Using Resource Certificates

Progress Report on the Trial of Resource Certification

October 2006

Geoff Huston
Chief Scientist
APNIC

From the PPML Mailing List …

2006-3 ("Capturing Originations in Templates")

Sandy Murphy:

If the discipline and scrutiny could be transferred somehow to the routing registry, that's great.

Mark Kosters:

The PKI effort [...] allows for strong security. However, there much work to be done here and the end result may be complex

Ed Lewis:

ARIN can only offer up the attestations from the what it knows (securely)

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

Motivation: 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.**

Motivation: 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?

Motivation: 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

A sequence of valid ASs that represents the path of the routing update message

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

  Object Signing plus *Publication*

- Allow third parties to authenticate that an address or routing assertion was made by the current right-of-use holder of the address resource

  Validation using a *Resource Certificate PKI*

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

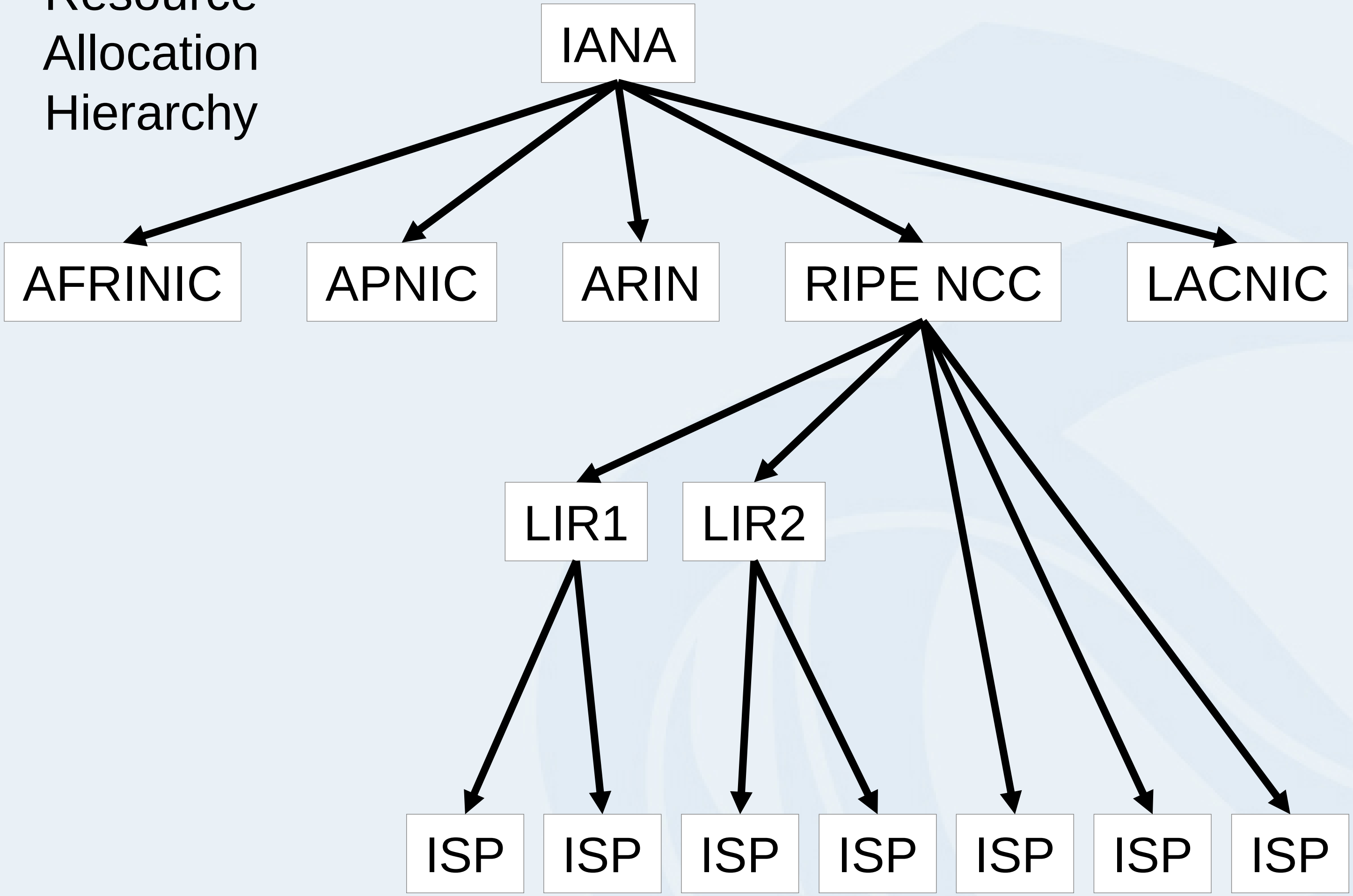
that are listed in the certificate's resource extension

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

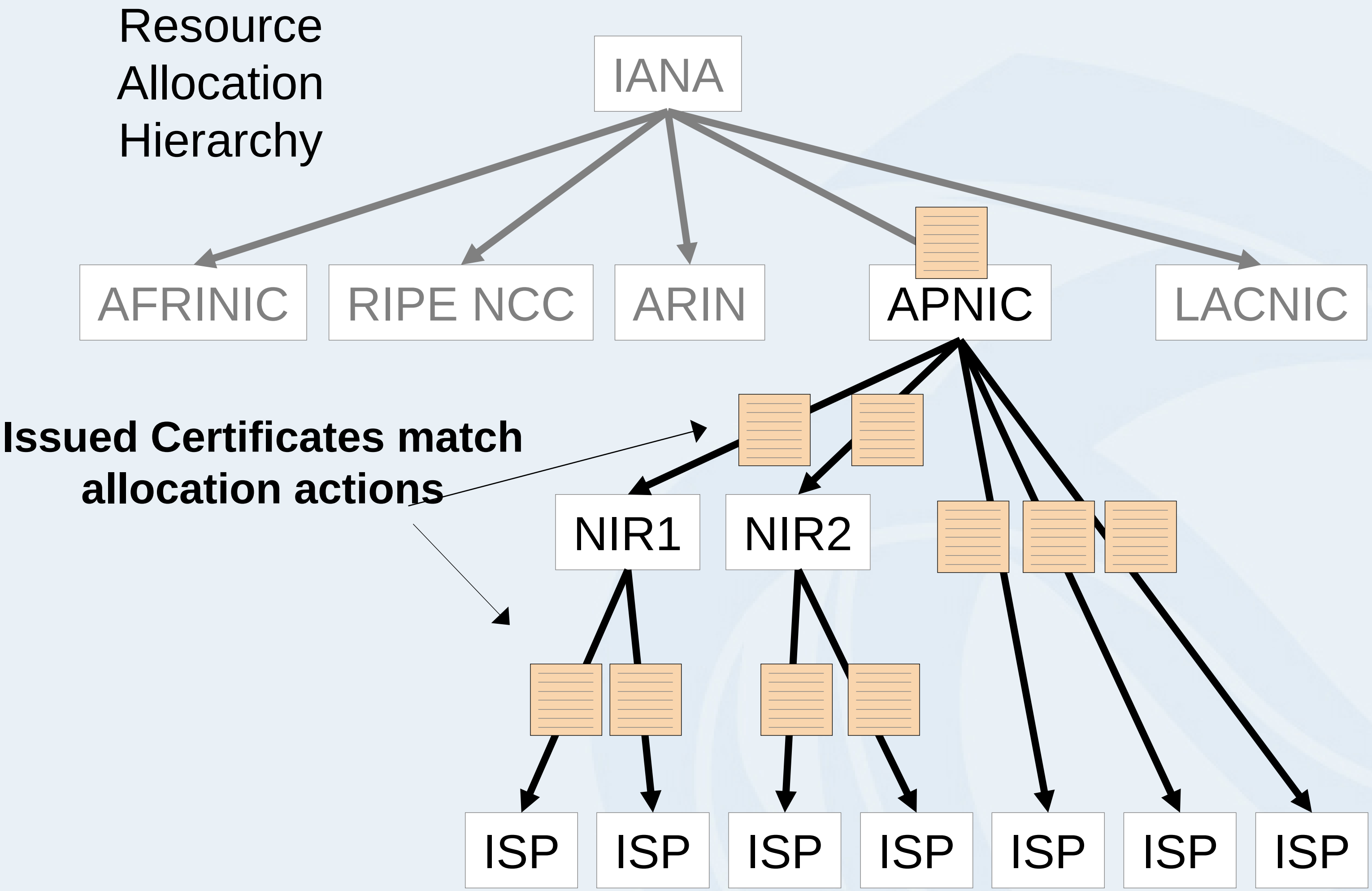
This is not an attestation about any form of routing policies

