Using Resource Certificates

Progress Report on the Trial of Resource Certification

October 2006

Geoff Huston

From the RIPE Address Policy Mail List…

22 – 25 Sept 06, address-policy-wg@lists.ripe.net

Joao Damas:

> Though hopefully it will have public records for ISPs to see who has been assigned the IP block through the established process, right?

From the RIPE Address Policy Mail List…

22 – 25 Sept 06, address-policy-wg@lists.ripe.net

Joao Damas:

> Though hopefully it will have public records for ISPs to see who has been assigned the IP block through the established process, right?

Randy Bush:

> If we are lucky, this time next year, you will be able to verify an X.509 certificate chain with rfc 3779 resource extensions, and have significant confidence in rights to address and asn resources.

From the RIPE Address Policy Mail List…

22 – 25 Sept 06, address-policy-wg@lists.ripe.net

Joao Damas:

> Though hopefully it will have public records for ISPs to see who has been assigned the IP block through the established process, right?

Randy Bush:

> If we are lucky, this time next year, you will be able to verify an X.509 certificate chain with rfc 3779 resource extensions, and have significant confidence in rights to address and asn resources.

Max Tulyev:

> As I can understand, I can verify origin of prefix, prefix itself, but it can't authorize is that certain as-path legitimate or not. Like I can figure it out from routing registry DB. Isn't it?

From the RIPE Address Policy Mail List…

22 – 25 Sept 06, address-policy-wg@lists.ripe.net

Joao Damas:

Though hopefully it will have public records for ISPs to see who has been assigned the IP block through the established process, right?

Randy Bush:

If we are lucky, this time next year, you will be able to verify an X.509 certificate chain with rfc 3779 resource extensions, and have significant confidence in rights to address and asn resources.

Max Tulyev:

As I can understand, I can verify origin of prefix, prefix itself, but it can't authorize is that certain as-path legitimate or not. Like I can figure it out from routing registry DB. Isn't it?

Randy Bush:

The current work will provide a formally verifiable demonstration of [right-of-use] of address space. To achieve your goal _formally_ will require something like sbgp. The irr is an informal way to kinda achieve what you want. And we use it today.

One first useful step for an ISP is to use the x.509 data to verify ownership assertions in the irr when building filter lists, for example.

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?

What would be good ...

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

- Allow third parties to authenticate that an address or routing assertion was made by the current right-of-use holder of the address resource
- Confirm that the asserted information is complete and unaltered from the original
- Convey routing authorities from the resource holder to a nominated party that cannot be altered or forged

Resource Certificate Trial

Parameters:

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

Approach:

- Use X.509 v3 Public Key Certificates (RFC3280) with IP address and ASN extensions (RFC3779), using OpenSSL as the foundation platform for the trial

Resource Public Key Certificates

The certificate's Issuer certifies that:

