

TWNIC 12TH OPM 2009

IP ADDRESS AND ASN CERTIFICATION

George Kuo, APNIC Member Services Manager

Overview

- What is Resource Certification?
 - Definition
 - How it works
 - Why use Resource Certificates
 - Routing security
 - Resource custodianship
- How to get Resource Certification
- Conclusion

WHAT IS RESOURCE CERTIFICATION?

Definition of 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)

Definition of Resource Certificates



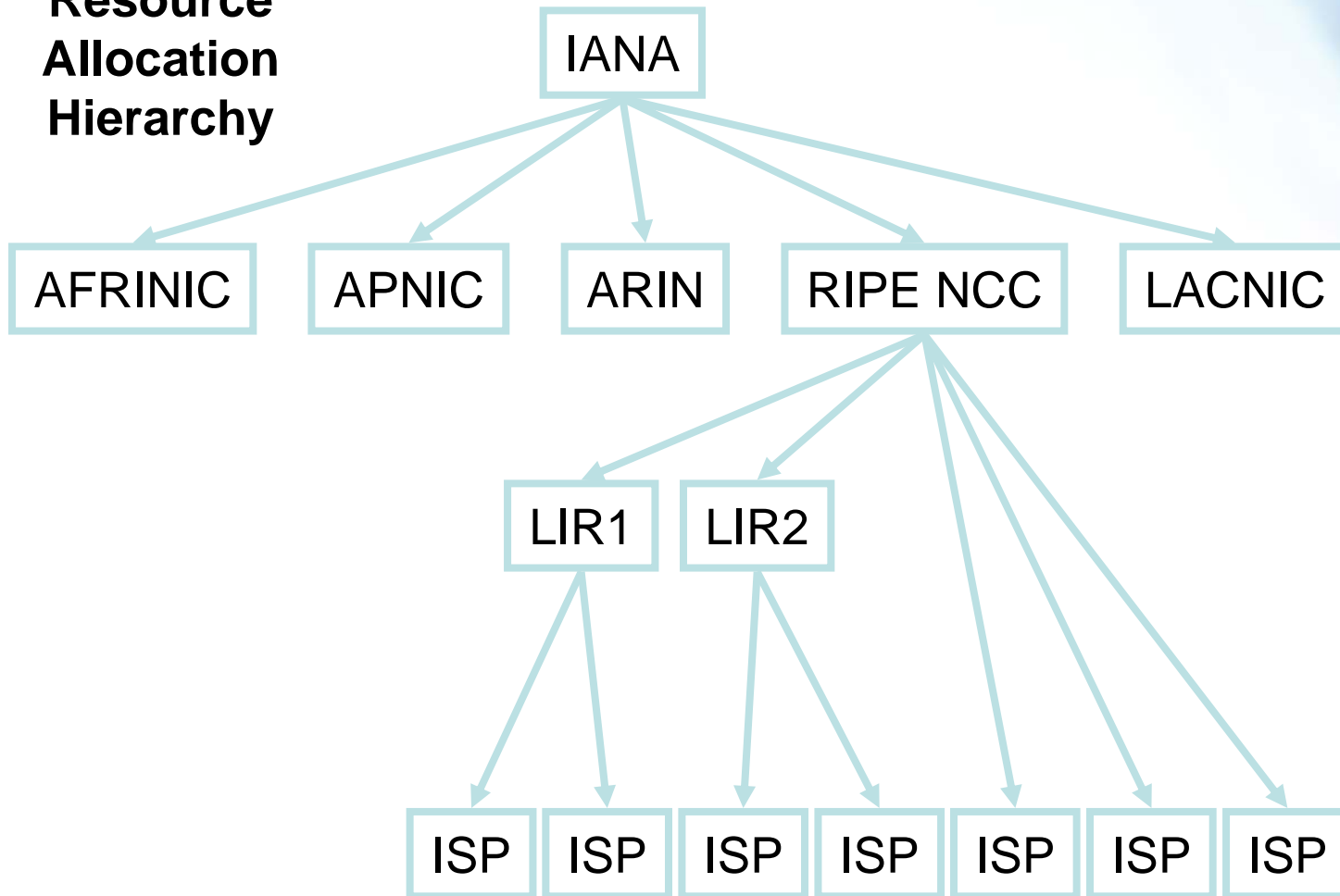
APNIC

- 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 (that is, 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 (that is, end user)

HOW DOES THE RESOURCE CERTIFICATE WORK?