Resource Certificates

Resource Allocation Hierarchy



Resource Certificates

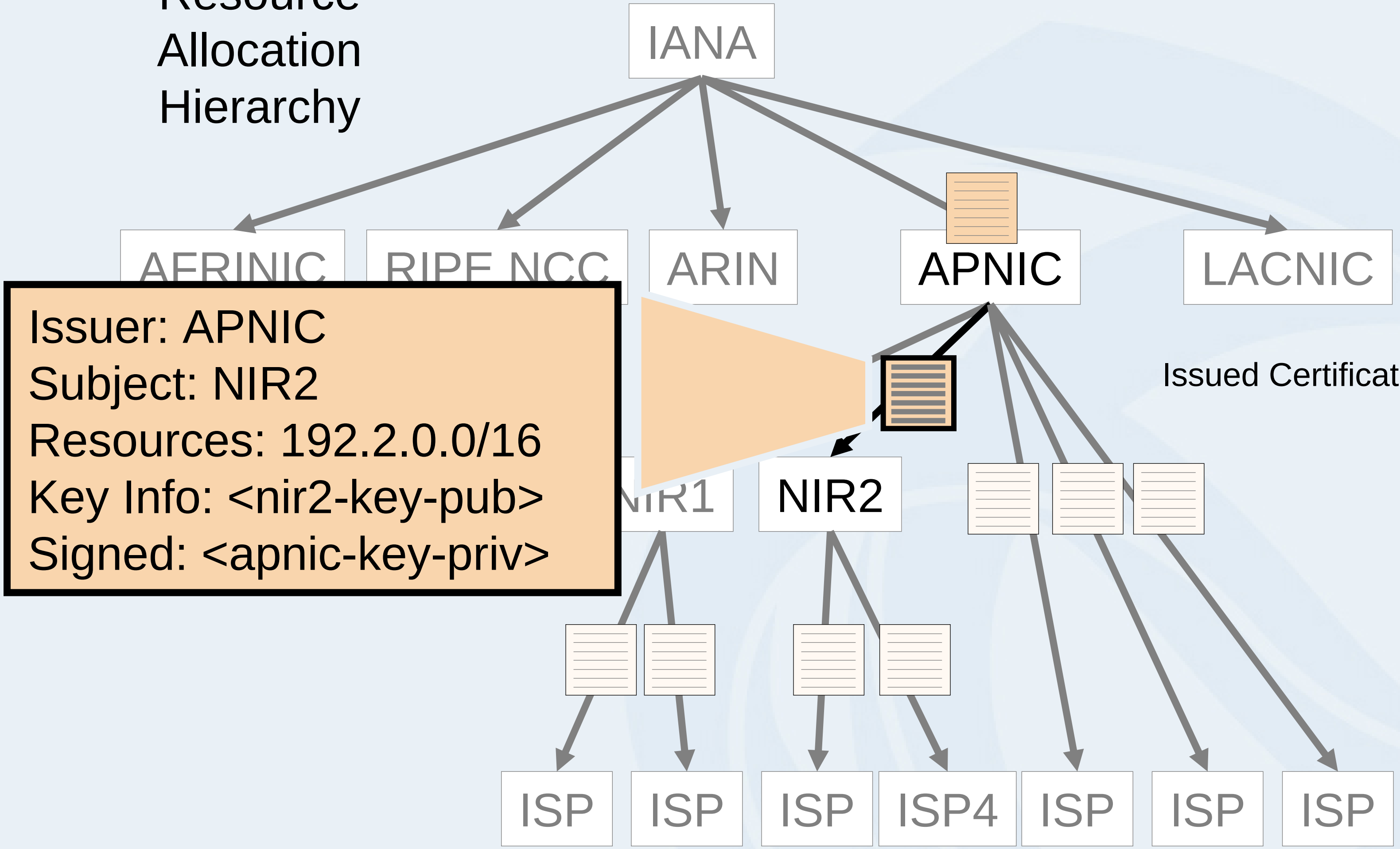


Resource Allocation Hierarchy

Issued Certificates match allocation actions

Resource Certificates

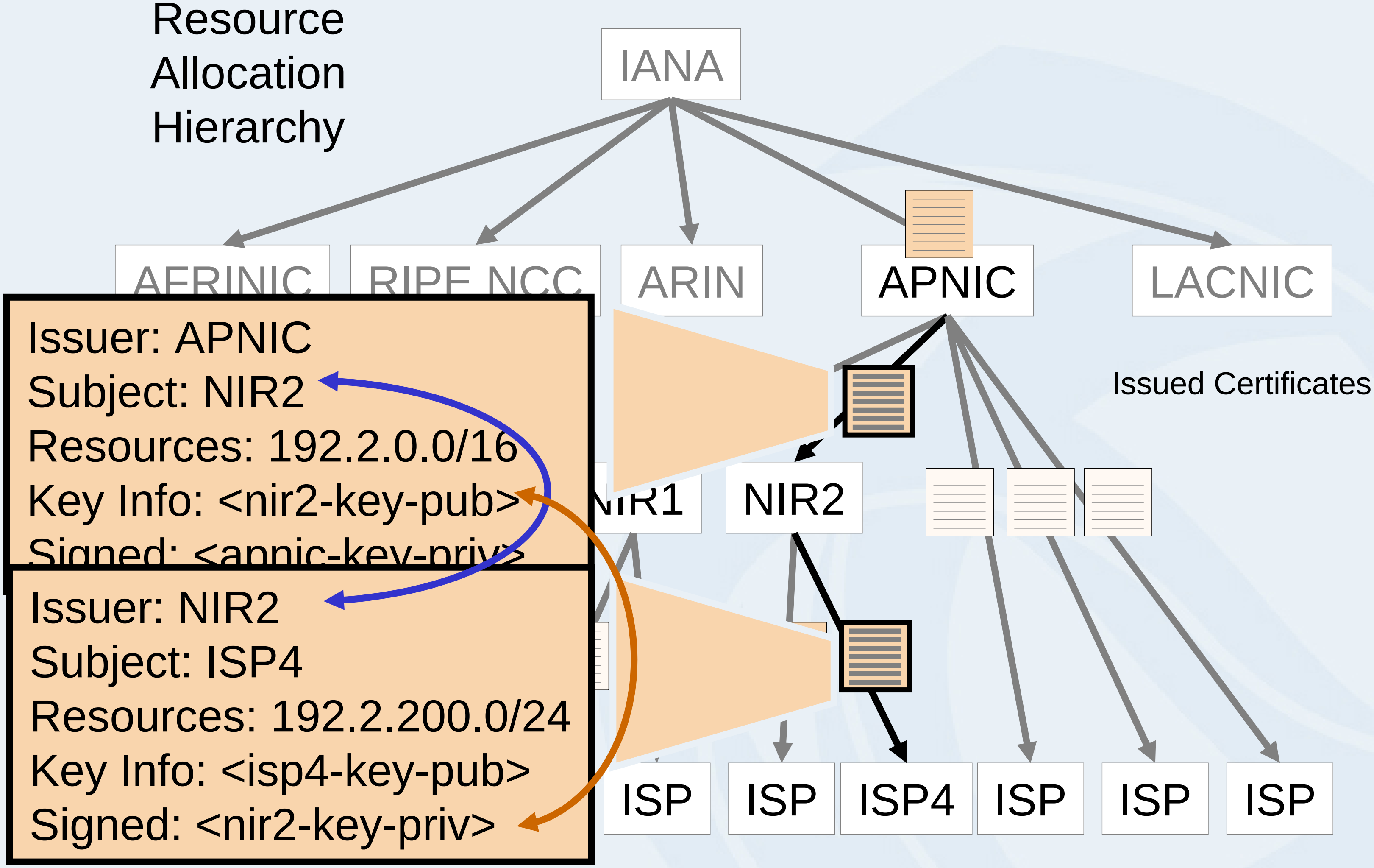
Resource Allocation Hierarchy