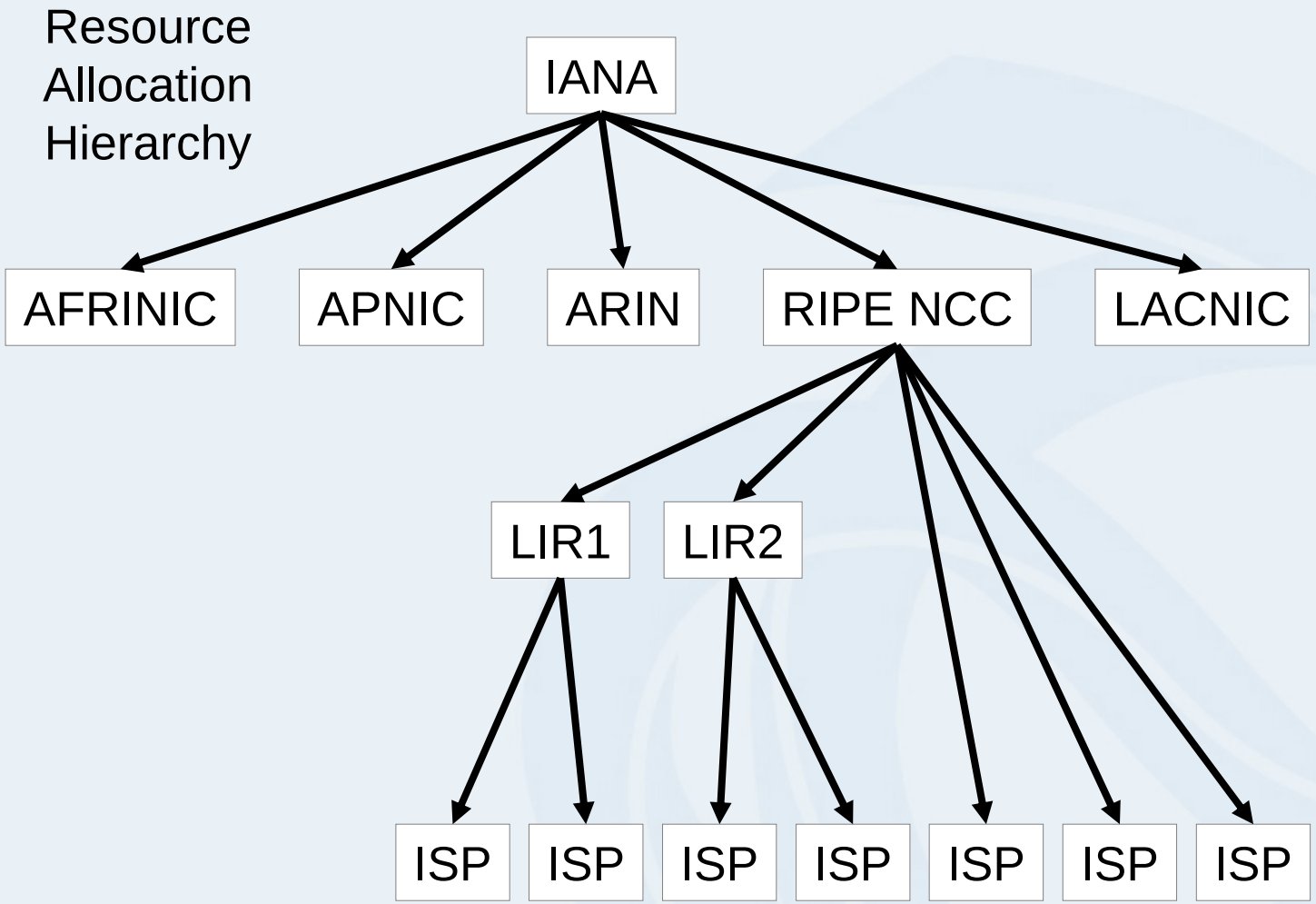
the certificate's Subject

whose public key is contained in the certificate

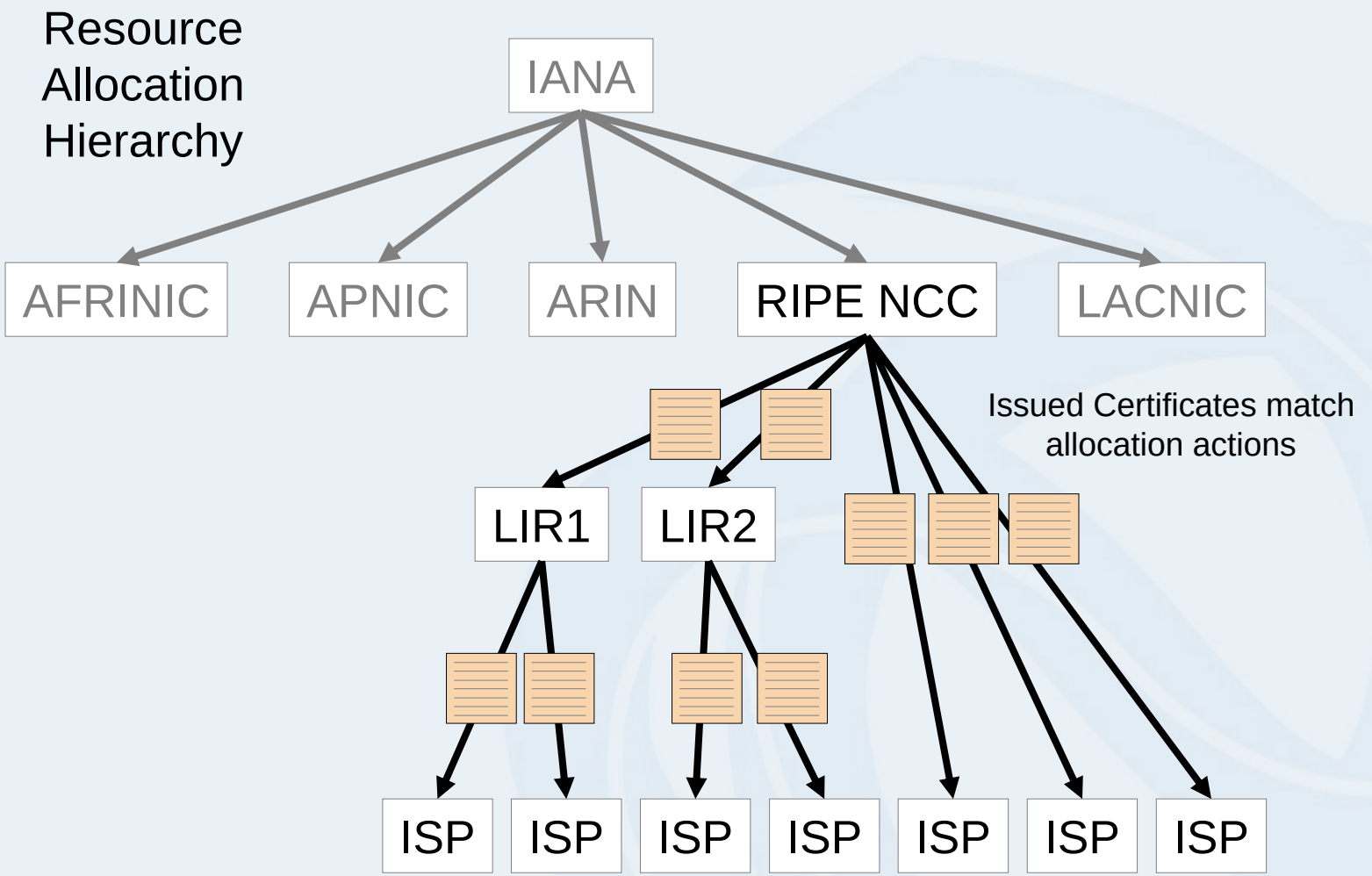
is the current controller of a collection of IP address and AS resources

