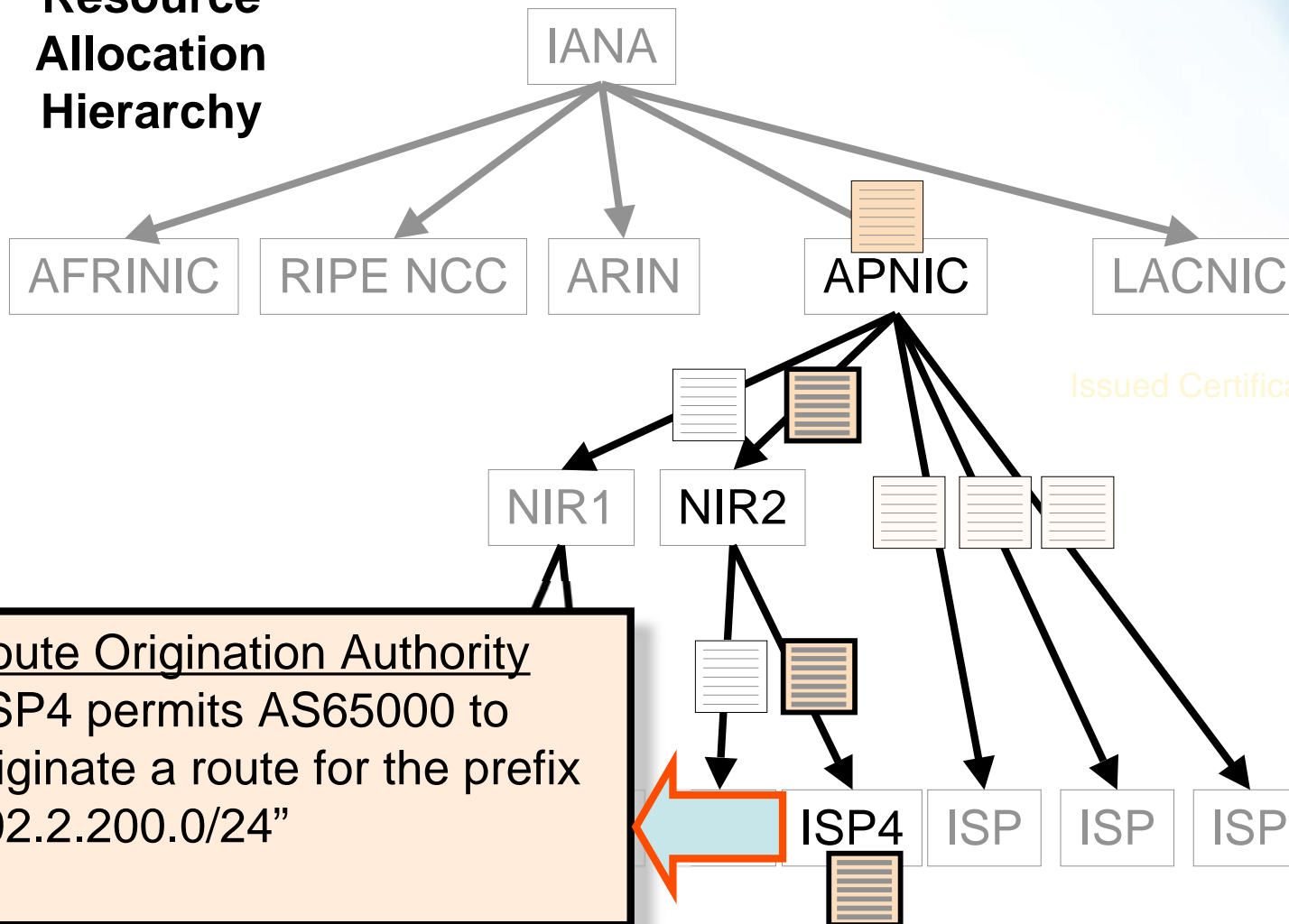
# Resource Certificates

## Resource Allocation Hierarchy



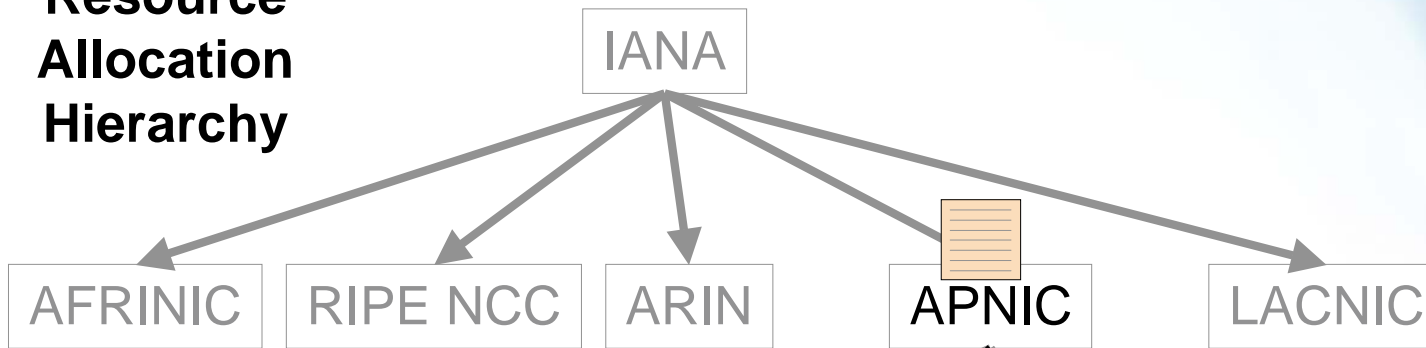
# Route Origination Authority document

## Resource Allocation