# Using Resource Certificates

## Progress Report on the Trial of Resource Certification

November 2006

Geoff Huston
APNIC

# What would be good …

To be able to use a reliable infrastructure to validate assertions about addresses and their use:

- Publish routing authorities authored by a resource holder that cannot be altered or forged
- Allow third parties to authenticate that an address or routing assertion was made by the current right-of-use holder of the number resource

# What would be even gooder …

- Is to have a reliable, efficient, and effective way to underpin the integrity of the Internet's address resource distribution structure and our use of these resources in the operational Internet

- Is to replace various forms of risk-prone assertions, rumours, implicit trust and fuzzy traditions about addresses and their use with demonstrated validated authority

# Resource Certificate Trial

Approach:

- Use X.509 v3 Public Key Certificates (RFC3280) with IP address and ASN extensions (RFC3779)

Parameters:

- Use existing technologies where possible
- Leverage on existing open source software tools and deployed systems
- Contribute to open source solutions and open standards

OpenSSL as the foundational platform

- Add RFC3779 (resource extension) support

Design of a Certification framework

- anchored on the IP resource distribution function

# Resource Public Key Certificates

**The certificate's Issuer certifies that:**

**the certificate's Subject**

***whose public key is contained in the certificate***

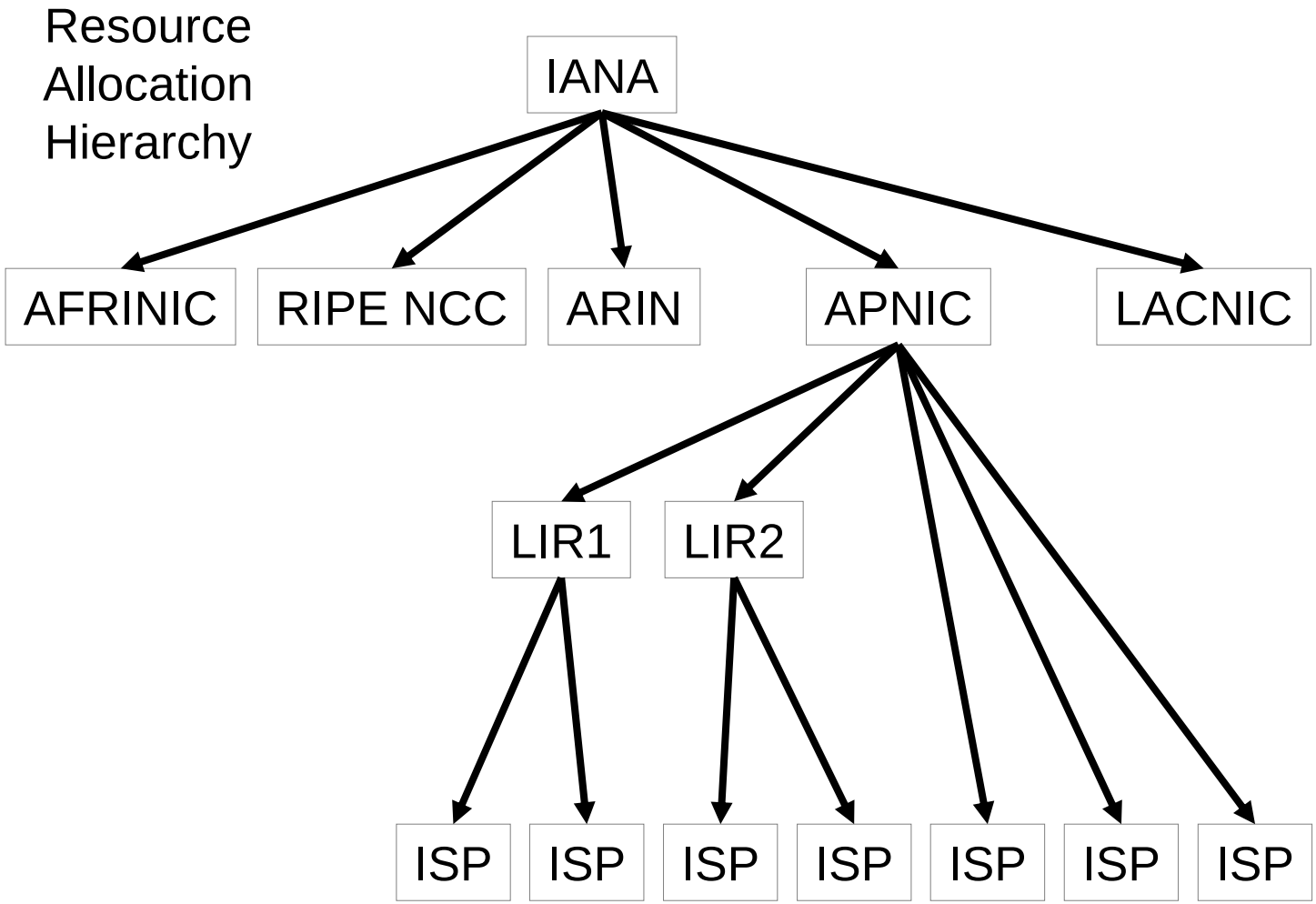
**is the current controller of a collection of IP address and AS resources**