that are listed in the certificate's resource extension

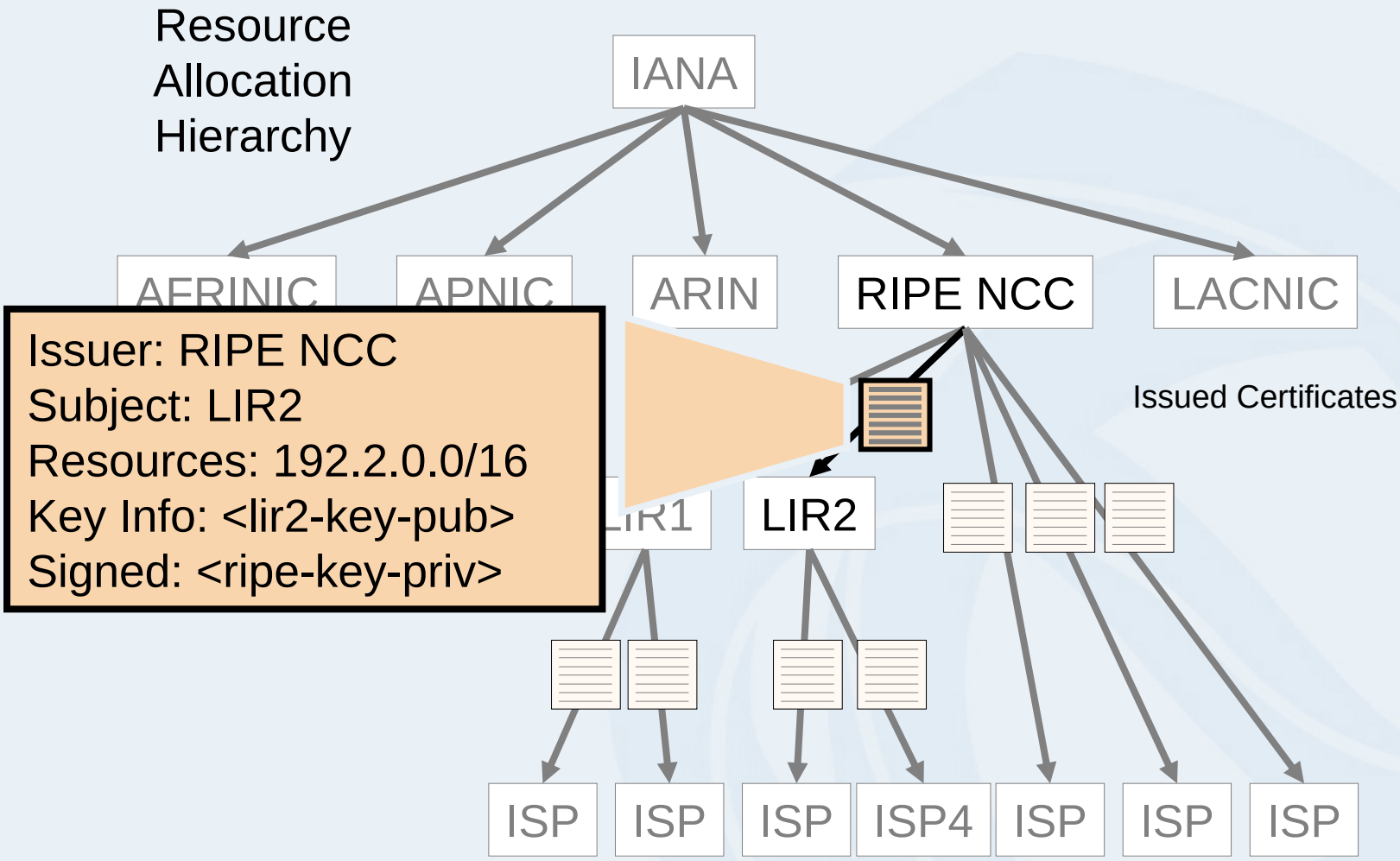
Resource Certificates



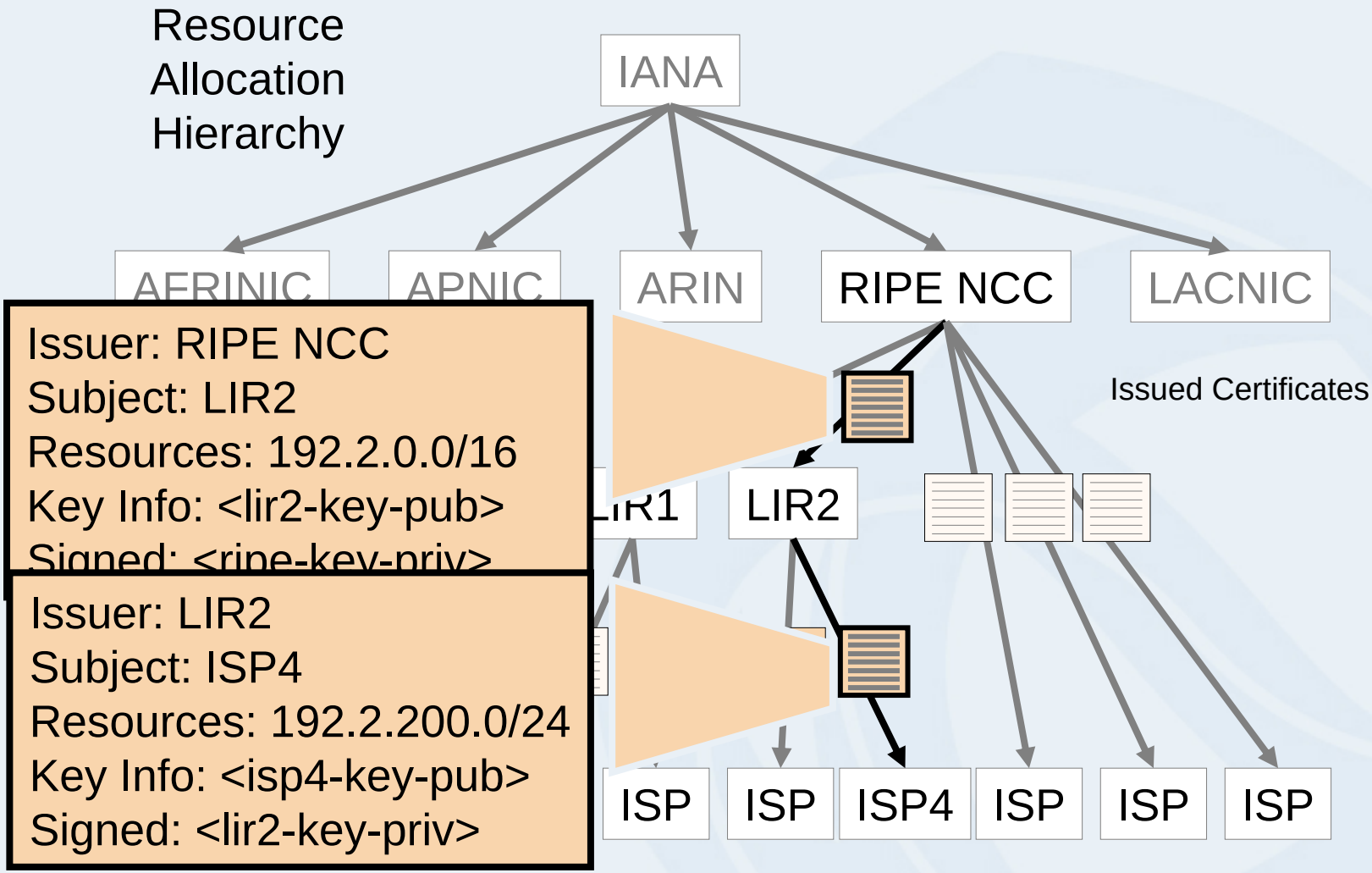
Resource Certificates



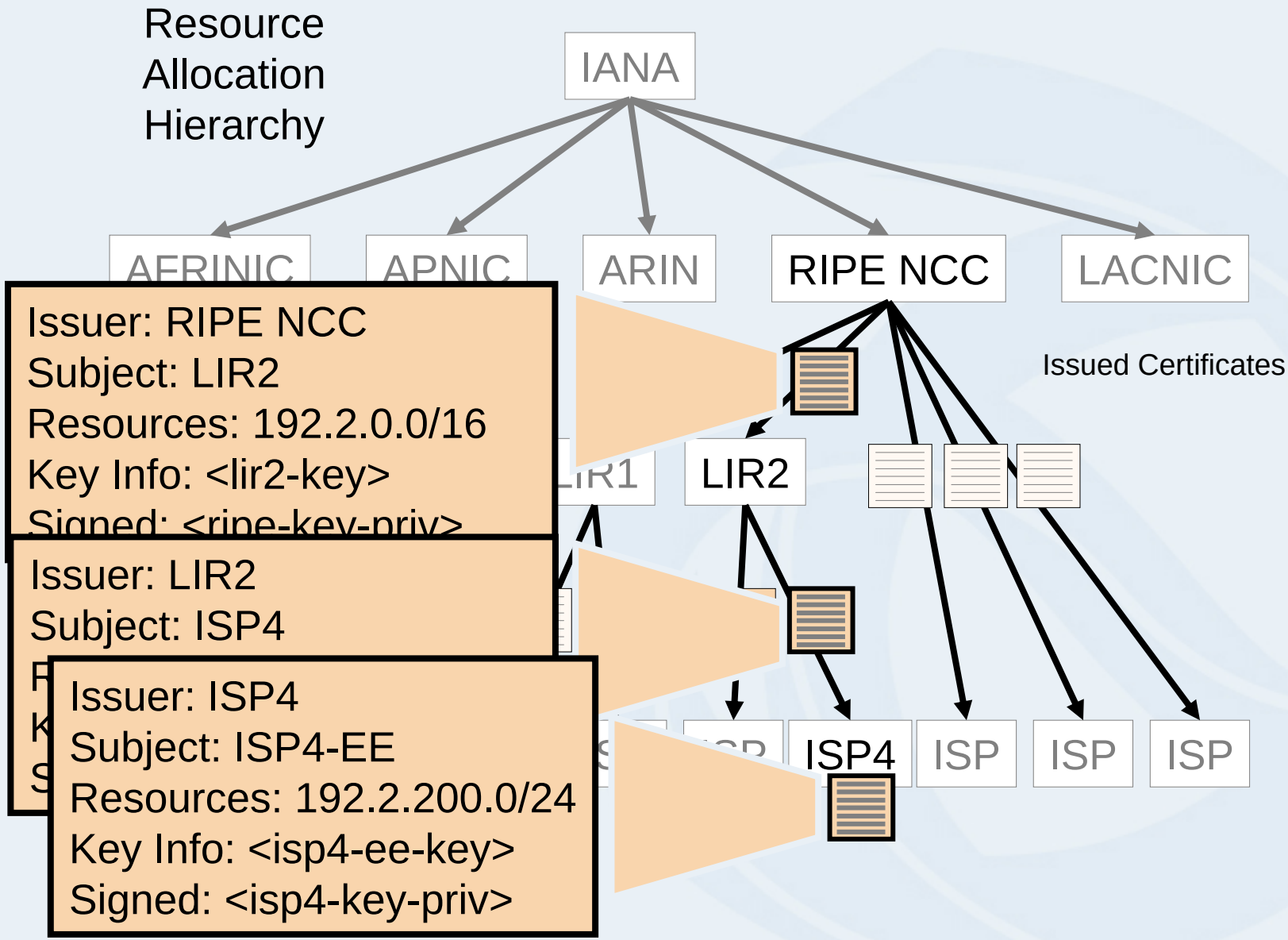
Resource Certificates



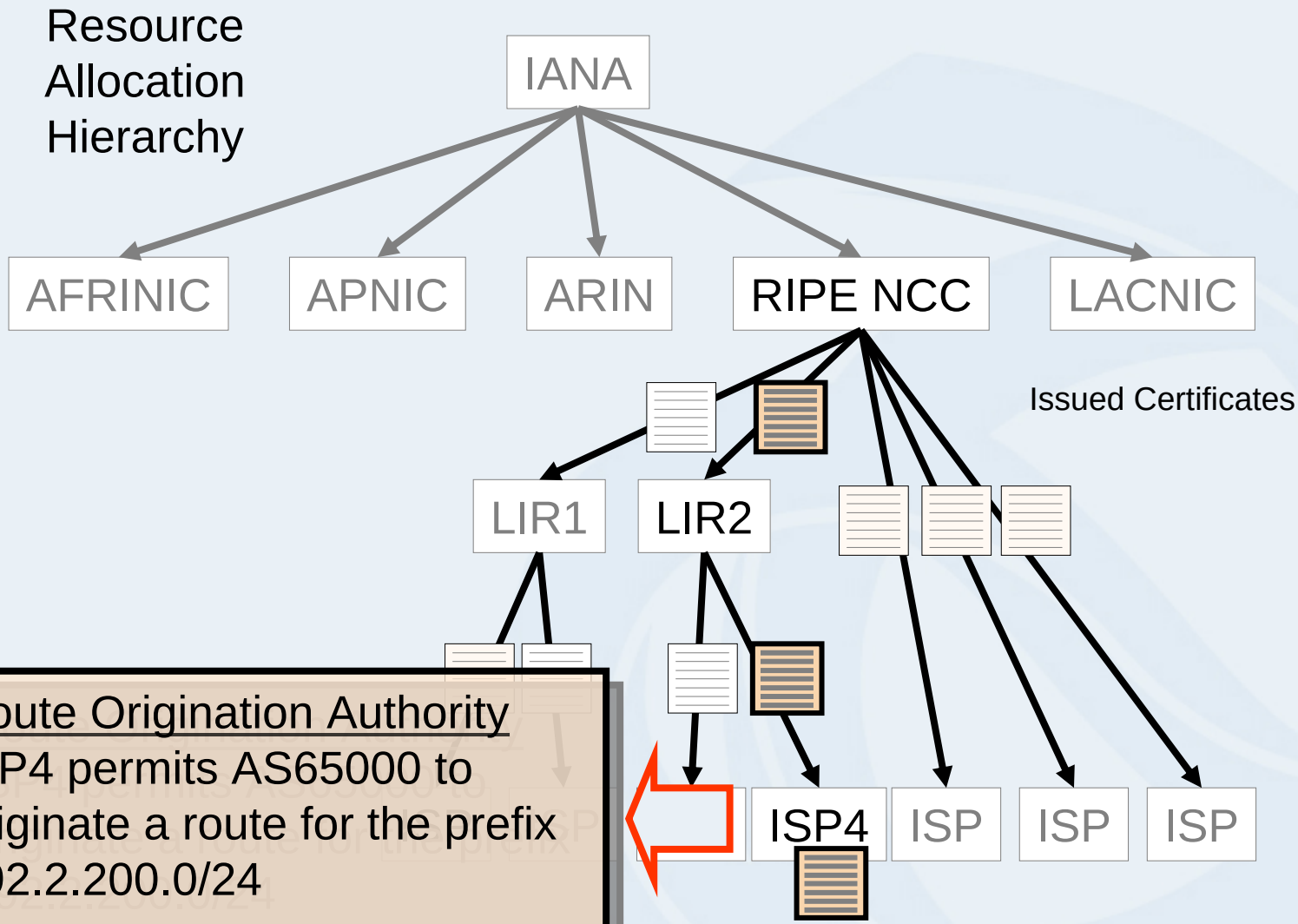