Hierarchy

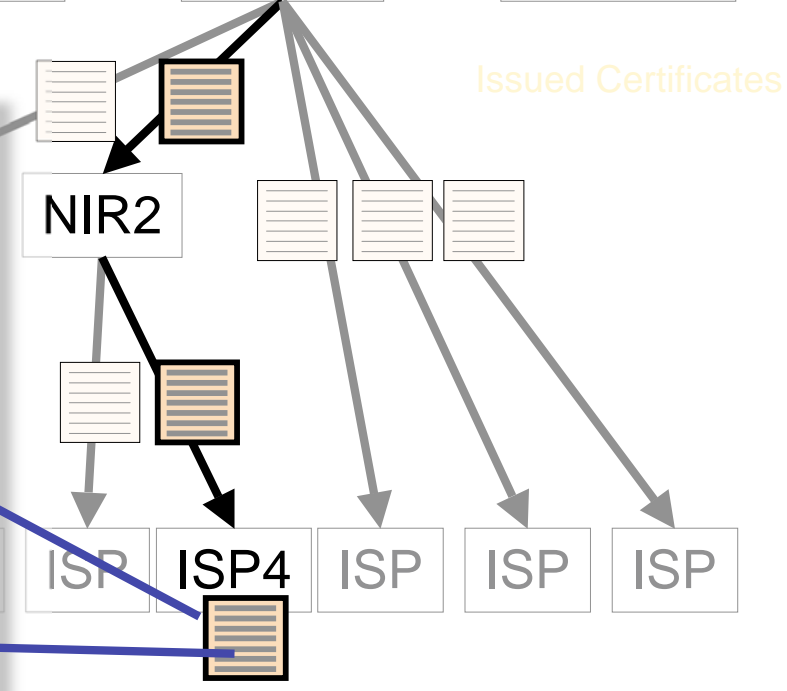


# Signed Objects

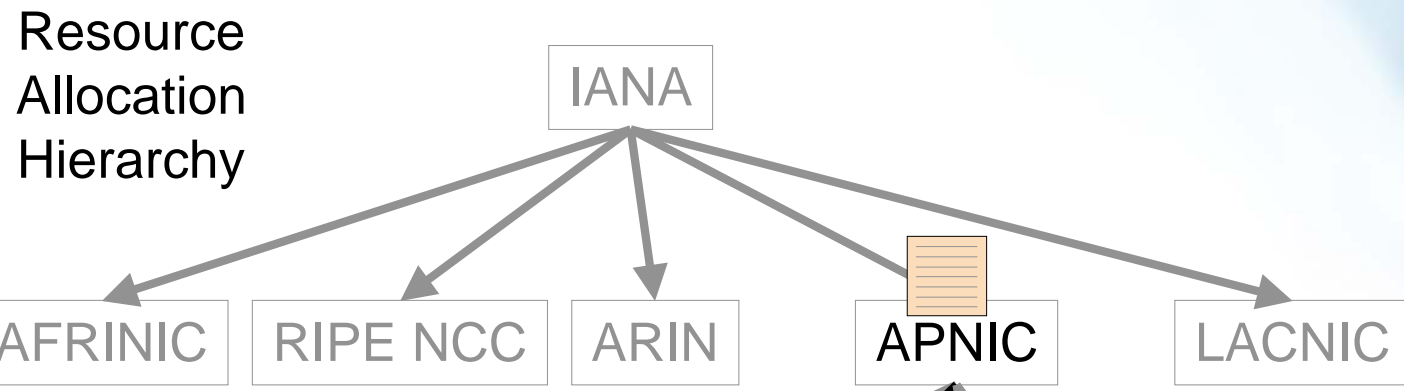
## Resource Allocation Hierarchy



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>