***that are listed in the certificate's resource extension***

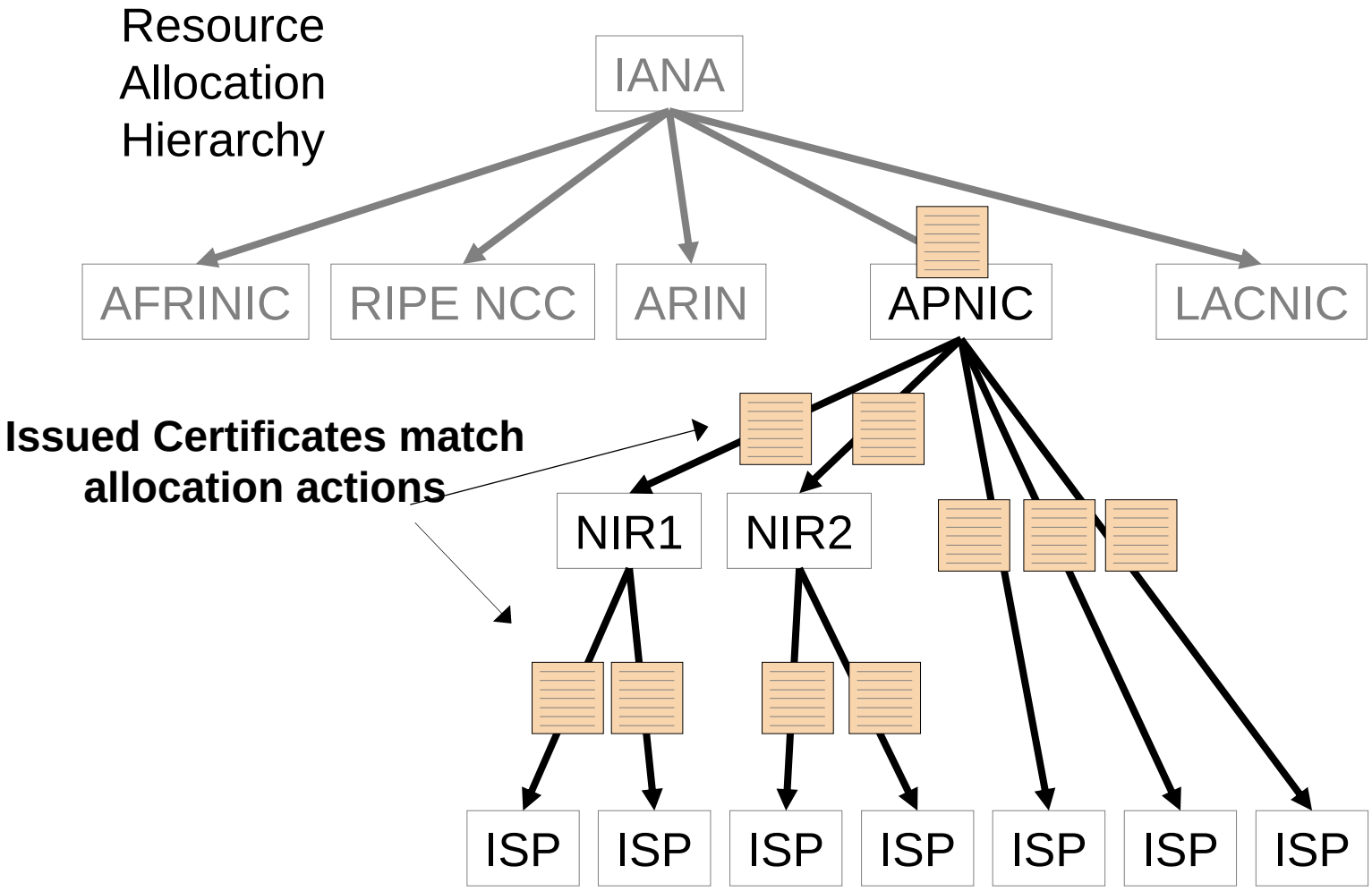
This is not an attestation relating to identity or role – it is an attestation that in effect binds a private key to a right-of-use of a number resource collection