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

Issued Certificates

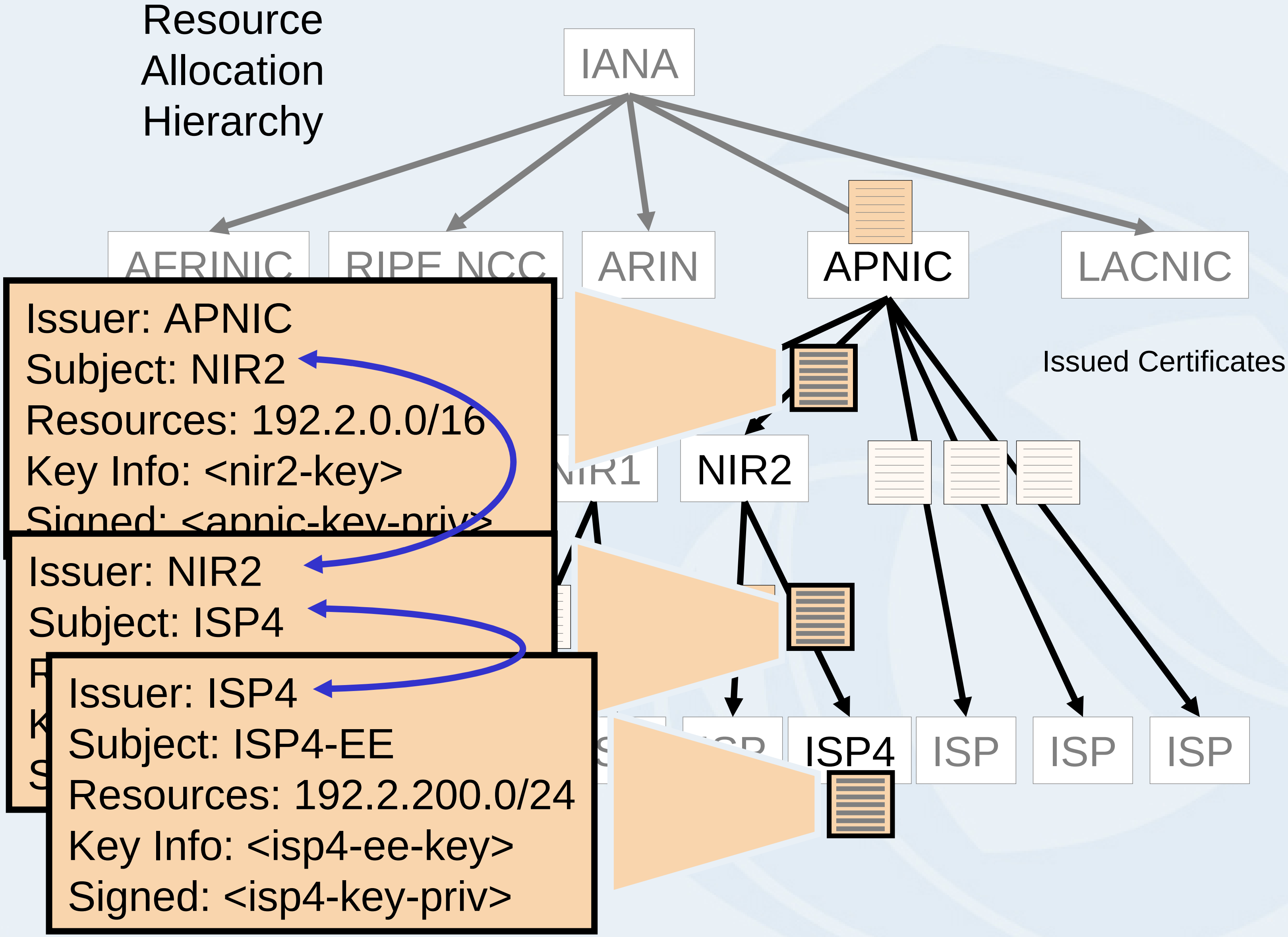
Resource Certificates



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

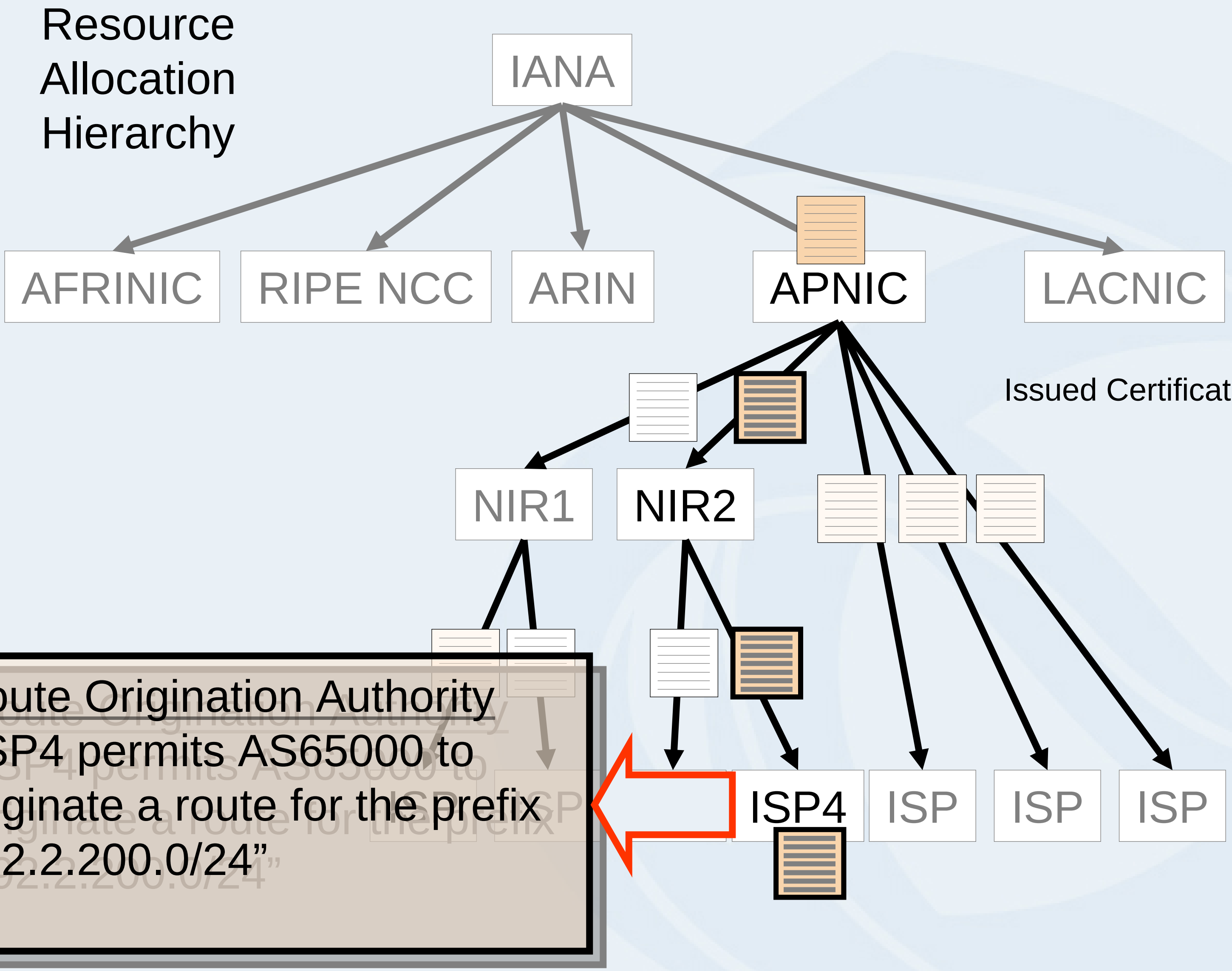


Issuer: APNIC
Subject: NIR2
Resources: 192.2.0.0/16
Key Info: <nir2-key>
Signed: <apnic-key-priv>