Resource Certificates



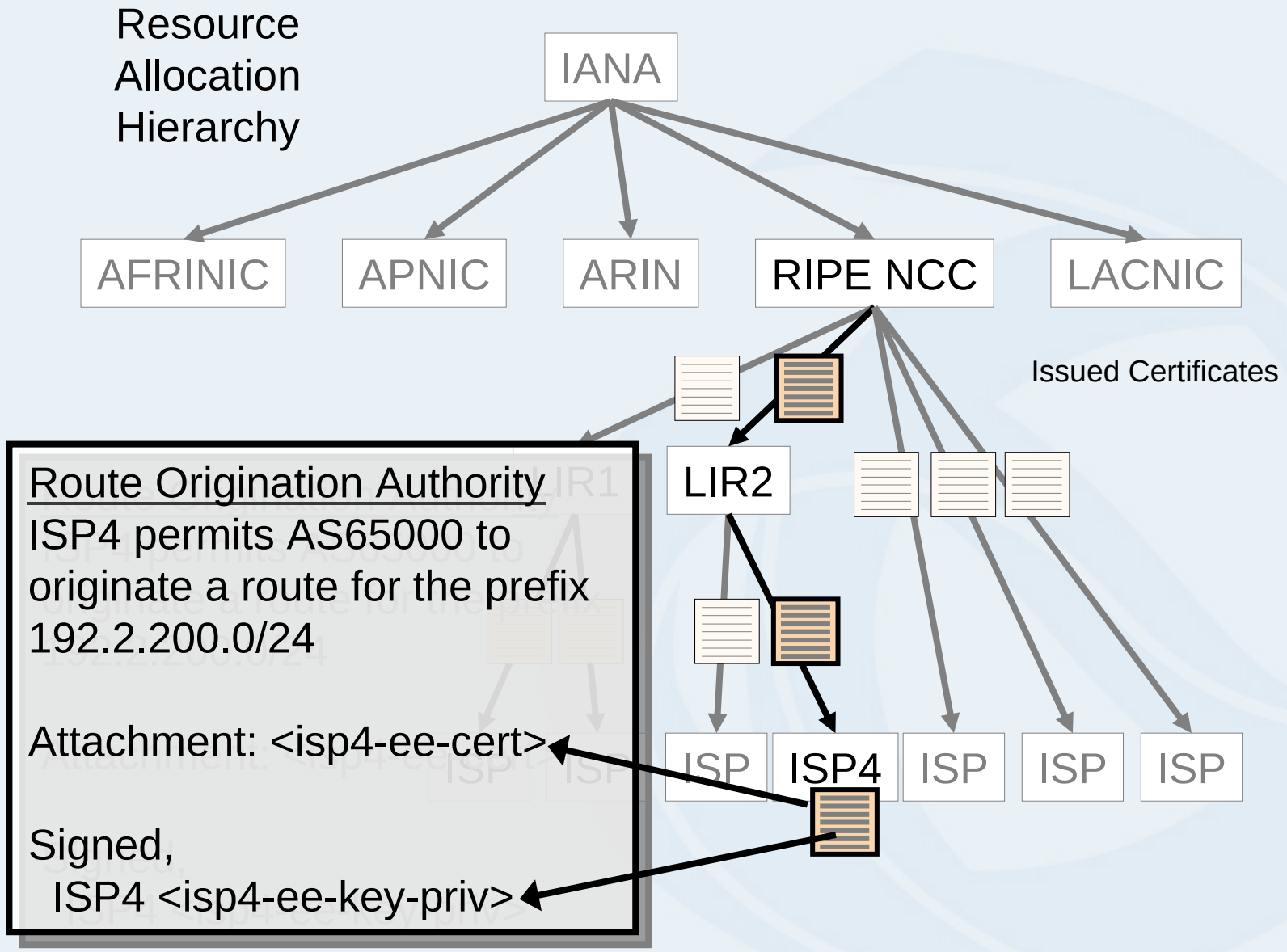
Resource Certificates



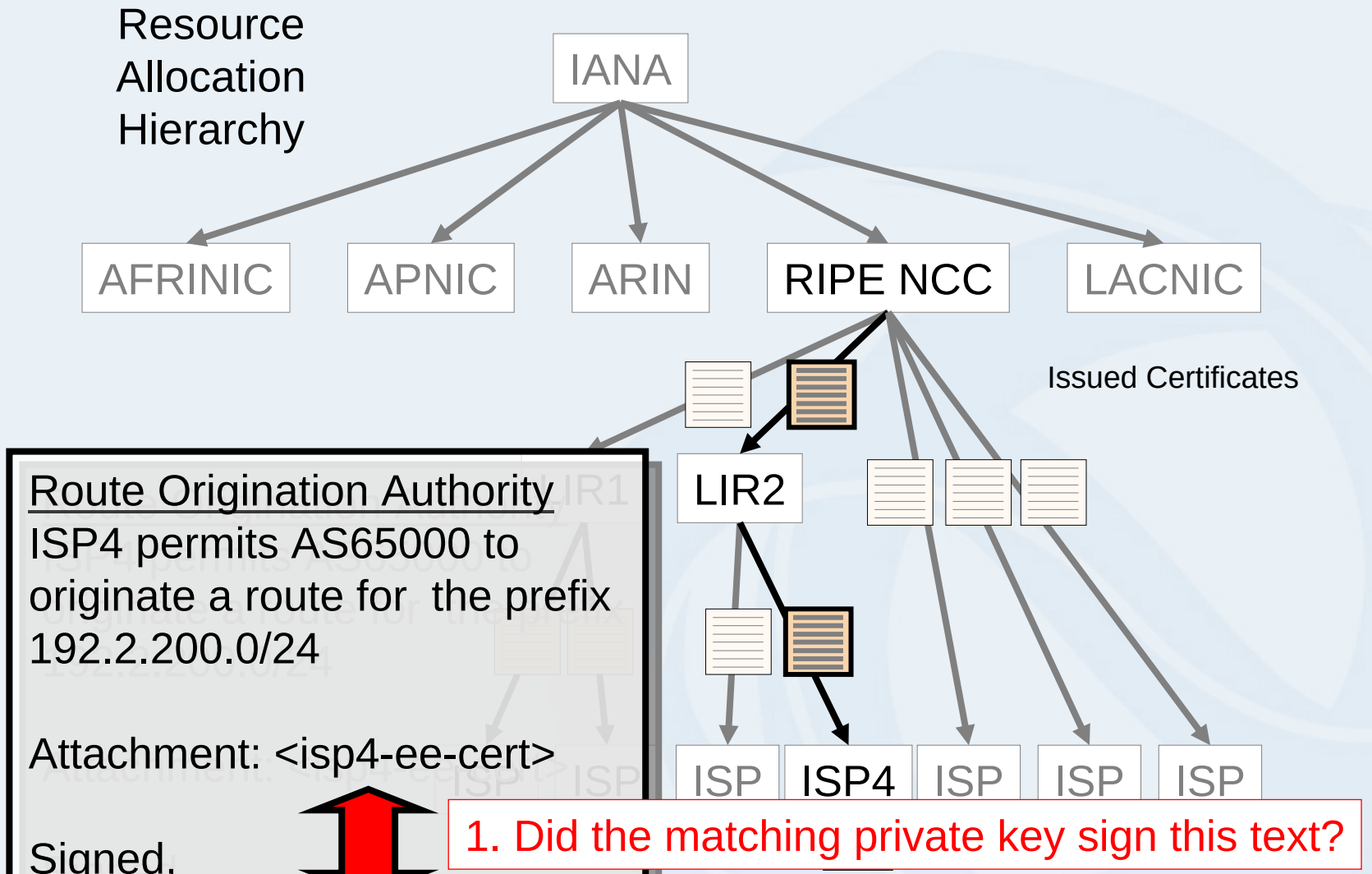
Signed Objects



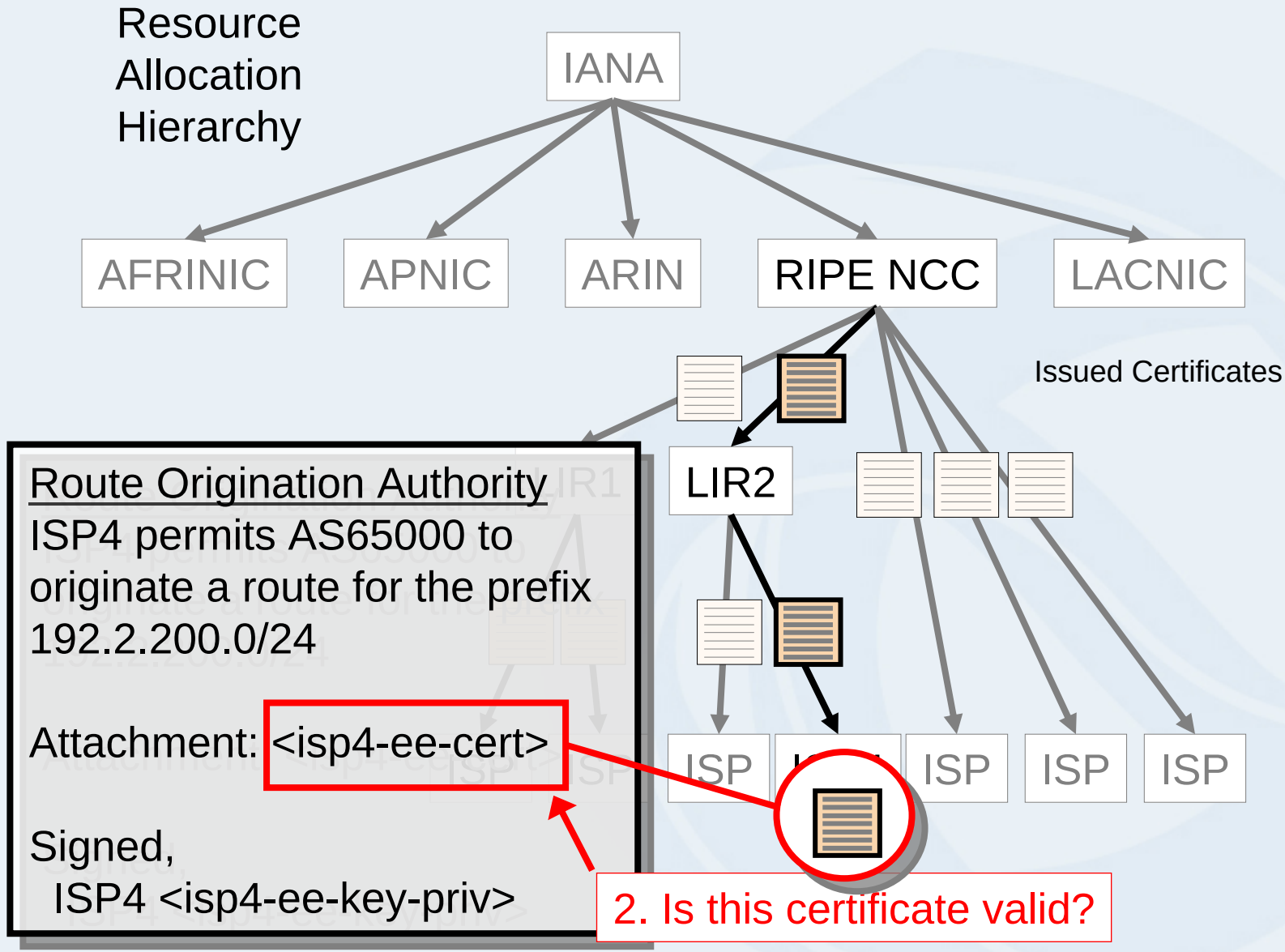
Signed Objects



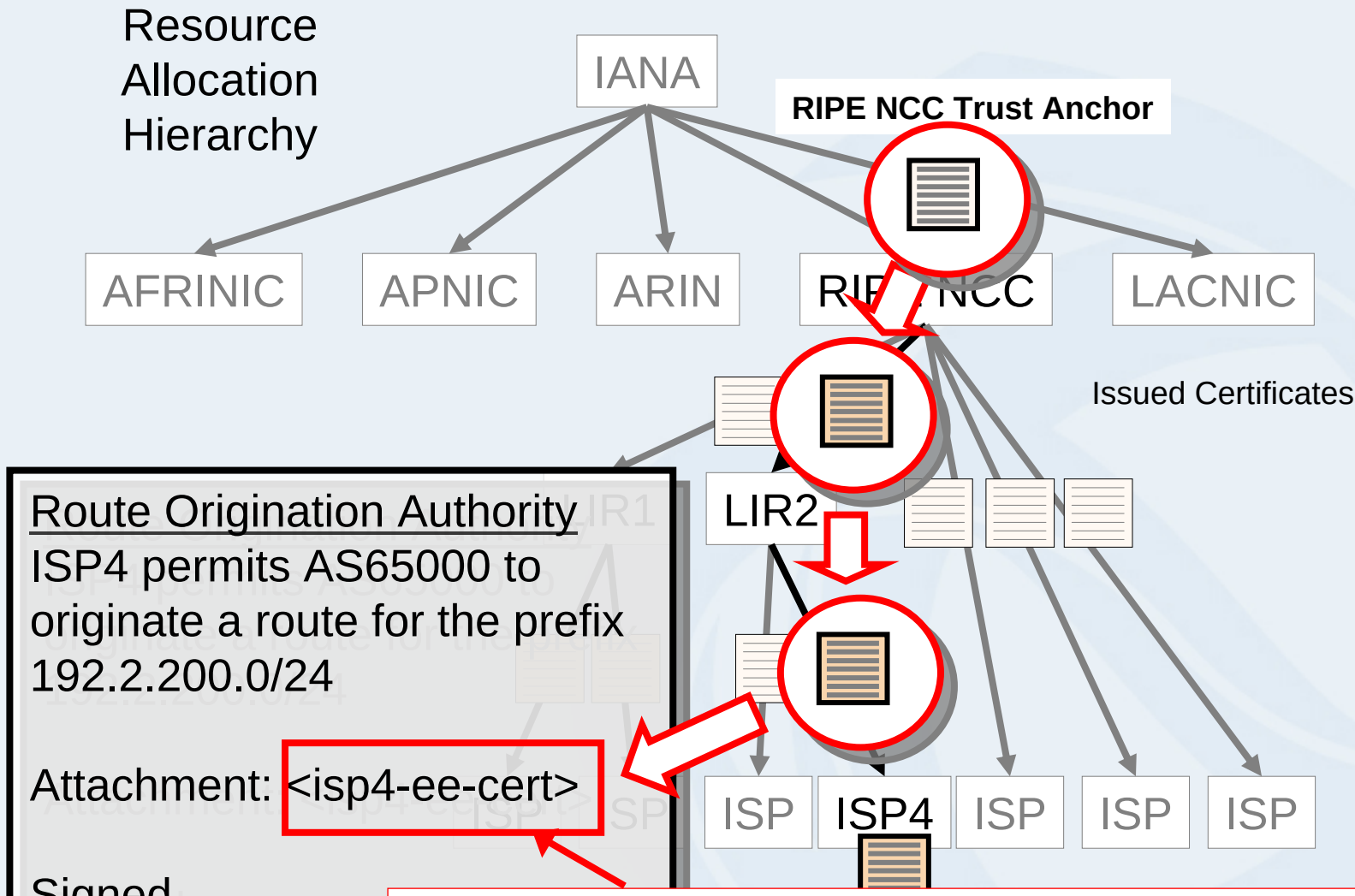
Signed Object Validation



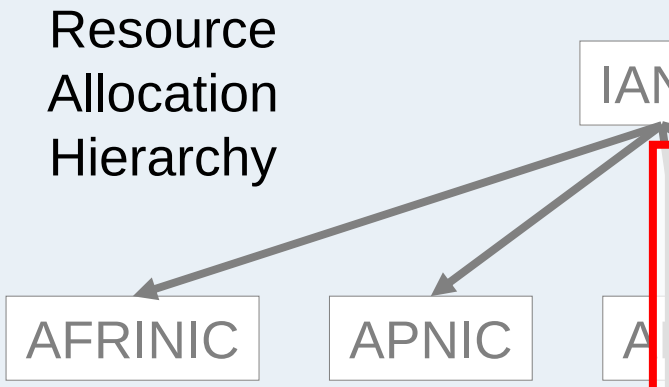
Signed Object Validation



Signed Object Validation



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>

Validation Outcomes

1. ISP4 authorized this Authority document
2. 192.2.200.0/24 is a valid address
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, or WHOIS objects or IR 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

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:
  - 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

```
route-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/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
           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
```

Potential Scenarios

Service interface via a Web Portal:

- Generate and Sign routing-related 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