This is not an attestation about any form of related routing policies

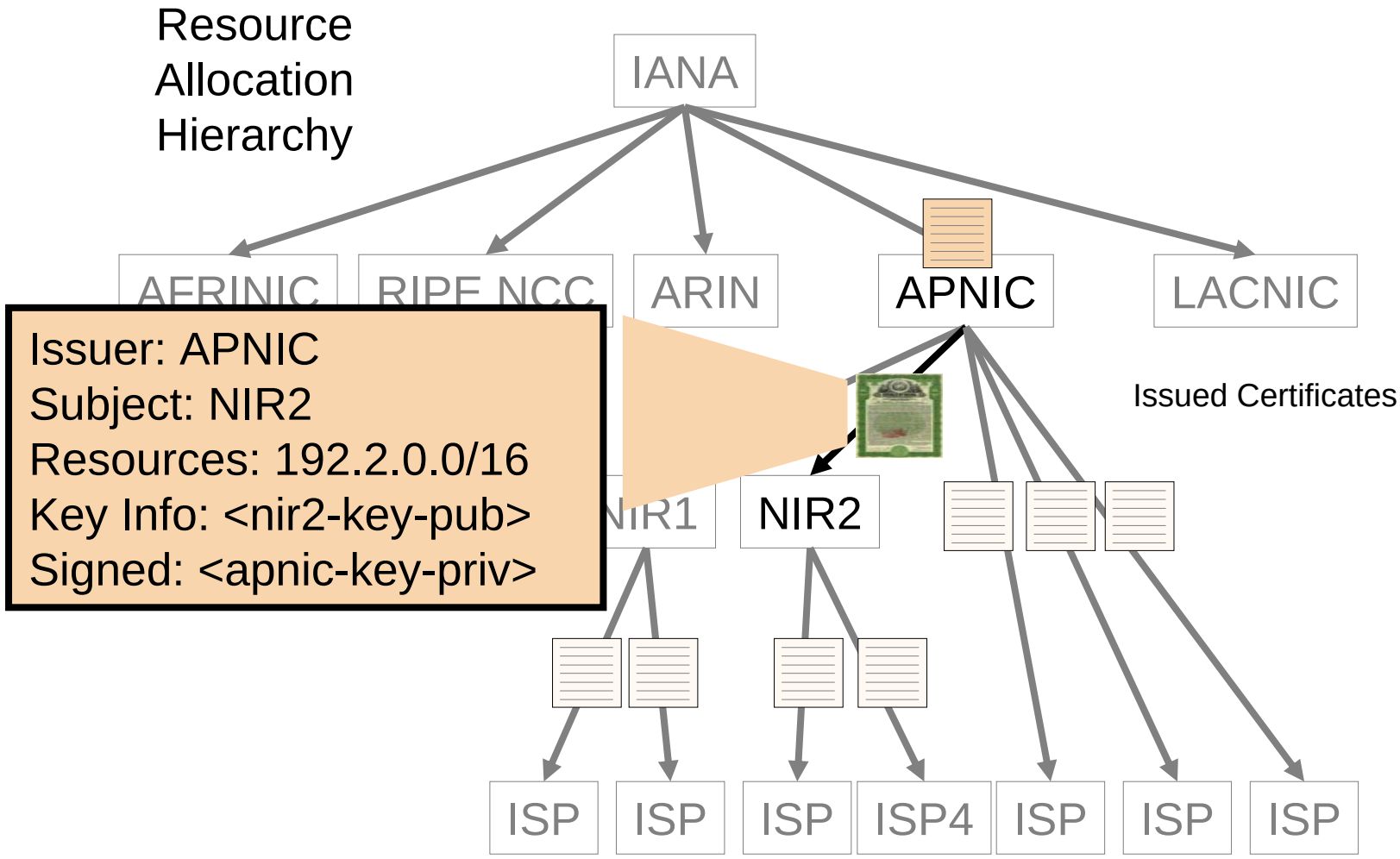
# Resource Certificates



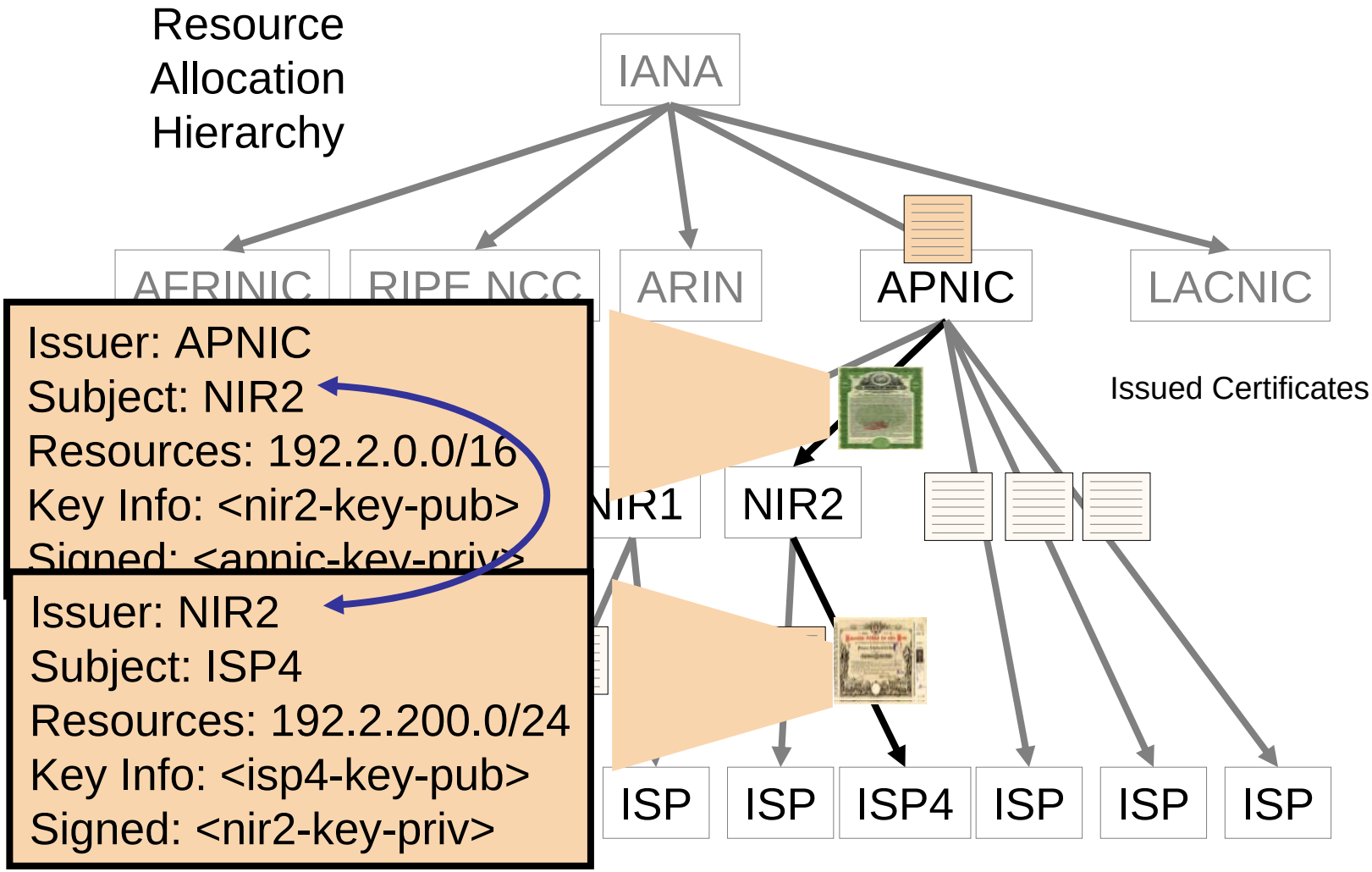