Issuer: NIR2
Subject: ISP4
R
K
S

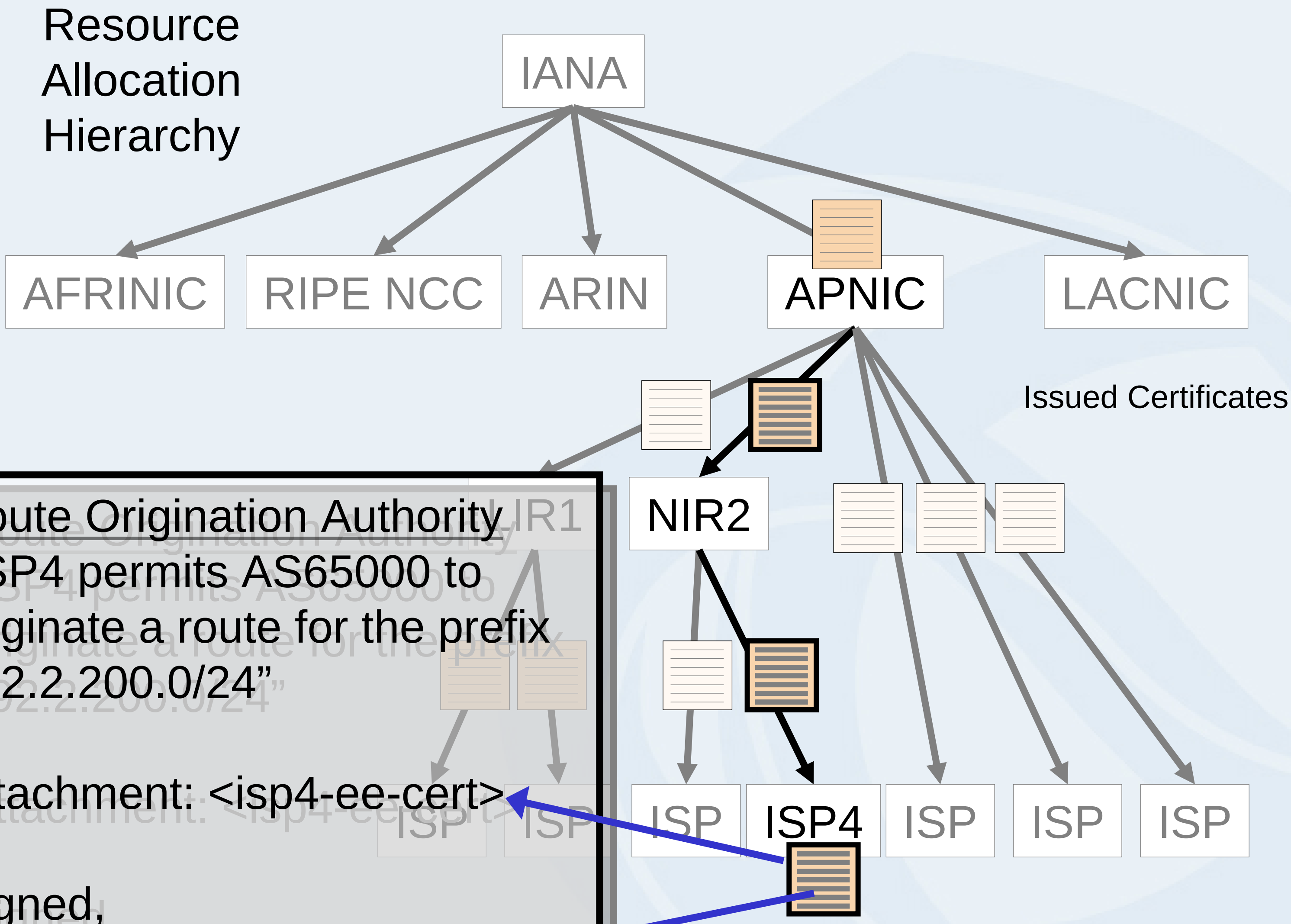
Issuer: ISP4
Subject: ISP4-EE
Resources: 192.2.200.0/24
Key Info: <isp4-ee-key>
Signed: <isp4-key-priv>

Base Object in a Routing Authority Context



<u>Route Origination Authority</u>
"ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24"