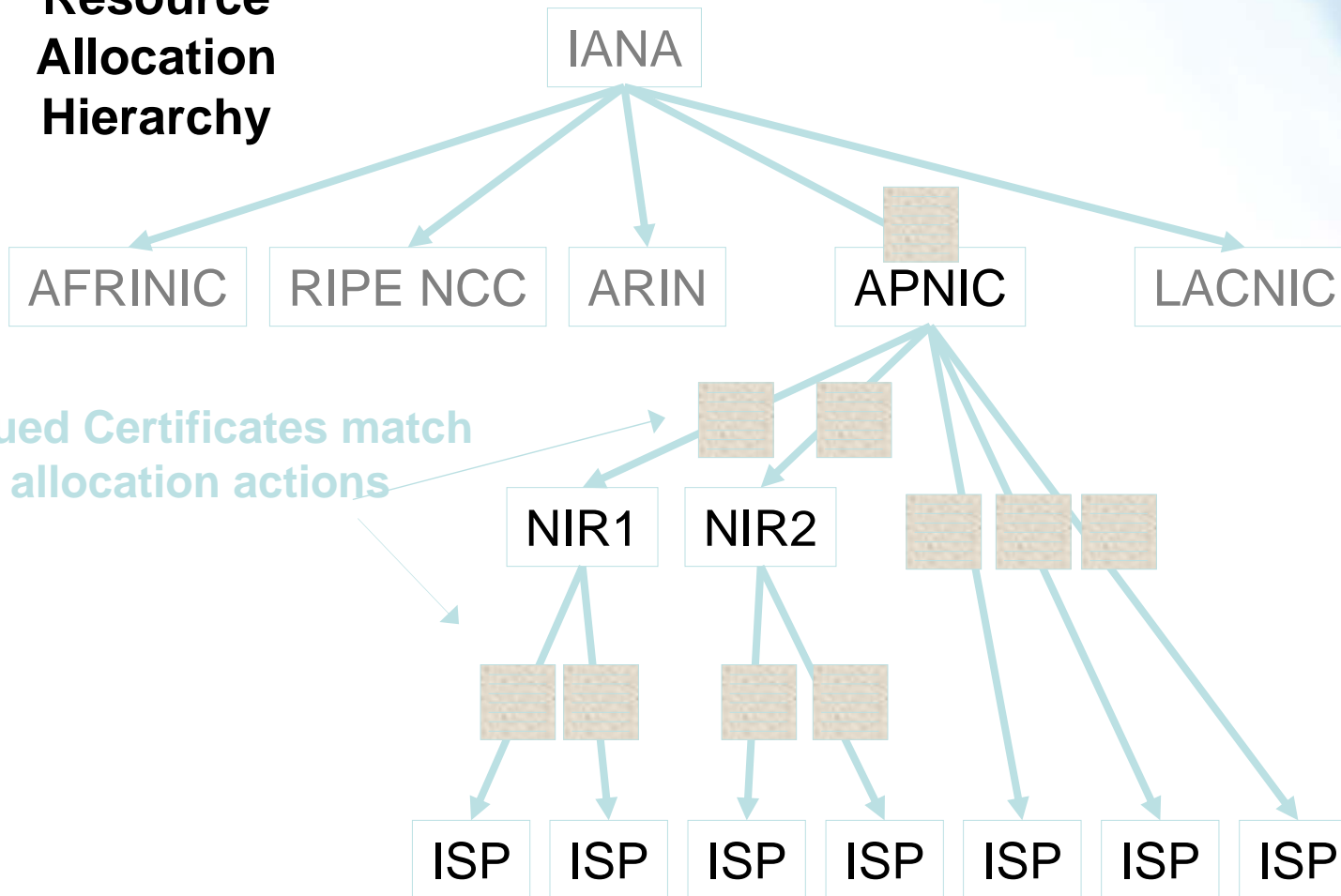
Resource Certificates

Resource Allocation Hierarchy



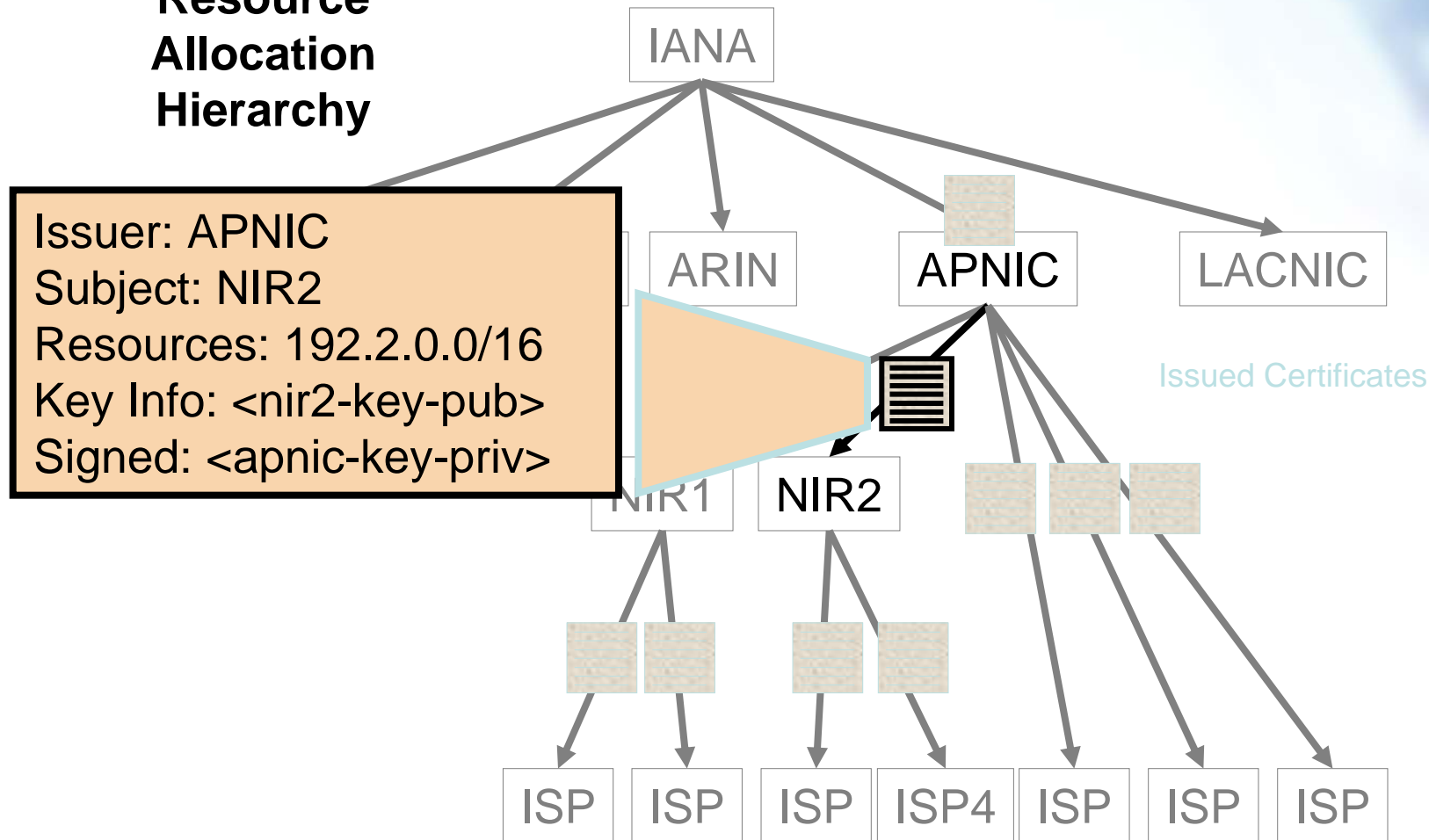