# Resource Certificates



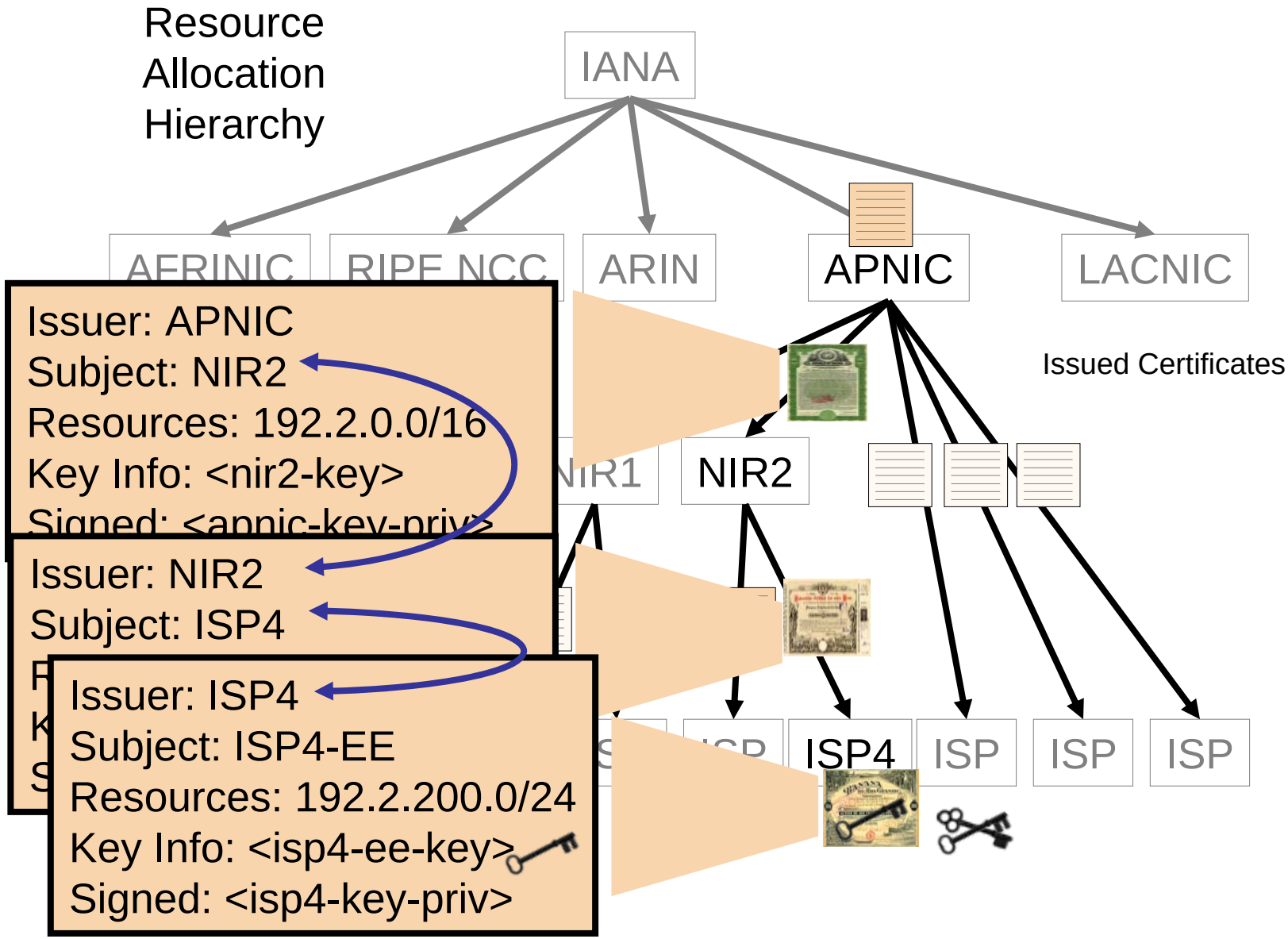
# Resource Certificates



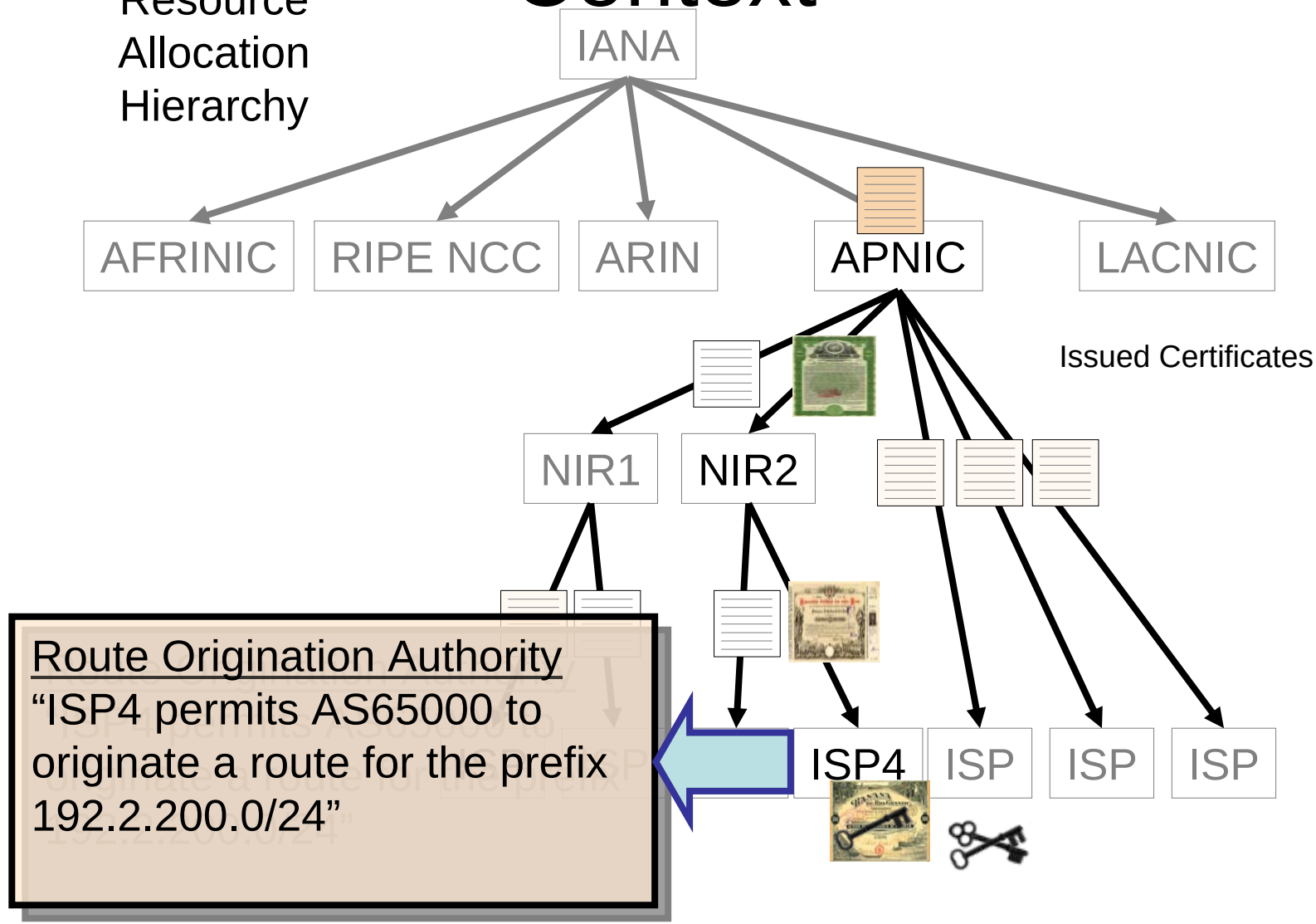
# Resource Certificates



# Resource