Signed Objects



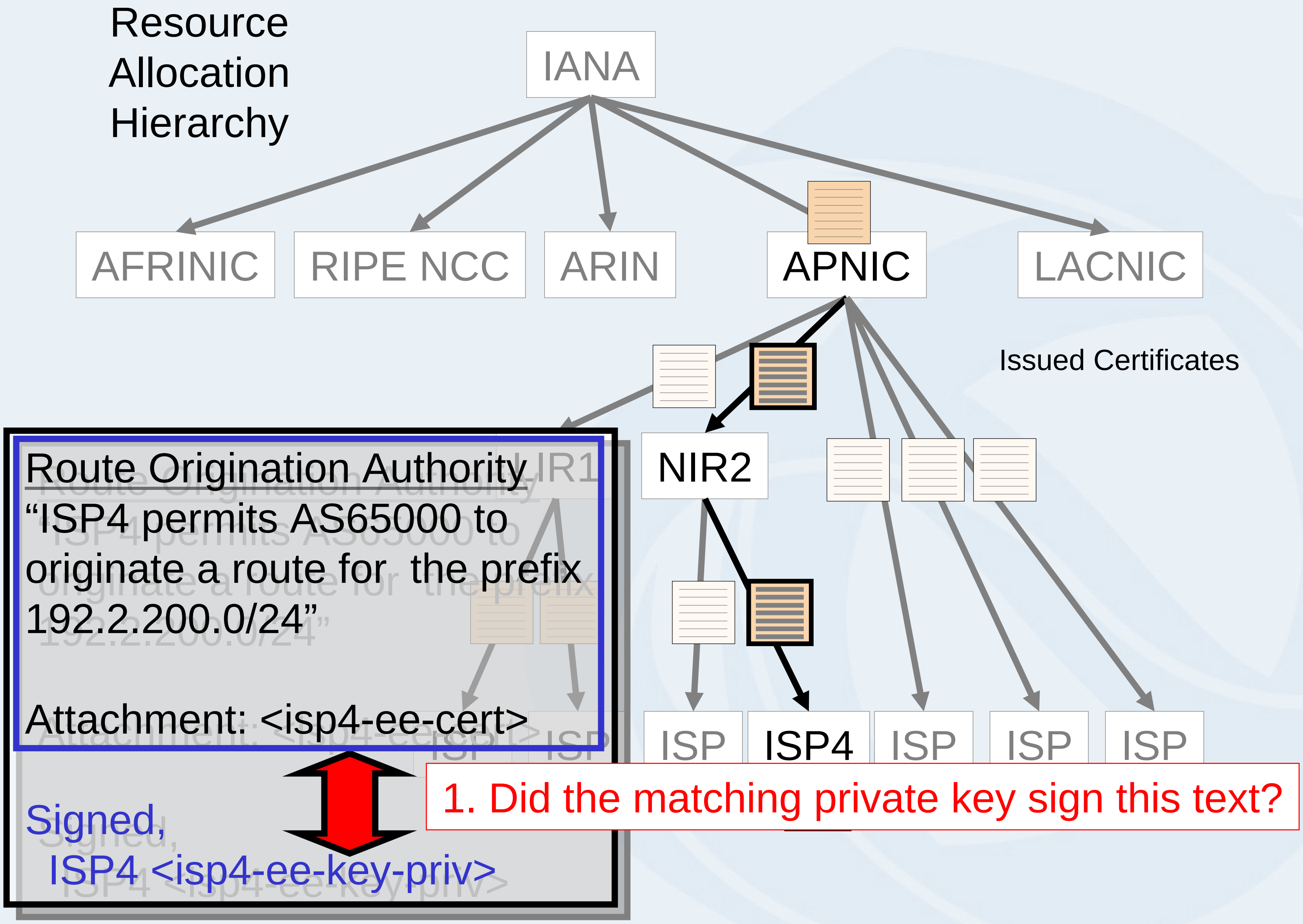
Route Origination Authority

“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



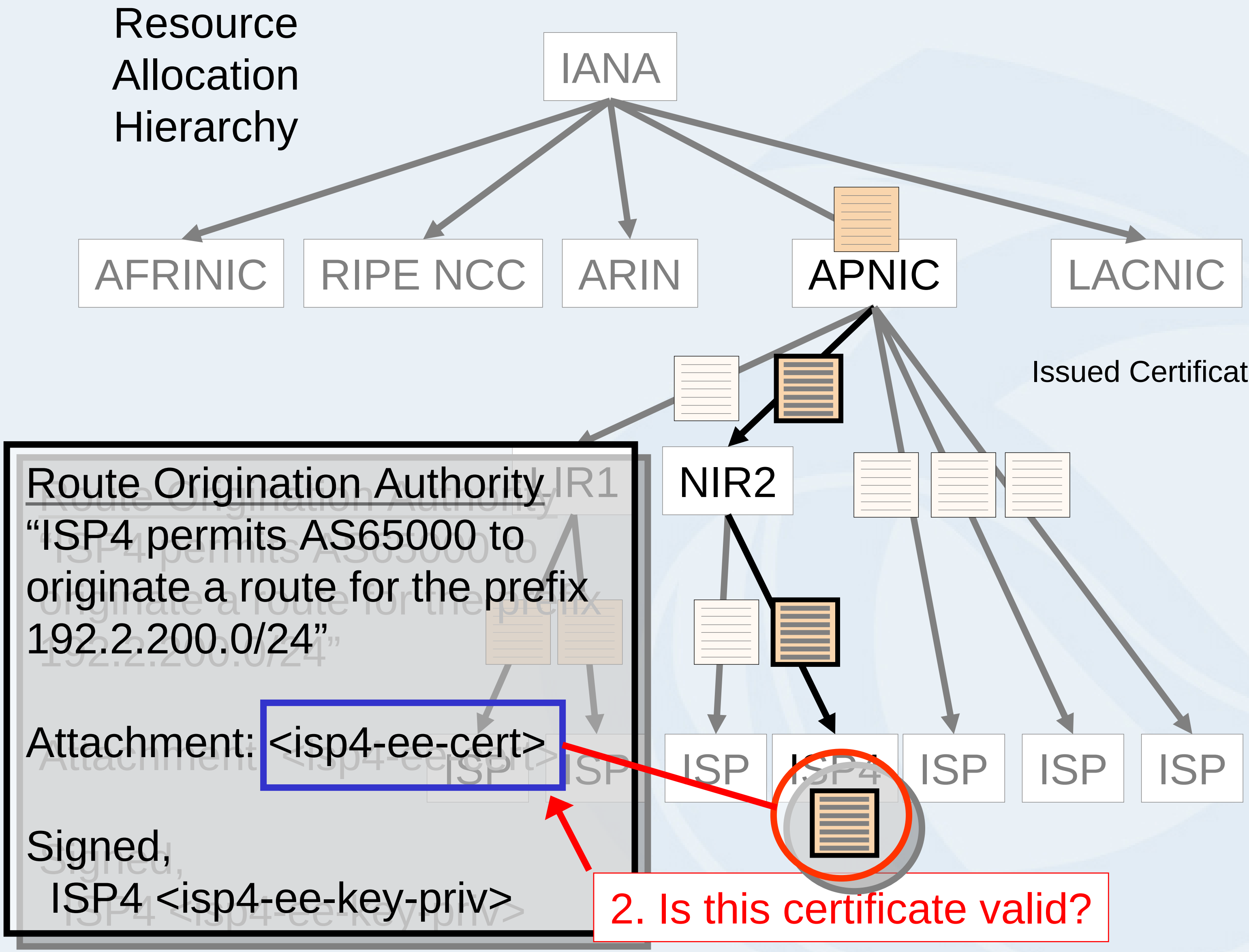
Route Origination Authority
"ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24"

Attachment: <isp4-ee-cert>

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

1. Did the matching private key sign this text?

Signed Object Validation



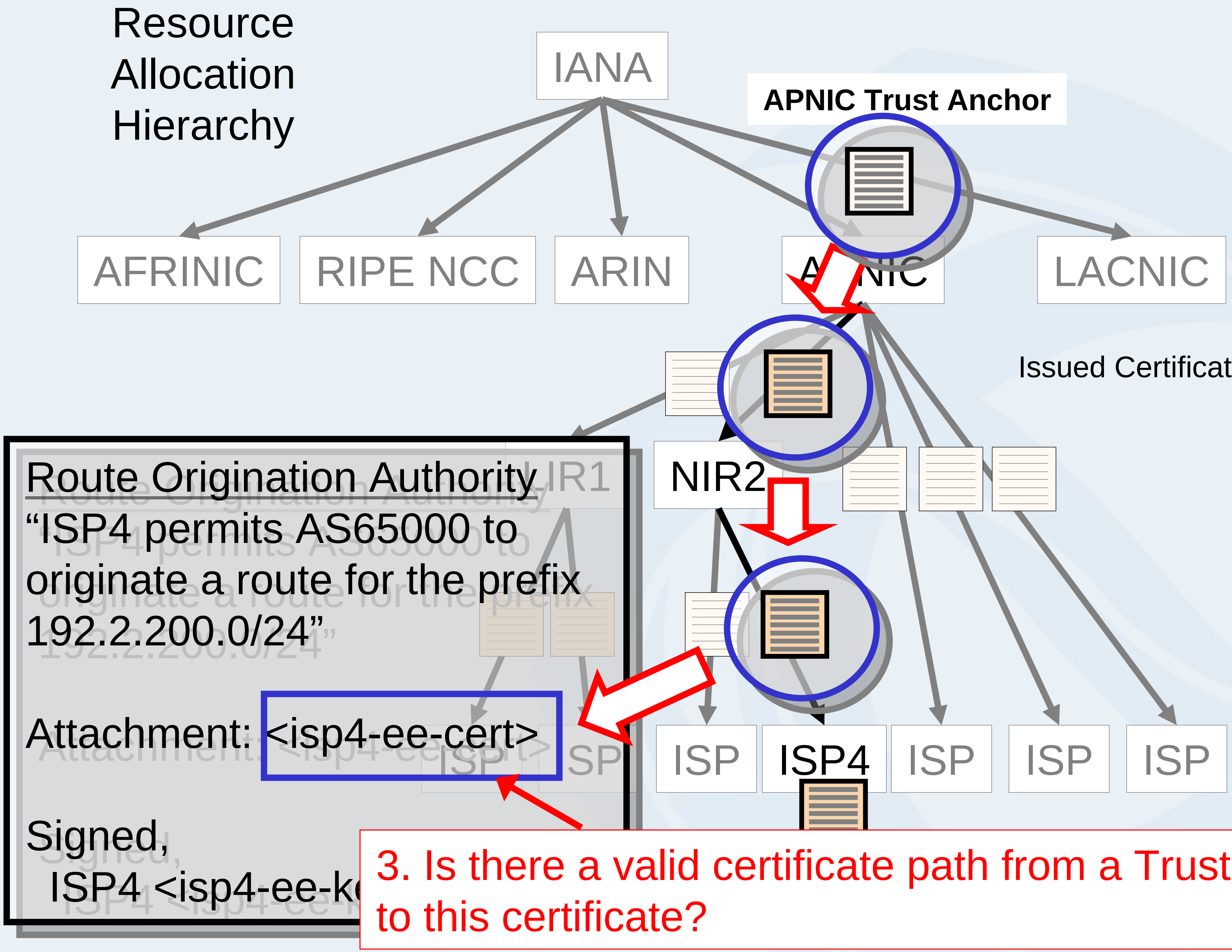
Route Origination Authority
"ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24"

Attachment: <isp4-ee-cert>

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

2. Is this certificate valid?

Signed Object Validation



Route Origination Authority
“ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24”