# Signed Object Validation



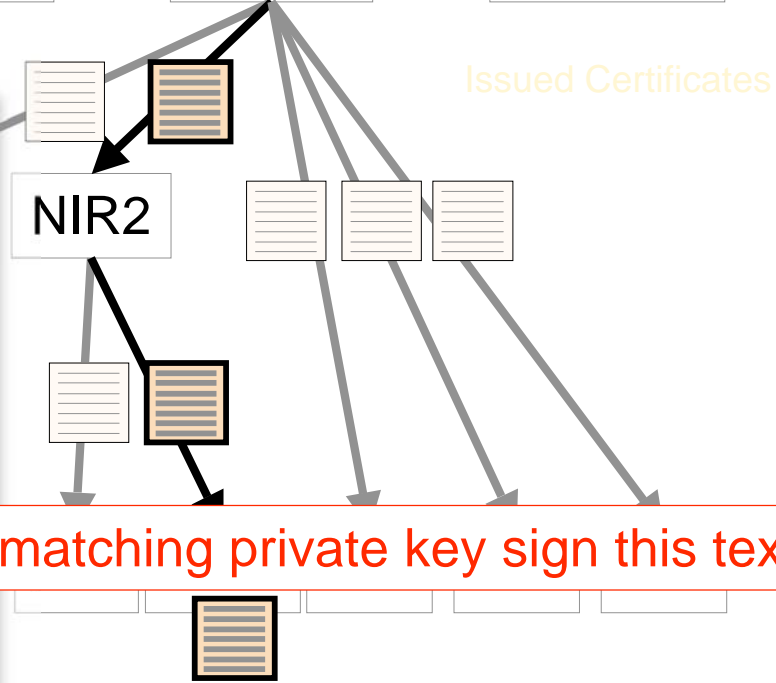
Route Origination Authority  
 "ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24"  
 Attachment: <isp4-ee-cert>