Certificates

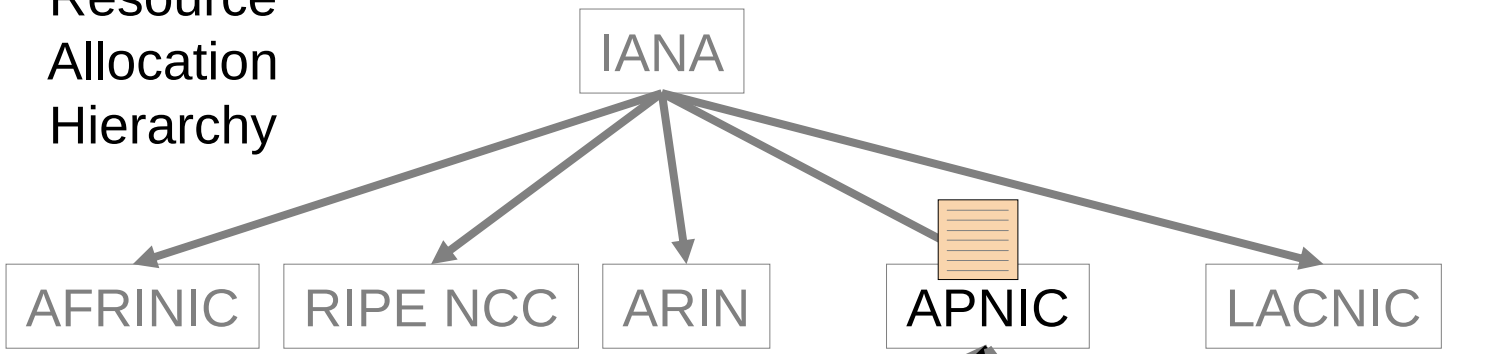


# Base Object in a Routing Authority Context

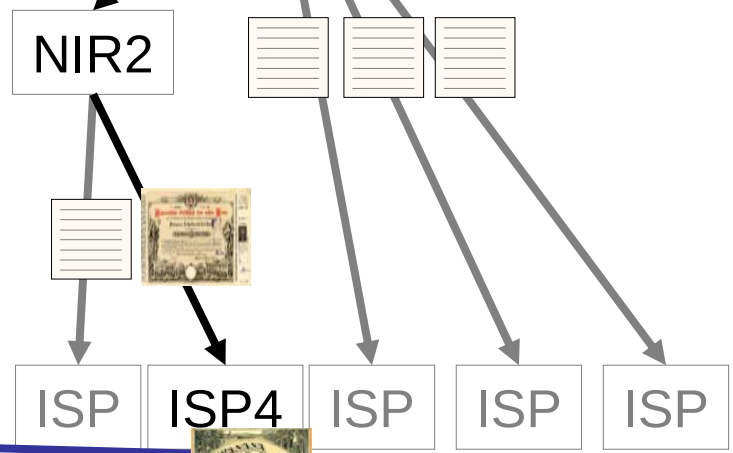


# Signed Objects

Resource Allocation Hierarchy