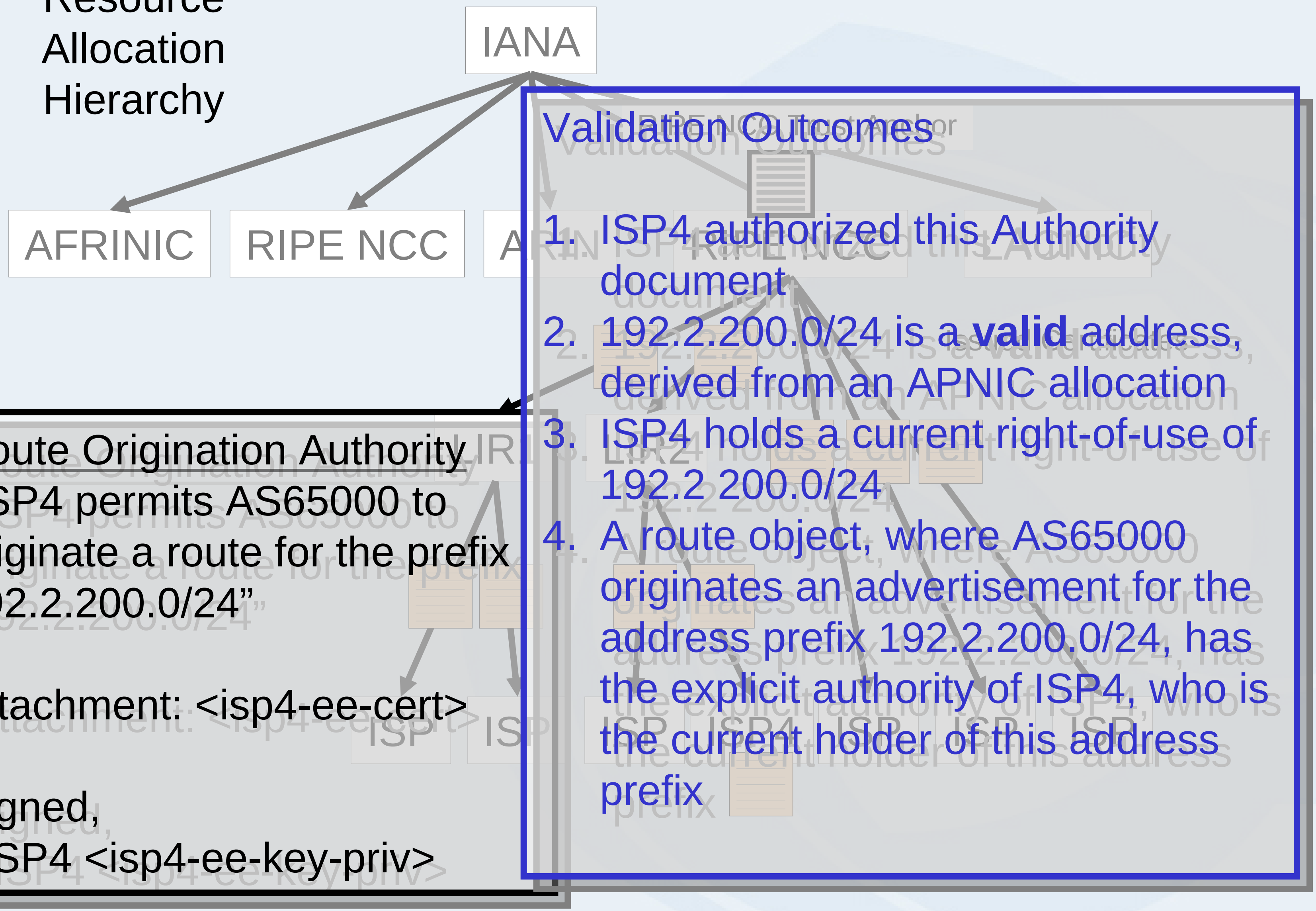
Attachment: <isp4-ee-cert>

Signed,
ISP4 <isp4-ee-k

3. Is there a valid certificate path from a Trust Anchor to this certificate?

Signed Object Validation

Resource
Allocation
Hierarchy



<u>Route Origination Authority</u>
"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>

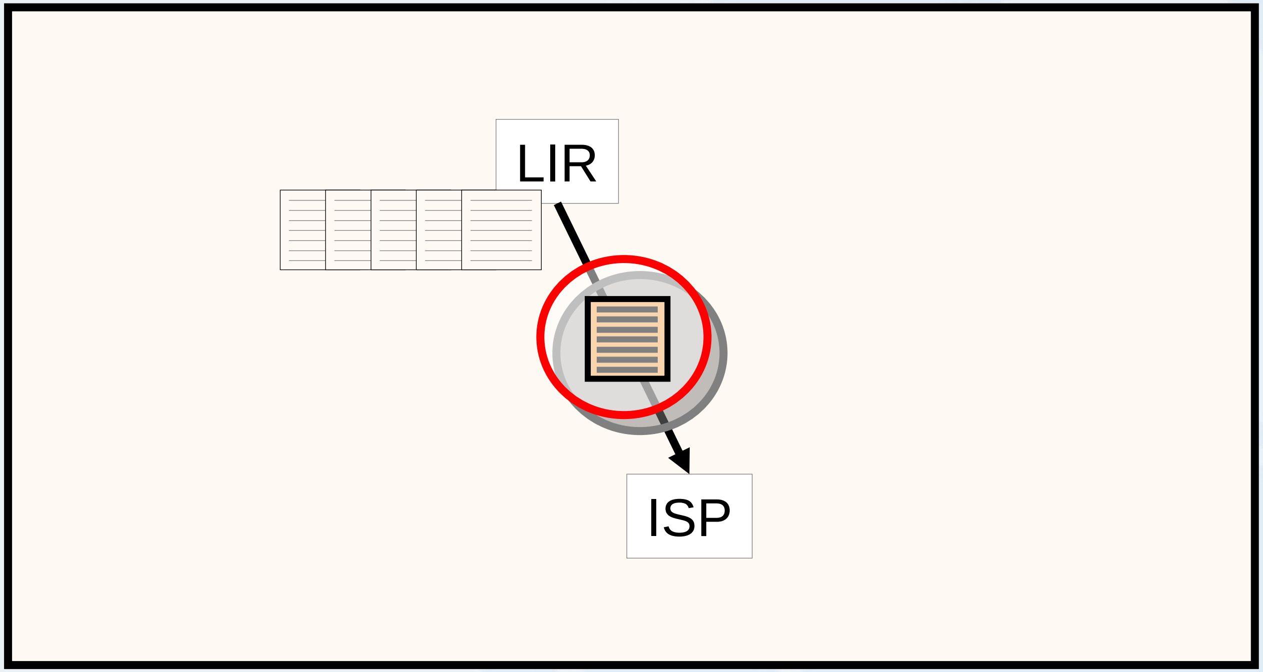
Validation Outcomes

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

What could you do with Resource Certificates?