Resource Certificates

Resource Allocation Hierarchy



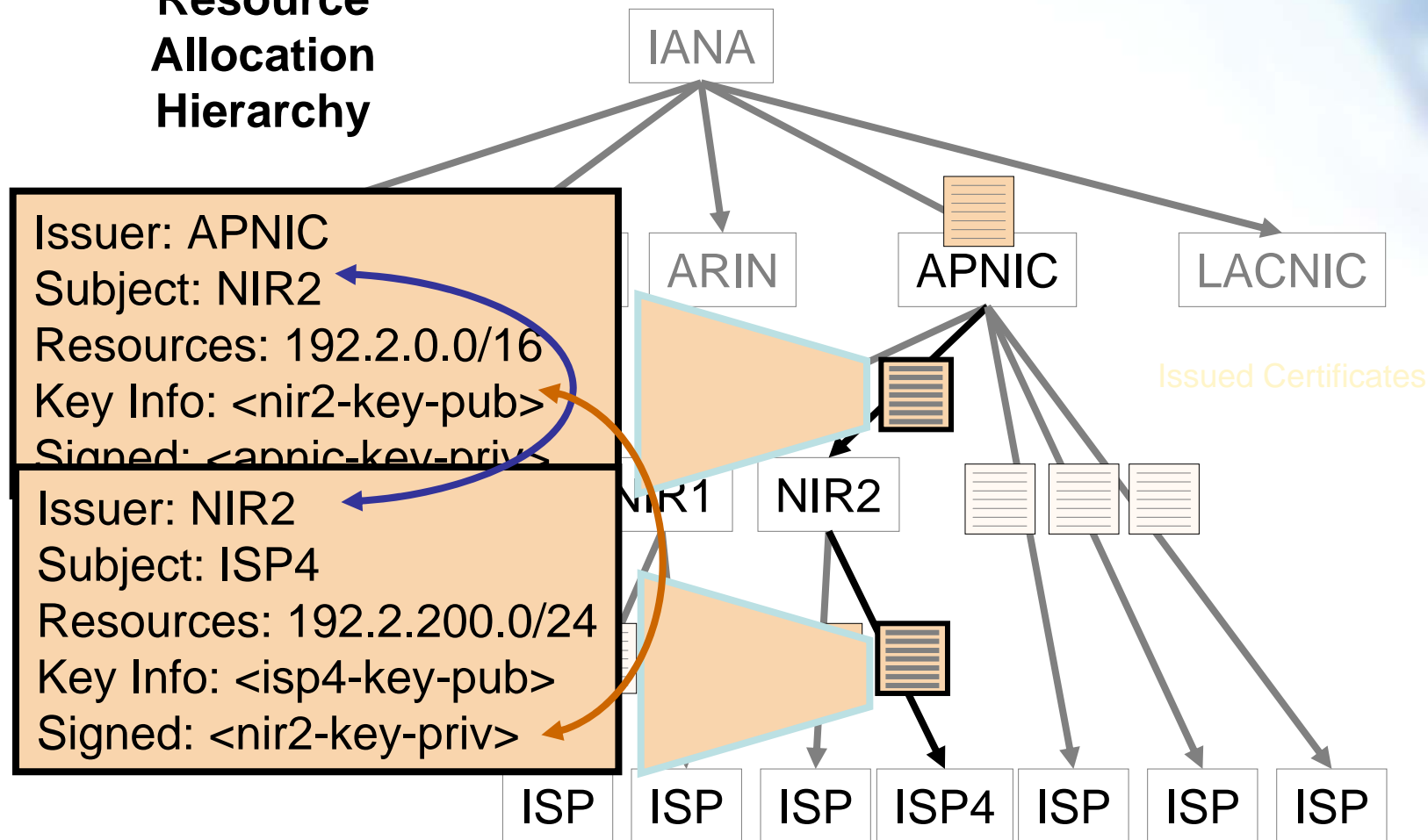