Issued Certificates




Route Origination Authority

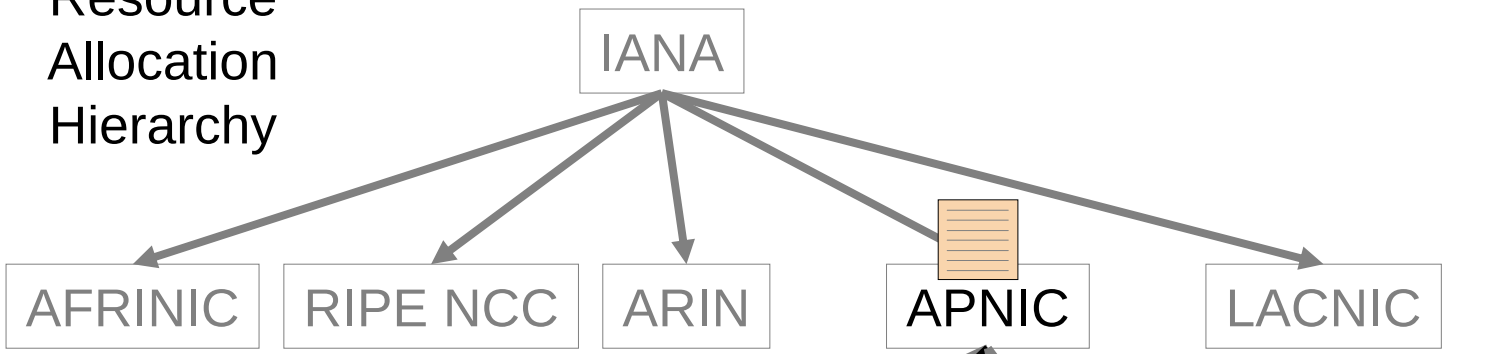
"ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24"