---

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

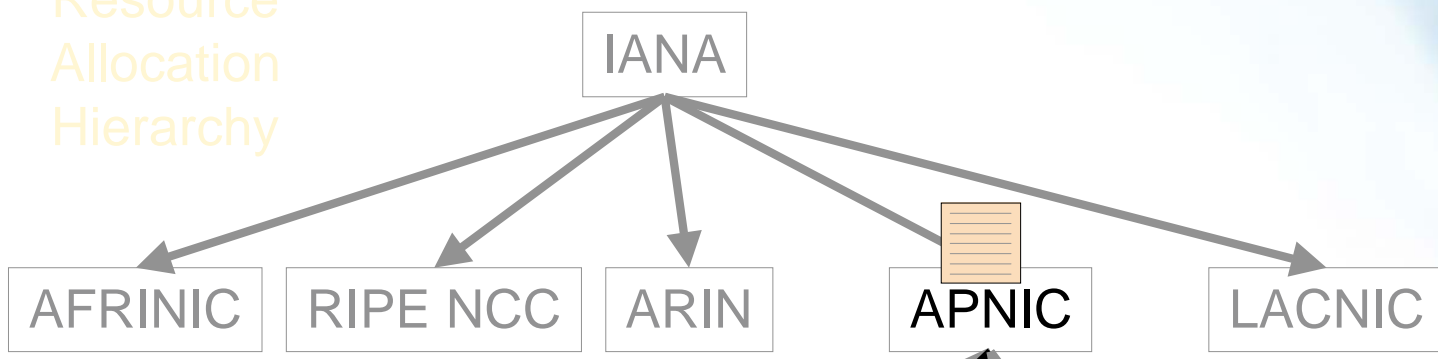


1. Did the matching private key sign this text?

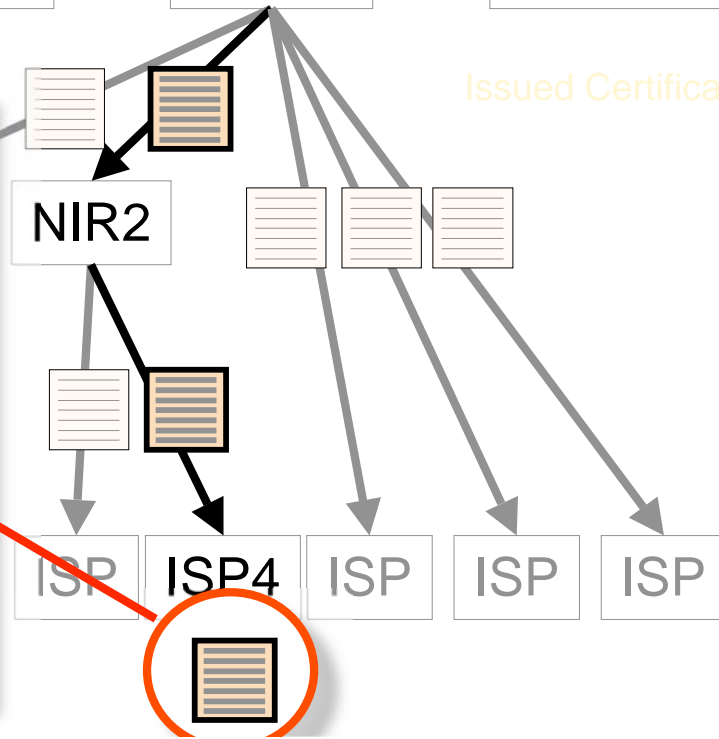


# Signed Object Validation

Resource Allocation Hierarchy



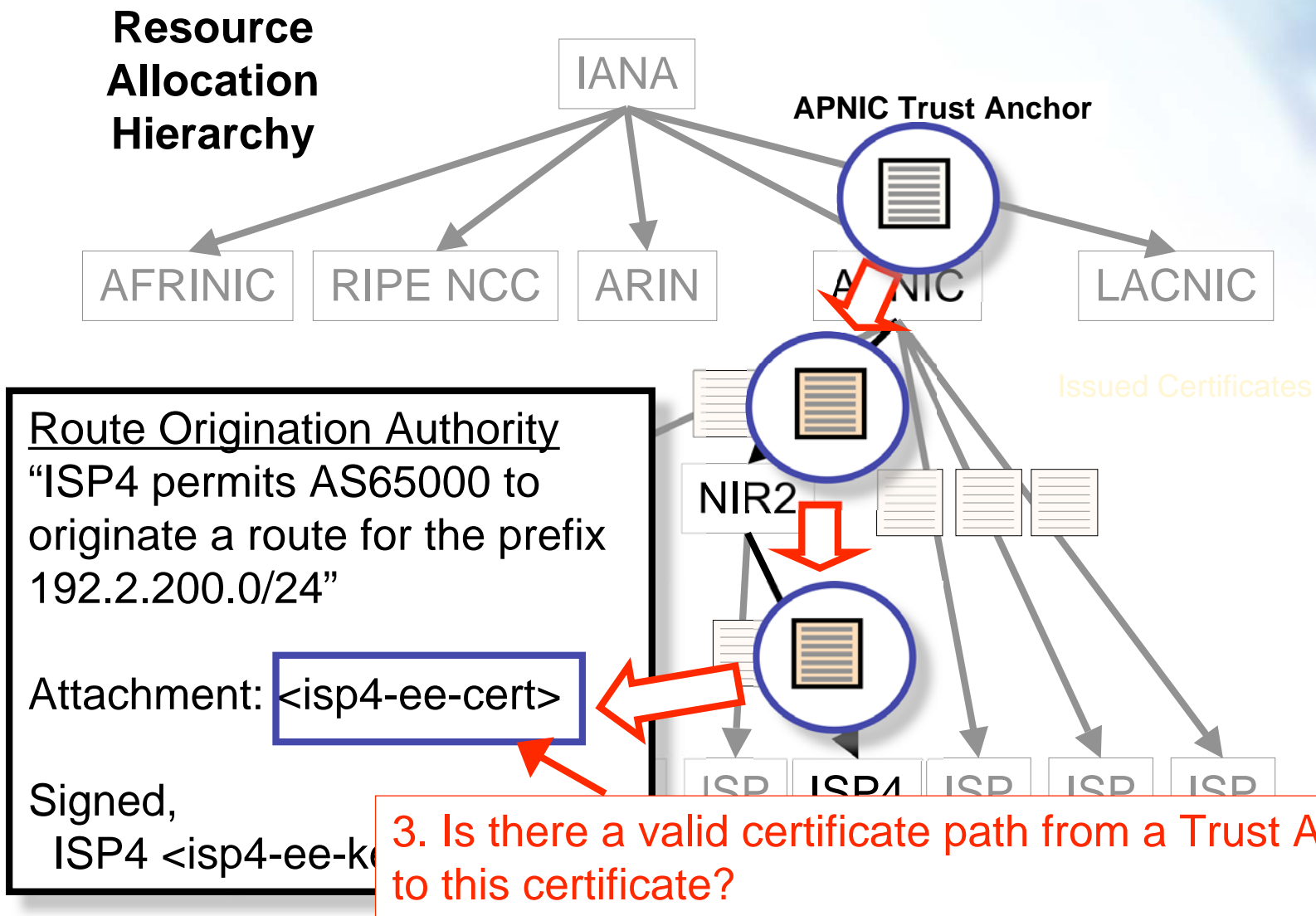
Issued Certificates



Route Origination Authority  
 "ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24"  
 Attachment: <isp4-ee-cert>  
 ISP4 <isp4-ee-key-priv>

2. Is this certificate valid?

# Signed Object Validation



# Signed Object Validation

## Resource Allocation Hierarchy



## 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

### 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>

## Summary

- Certification of IP Addresses and ASNs could help improve routing security by:
  - Mapping the delegation hierarchy to a Public Key Infrastructure hierarchy
  - Enabling routing instructions to be signed and validated by cryptographically secure processes.

## Questions?



- BGP incidents/attack article
  - <http://www.networkworld.com/news/2009/011509-bgp-attacks.html>
- Resource certification information available at
  - <http://www.apnic.net/services/resource-cert/index.html>