Resource Certificates

Resource Allocation Hierarchy



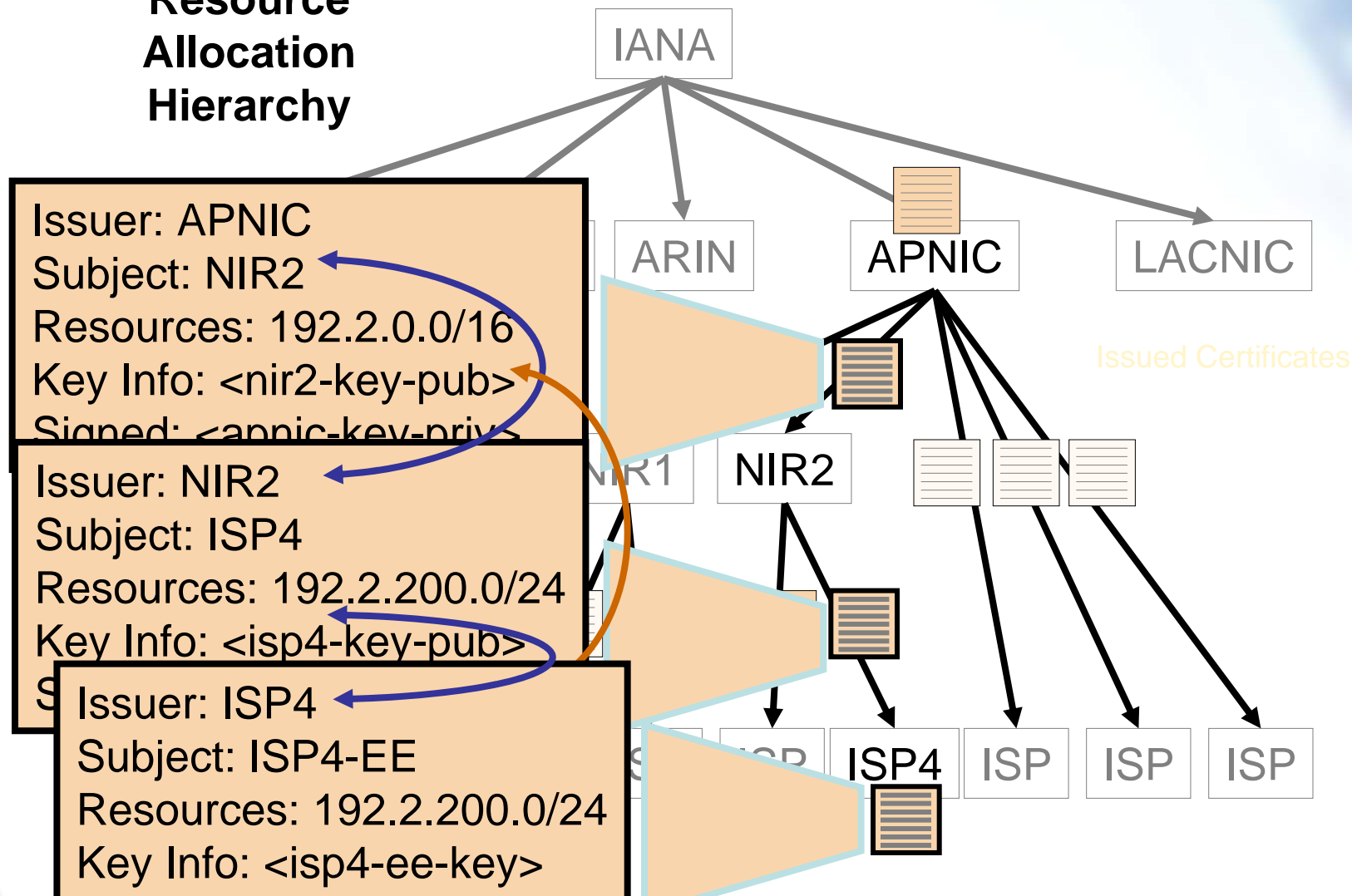
Resource Certificates

Resource Allocation Hierarchy



Resource Certificates

Resource Allocation Hierarchy



WHY USE RESOURCE CERTIFICATES?