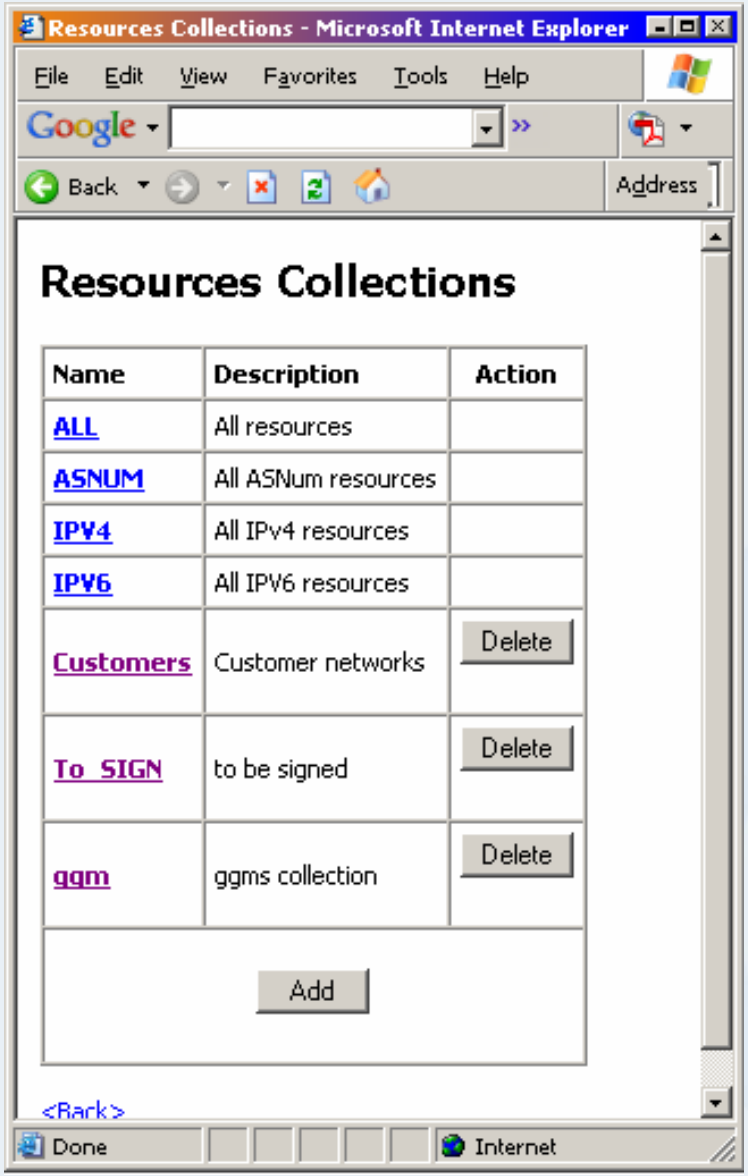
Demonstration - Signing

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

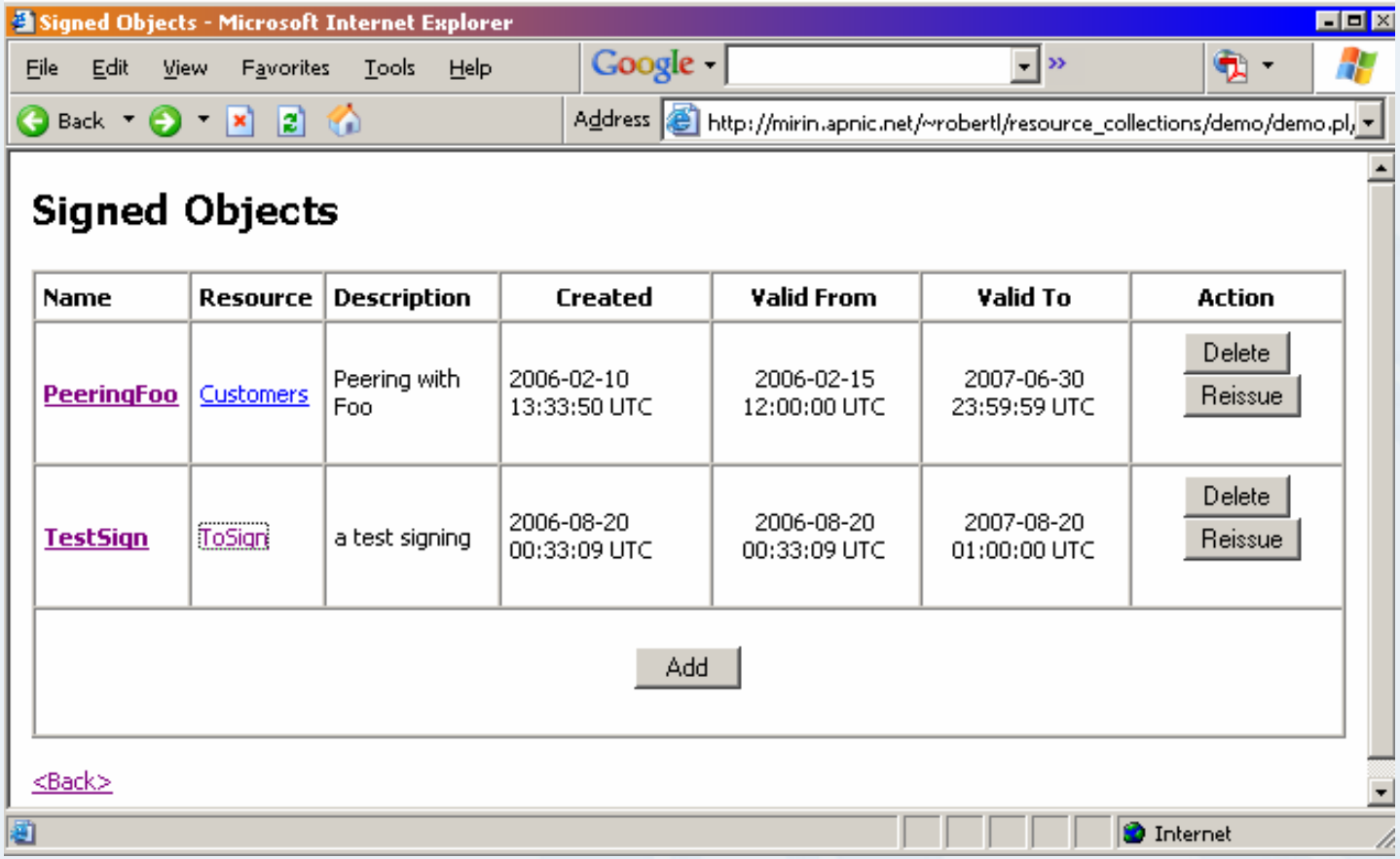
Resource Signing Tool



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



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

Demonstration - Validation

The Setup:

- Local instance of a signed object validator
  - 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 the RIR keys as 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
- ✸ Operational service profile specification

Next Steps …

- Complete current trial activities by EOY 06
- 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

Thank You

Questions?