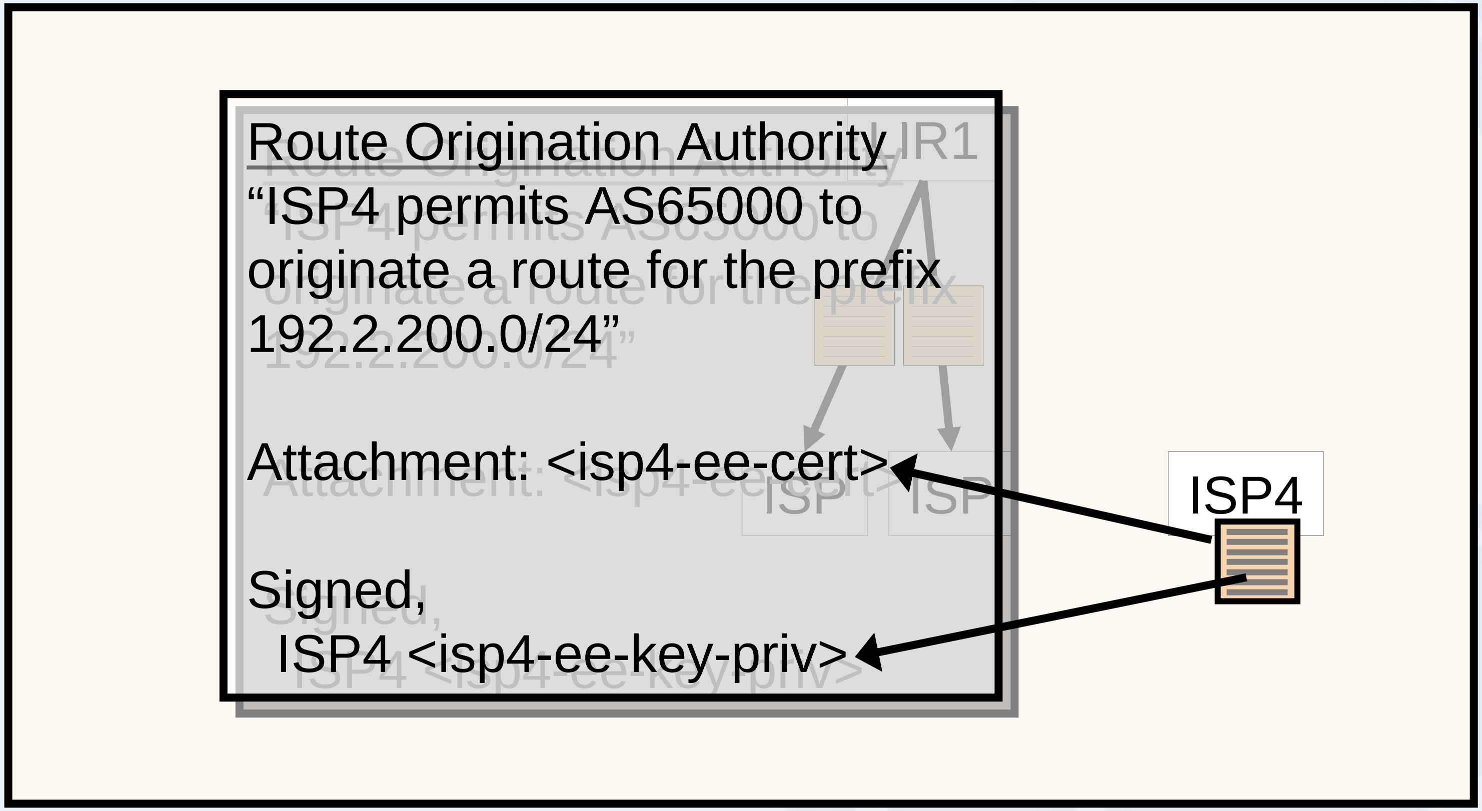
Issue signed subordinate resource certificates for any sub-allocations of resources, such as may be seen in a LIR context

- Maintain a certificate collection that matches the current resource allocation state



What could you do with Resource Certificates?

- **Sign** routing authorities, routing requests, WHOIS objects or IRR objects with your private key
  - Use the private key to sign attestations with a signature that is associated with a right-of-use of a resource



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>

Asia Pacific Network Information Centre

APNIC

What could you do with Resource Certificates?

Validate signed objects

Authentication: Did the resource holder really produce this document or object?

Authenticity: Is the document or object in exactly the same state as it was when originally signed?

Validity: Is the document valid today?

– A relying party can use Resource Certificate tools to:
  - authenticate that the signature matches the signed object,
  - validate the signature against the matching certificate’s public key,
  - validate the certificate in the context of the Resource PKI

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
            Ck010p5Q/Hc4yxwhTamNXW-cDWtQcmvOVGjU.cer
sigblk:     -----BEGIN PKCS7-----
            MIIBdQYJKoZIhvcNAQcCoIIBZjCCAWICAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3
            DQEHATGCAUEwggE9AgEBMBowFTETMBEGA1UEAxMKdGVsc3RyYS1hdQIBATAJBgUr
            DgMCGgUAMA0GCSqGSIb3DQEBAQUABIIBAEZGI2dAG3lAAGi+mAK/S5bsNrgEHOmN
            1leJF9aqM+jVO+tiCvRHyPMeBMiP6yoCm2h5RCR/avP40U4CC3QMhU98tw2Bq0TY
            HZvqXfAOVhjD4Apx4KjiAyr8tfeC7ZDhO+fpvsydV2XXtHIvjwjcL4GvM/gES6dJ
            KJYFWWlrPqQnfTFMm5oLWBUhNjuX2E89qyQf2YZVizITTNg3ly1nwqBoAqmmDhDy
            +nsRVAxax7II2iQDTr/pjI2VWfe4R36gbT8oxyvJ9xz7I9IKpB8RTvPV02I2HbMI
            1SvRXMx5nQOXyYG3Pcxo/PAhbBkVkgfudLki/IzB3j+4M8KemrnVMRo=
            -----END PKCS7-----
changed:    test@telstra.net 20060822
source:     APNIC
```

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
            Ck010p5Q/Hc4yxwhTamNXW-cDWtQcmvOVGjU.cer
sigblk:     -----BEGIN PKCS7-----
            MIIBdQYJKoZIhvcNAQcCoIIBZjCCAWICAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3
            DQEHATGCAUEwggE9AgEBMBowFTETMBEGA1UEAxMKdGVsc3RyYS1hdQIBATAJBgUr
            DgMCGgUAMA0GCSqGSIb3DQEBAQUABIIBAEZGI2dAG3lAAGi+mAK/S5bsNrgEHOmN
            1leJF9aqM+jVO+tiCvRHyPMeBMiP6yoCm2h5RCR/avP40U4CC3QMhU98tw2Bq0TY
            HZvqXfAOVhjD4Apx4KjiAyr8tfeC7ZDhO+fpvsydV2XXtHIvjwjcL4GvM/gES6dJ
            KJYFWWlrPqQnfTFMm5oLWBUhNjuX2E89qyQf2YZVizITTNg3ly1nwqBoAqmmDhDy
            +nsRVAxax7II2iQDTr/pjI2VWfe4R36gbT8oxyvJ9xz7I9IKpB8RTvPV02I2HbMI
            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
           Ck010p5Q/Hc4yxwhTamNXW-cDWtQcmvOVGjU
Key Usage: DigitalSignature, nonRepudiation
CRL Distribution Points:
           rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5
           Ck010p5Q.crl
Authority Info Access: caIssuers –
           rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5
           Ck010p5Q.cer
Authority Key Identifier:
           Key Identifier g(AKI): cbh3Sk-iwj8Yd8uqaB5Ck010p5Q
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
```