- Routing security

Routing Security

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

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

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

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](#)

**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
- Global 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%

Routing Security Issues

- 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 ASes that represents a transit path from the current location to the prefix **and/or** a sequence of valid ASes 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
- AS Adjacency Attestation Objects (AAO)
 - “I attest that AS456 is adjacent to AS123 and AS789”, signed the holder of AS456
- Other signed data

WHY USE RESOURCE CERTIFICATES?

- Resource custodianship**

Resource Custodianship

- To potentially sign
 - Whois objects
 - Internet Routing Registry (IRR) objects
 - Resource Transfer requests

HOW TO GET RESOURCE CERTIFICATES? - MyAPNIC



[Home](#) / [Resources](#) / [Certification](#)

Resource Certification

Resource Certificate Download

Download the [current issued certificate](#) covering your owned resource set.

Sign Route Origin Authorization

Create a [signed ROA document](#), certifying your authorization for an Autonomous System to originate routes for your resources.

Sign Adjacency Attestation Object

Create a [signed AAO document](#), certifying that one of your Autonomous Systems is adjacent to other Autonomous Systems.

Recent Signed Products

You have no recently signed products

Advanced Management

For [more advanced management](#) of your [Route Origin Authorization](#), [Adjacency Attestation Object](#) details or viewing of the [activity log](#).

Resource Certificate

[Download this Certificate](#)

Version:	3
Serial Number:	23:88
Issuer:	/CN=APNIC Production-CVPQ5gUkLy7pOXdNeVWGvFX_0s
Not Valid Before:	Mar 20 2009 8:35:43 GMT
Not Valid After:	Jul 30 2020 0:00:00 GMT
Subject:	/CN=A91E170B

Authority Key Identifier

keyid: 09:53:D0:4A:05:24:2F:2E:E9:39:77:4D:79:55:86:BE:71:57:FF:4B

Subject Key Identifier

87:87:D3:F3:87:17:97:95:7F:BA:69:5B:1B:EB:B7:0E:92:8C:2C:88

Key Usage

Certificate Signing, CRL Signing

* CRITICAL *

Basic Constraints

ca: TRUE

* CRITICAL *

CRL Distribution Points

rsync://rpki.apnic.net/repository/A3C38A24D60311DCAB08F319798DBE39
/CVPQ5gUkLy7pOXdNeVWGvFX_0s.crl

Certificate Policies

1.3.6.1.5.5.7.14.2

* CRITICAL *

Authority Information Access

caIssuers - rsync://rpki.apnic.net/repository/88DFC7DED5FD11DCB14CF4B1A703F987
/CVPQ5gUkLy7pOXdNeVWGvFX_0s.cer

Subject Information Access

caRepository - rsync://rpki.apnic.net/member_repository/A91E170B/7065DCFAA35C11DD977174C51F86D636/
rpkiManifest - rsync://rpki.apnic.net/member_repository/A91E170B/7065DCFAA35C11DD977174C51F86D636/
/h4FT84cX5V_umibG-uJDpKMLLs.mft

SBGP AS Identifiers

Autonomous System Numbers

45192 131107

* CRITICAL *

SBGP IP Address Families

IPv4

203.176.189.0/24

IPv6

2001:0d0:000a::/48

* CRITICAL *

[Download this Certificate](#)

Conclusion

- The Internet community at forums such as the IETF have recognized the need to secure the Internet and the IP address layer.
- Certification of Internet resources (IP addresses/AS numbers) has many potential uses in applications that require verification or validation of resource custodianship

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>