Attachment: <isp4-ee-cert>

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

# Signed Object Validation

Resource Allocation Hierarchy




Issued Certificates

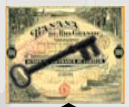


NIR2

ISP ISP4 ISP ISP ISP

Route Origination Authority

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



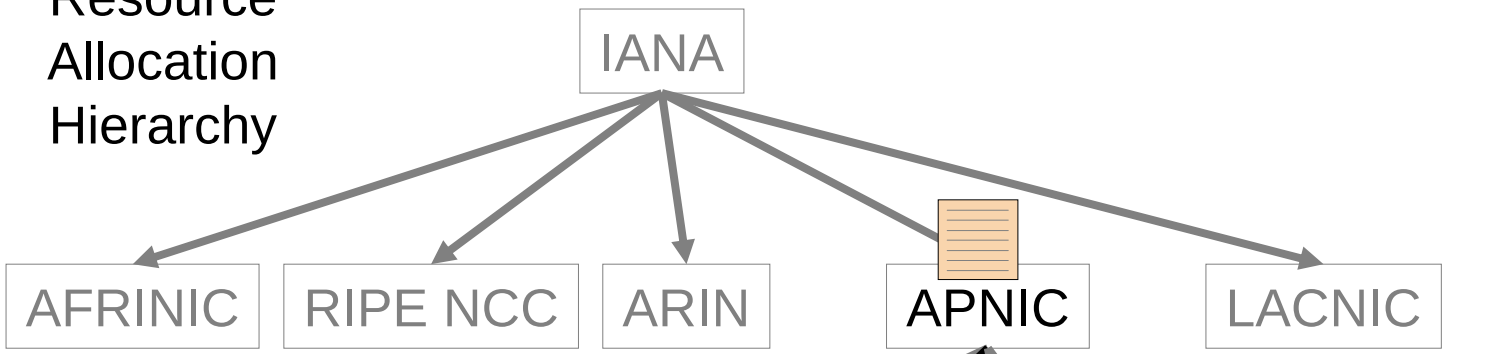
Attachment: <isp4-ee-cer

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

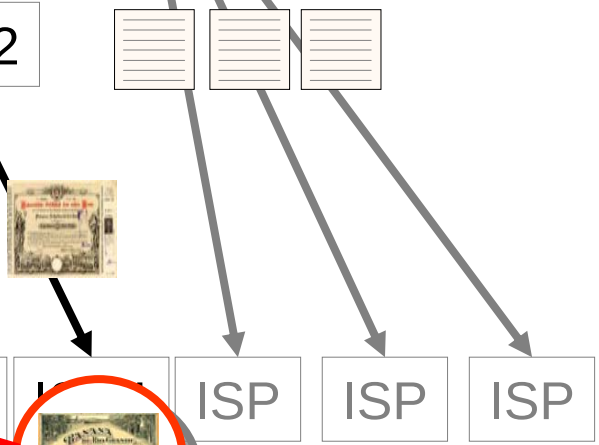
1. Did the matching private key sign this text?

# Signed Object Validation

Resource Allocation Hierarchy




Issued Certificates




Route Origination Authority

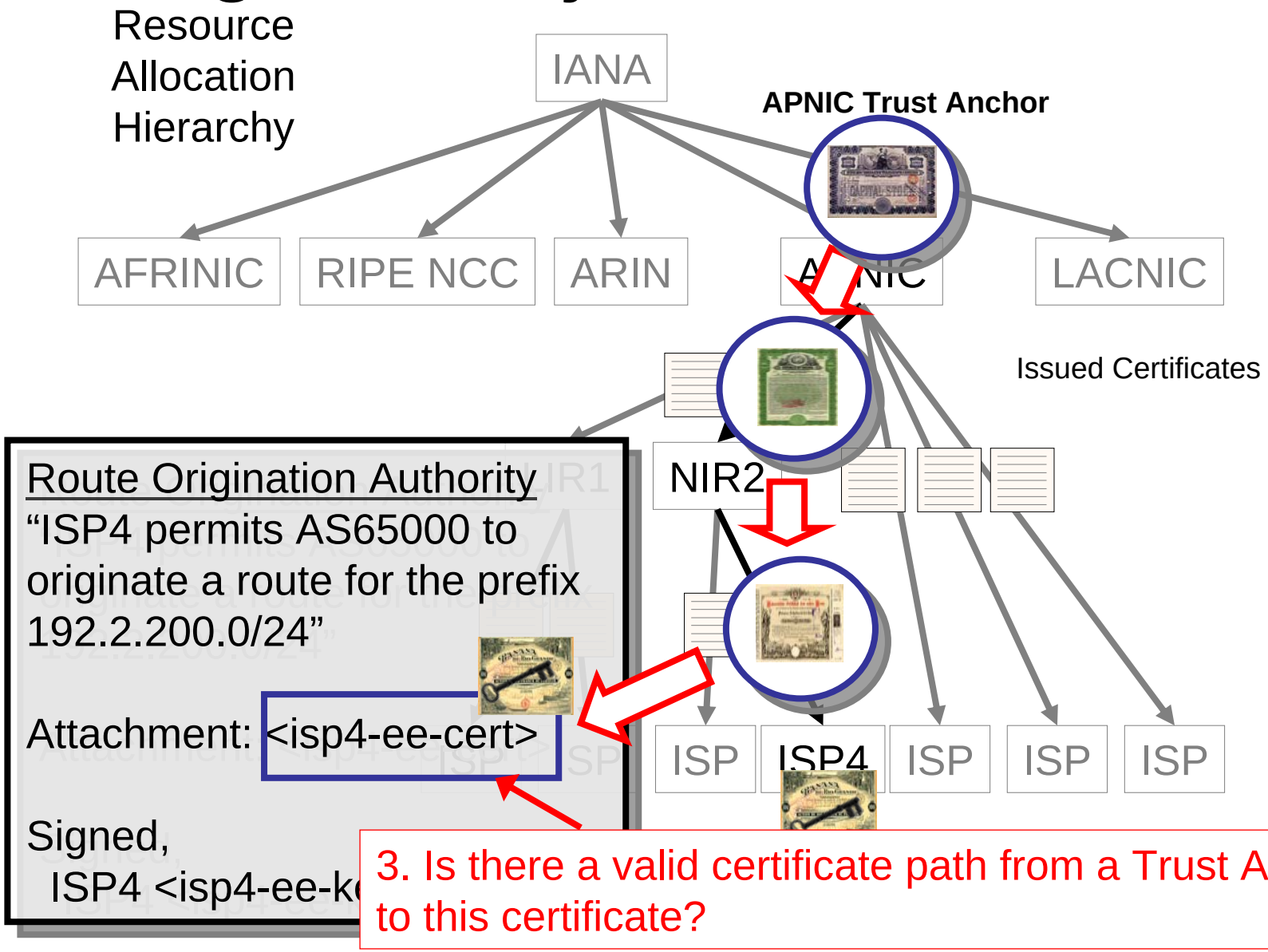
"ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24"