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
            Ck010p5Q/Hc4yxwhTamNXW-cDWtQcmvOVGjU
Key Usage: DigitalSignature, nonRepudiation
CRL Distribution Points:
            rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5
            Ck010p5Q.crl
Authority Info Access: caIssuers –
            rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5
            Ck010p5Q.cer
Authority Key Identifier:
            Key Identifier g(AKI): cbh3Sk-iwj8Yd8uqaB5Ck010p5Q
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
```

Potential Use Scenarios

Service interface via a Web Portal:

- Generate and Sign “objects”
- Validate signed objects against the PKI
- Manage subordinate certificate issuance
  - (Automated certificate management processes)

Local Tools – LIR Use

- Local repository management
- Resource object signing
- Generate and lodge certificate objects
- Local certificate cache management
- Validate signed objects against the PKI

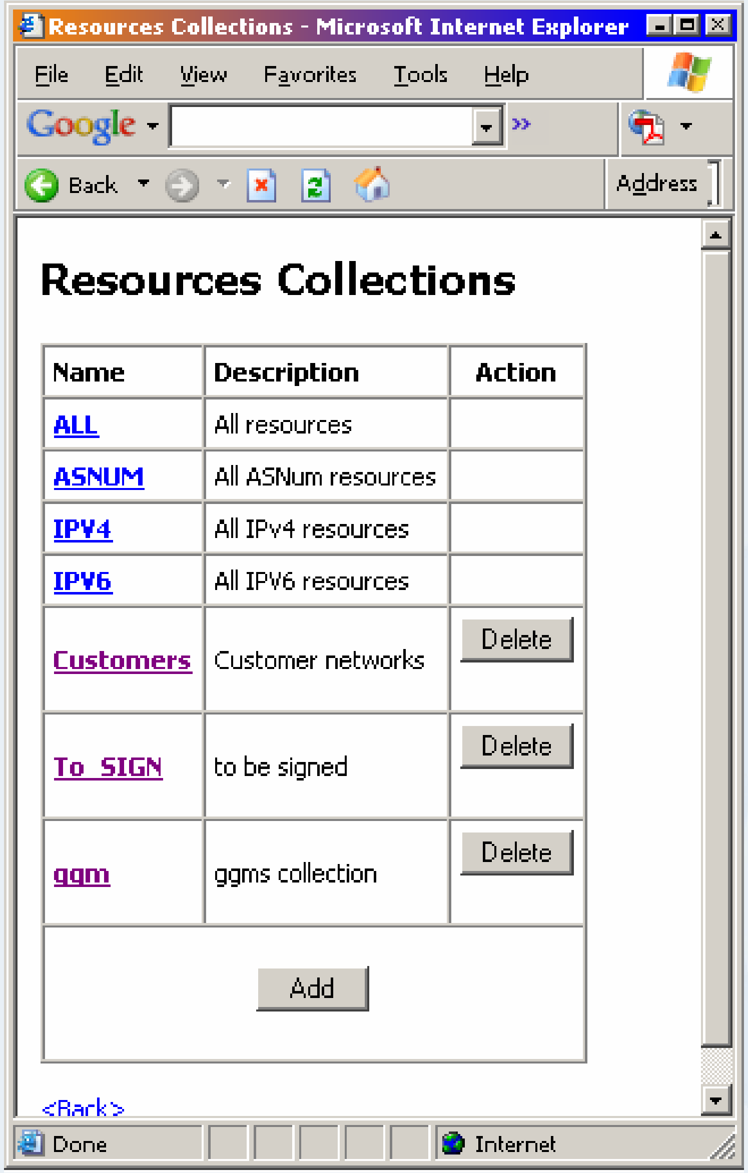
Demonstration - Signing

The Setup:

- Web Portal interface using REST framework
- Local instance of an ISP
  - Issued Certificate set matching allocated resources
  - Local CA and key manager
  - End-Entity Certificate Manager
  - Resource Collection Manager
  - Signed Object Manager

An ISP can sign objects using resource collections

Resource Collection Tool


Resources Collections - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Google
Back
Address
Done
Internet

Resources Collections

Name	Description	Action
ALL	All resources	
ASNUM	All ASNum resources	
IPV4	All IPv4 resources	
IPV6	All IPV6 resources	
Customers	Customer networks	Delete
To_SIGN	to be signed	Delete
ggm	ggms collection	Delete

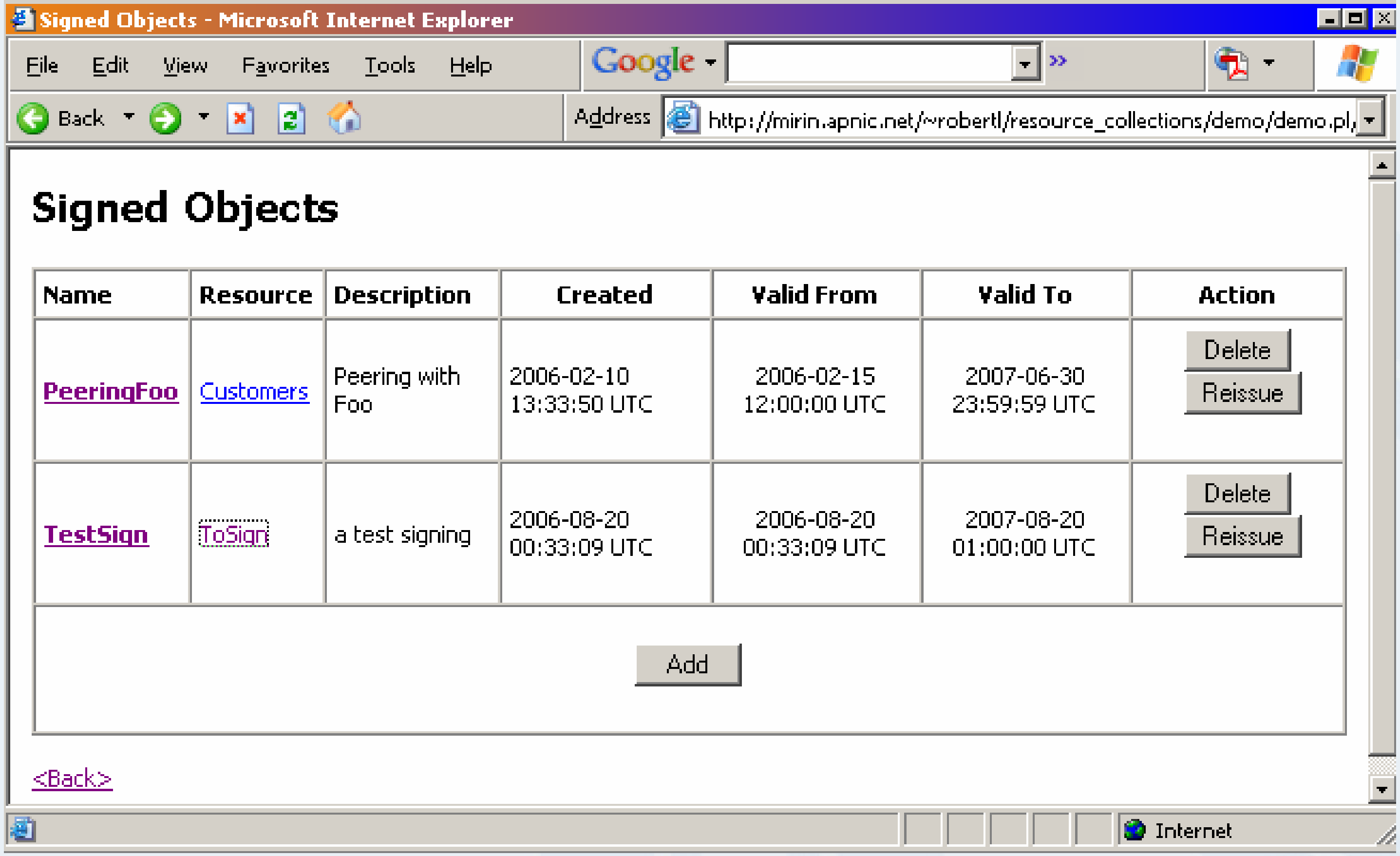
Add

<Back>

Resources can be subdivided into “collections” and each collection can be named. This section of the portal provides tools to manage resource collections

A resource collection is used to sign a document (or any other digital object)

Resource Signing Tool


Signed Objects - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Google
Back
Address http://mirin.apnic.net/~robertl/resource_collections/demo/demo.pl
Internet

Signed Objects

Name	Resource	Description	Created	Valid From	Valid To	Action
PeeringFoo	Customers	Peering with Foo	2006-02-10 13:33:50 UTC	2006-02-15 12:00:00 UTC	2007-06-30 23:59:59 UTC	Delete Reissue
TestSign	ToSign	a test signing	2006-08-20 00:33:09 UTC	2006-08-20 00:33:09 UTC	2007-08-20 01:00:00 UTC	Delete Reissue

Documents can be signed with a resource collection, and associated validity dates. Signed objects can also be reissued and deleted

The underlying resource certificate generation and management tasks are not directly exposed in this form of the signing tool

A Plea to the Demonstration Gods…

I received the following note about this code:….

“In all of the combinations I've tested, it seems to work.

Geoff, you will want to double check the particular examples you want to demonstrate, but it should work.”

So, with some trepidation………

Demonstration - Validation

The Setup:

- Local instance of a signed object validator
  - Local Trust Anchors
  - Local (partial) copy of a synchronized certificate collection
  - Takes a signed object and checks the integrity of the object, that the listed public keys match the signatures of the object, and that the certificates in the object are all valid (using Local Trust Anchors)
  - Reports the resources used to sign the object.

Resource Certificate Trial Program

- ✓ 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

Next Steps ...

1. Complete current trial activities by EOY 06
2. APNIC Evaluation of Trial activities
   - Status of work items
   - Does this approach meet the objectives?
   - What are the implications of this form of certification of resources?
   - Impact assessment
     - Service infrastructure, operational procedures
     - Utility of the authentication model
     - Policy considerations
   - Recommendations for production deployment

Credit where credit is due…..

- The design and implementation team involved in this trial:
  - George Michaelson
  - Rob Loomans
  - Geoff Huston
  - Randy Bush
  - Rob Austein
  - Rob Kisteleki
  - Steve Kent
  - Russ Housley

- Working notes and related material we’ve been working on in this trial activity are at

  http://mirin.apnic.net/resourcecerts

Thank You