Attachment: <isp4-ee-cert>

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

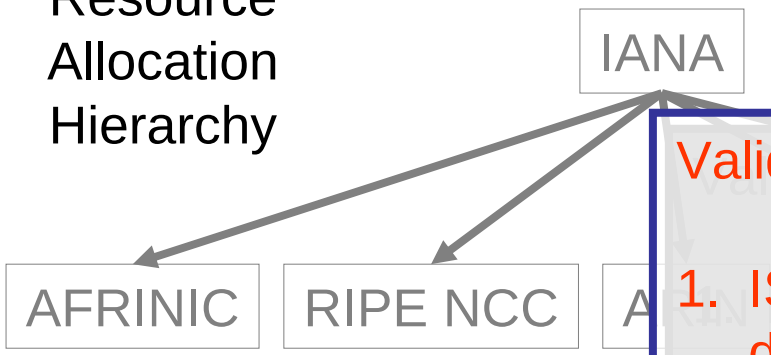
2. Is this certificate valid?

# Signed Object Validation



# Signed Object Validation

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>

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

# Example of a Signed Object

```
netnum-set:  RS-TELSTRA-AU-EX1
descr:       Example routes for customer with space under apnic
members:     58.160.1.0-58.160.16.255,203.34.33.0/24
tech-c:      GM85-AP
admin-c:     GM85-AP
notify:      test@telstra.net
mnt-by:      MAINT-AU-TELSTRA-AP
sigcert:     rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5
             Ck01Op5Q/Hc4yxwhTamNXW-cDWtQcmvOVGjU.cer
sigblk:      -----BEGIN PKCS7-----
             MIIBdQYJKoZIhvcNAQcCoIIBZjCCAWICAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3
             DQEHATGCAUEwggE9AgEBMBowFTETMBEGA1UEAxMKdGVsc3RyYS1hdQIBATAJBgUr
             DgMCGgUAMA0GCSqGSIb3DQEBAQUABIIBAEZGI2dAG3lAAGi+mAK/S5bsNrgEHOmN
             1leJF9aqM+jVO+tiCvRHyPMeBMiP6yoCm2h5RCR/avP40U4CC3QMhU98tw2BqOTY
             HZvqXfAOVhjD4Apx4KjiAyr8tfeC7ZDhO+fpvsydV2XXtHIvjwjcL4GvM/gES6dJ
             KJYFWWlrPqQnfTFMm5oLWBUhNjuX2E89qyQf2YZVizITTNg3ly1nwqBoAqmmDhDy
             +nsRVAxax7II2iQDTr/pjI2VWfe4R36gbT8oxyvJ9xz7I9IKpB8RTvPVO2I2HbMI
             1SvRXMx5nQOXyYG3Pcxo/PAhbBkVkgfudLki/IzB3j+4M8KemrnVMRo=
             -----END PKCS7-----
changed:     test@telstra.net 20060822
source:      APNIC
```

# Signer's certificate

```
Version:   3
Serial:    1
Issuer:    CN=telstra-au
Validity:  Not Before: Fri Aug 18 04:46:18 2006 GMT
Validity:  Not After:  Sat Aug 18 04:46:18 2007 GMT
Subject:   CN=An example sub-space from Telstra IANA, E=apnic-ca@apnic.net
Subject Key Identifier g(SKI): Hc4yxwhTamNXW-cDWtQcmvOVGjU
Subject Info Access: caRepository -
           rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5
           CkO1Op5Q/Hc4yxwhTamNXW-cDWtQcmvOVGjU
Key Usage: DigitalSignature, nonRepudiation
CRL Distribution Points:
           rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5
           CkO1Op5Q.crl
Authority Info Access: caIssuers -
           rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5
           CkO1Op5Q.cer
Authority Key Identifier:
           Key Identifier g(AKI): cbh3Sk-iwj8Yd8uqaB5CkO1Op5Q
Certificate Policies: 1.3.6.1.5.5.7.14.2
IPv4:       58.160.1.0-58.160.16.255, 203.34.33.0/24
```

# Trial Status

- ✓ Specification of X.509 Resource Certificates
- ✓ Generation of resource certificate repositories aligned with existing resource allocations and assignments
- ✓ Tools for Registration Authority / Certificate Authority interaction (undertaken by RIPE NCC)
- ✓ Tools to perform validation of resource certificates

Current Activities

- ✸ Extensions to OpenSSL for Resource Certificates (open source development activity, supported by ARIN)
- ✸ Tools for resource collection management, object signing and signed object validation (APNIC, and also open source development activity, supported by ARIN)
- ✸ LIR / ISP Tools for certificate management
- ✸ Testing, Testing, Testing
- ✸ Operational service profile specification

Working notes and related material we've been working on in this trial activity:

**http://mirin.apnic.net/resourcecerts**