Asia Pacific Network Information Centre

APNIC

APRICOT BALI 2007

Progress Report on resource certification

February 2007

Geoff Huston
Chief Scientist
APNIC

Objective

- To create a robust framework that allows validation of assertions relating to IP addresses and ASNs and their use

and

- To make it easier for anyone to see if someone is lying about actual control over addresses and/or routing!

Uses

- Signing of IRR entries

  "Yes, I am the right-of-use holder and that's *precisely* the information I entered into the IRR."

- Signing of Routing Origination

  "Yes, I am the right-of-use holder for this address prefix and I am permitting ASx to originate a route to this address prefix."

- Signing of Route Requests

  "Please route address prefix a.b.c.d/x through customer interface xxx."

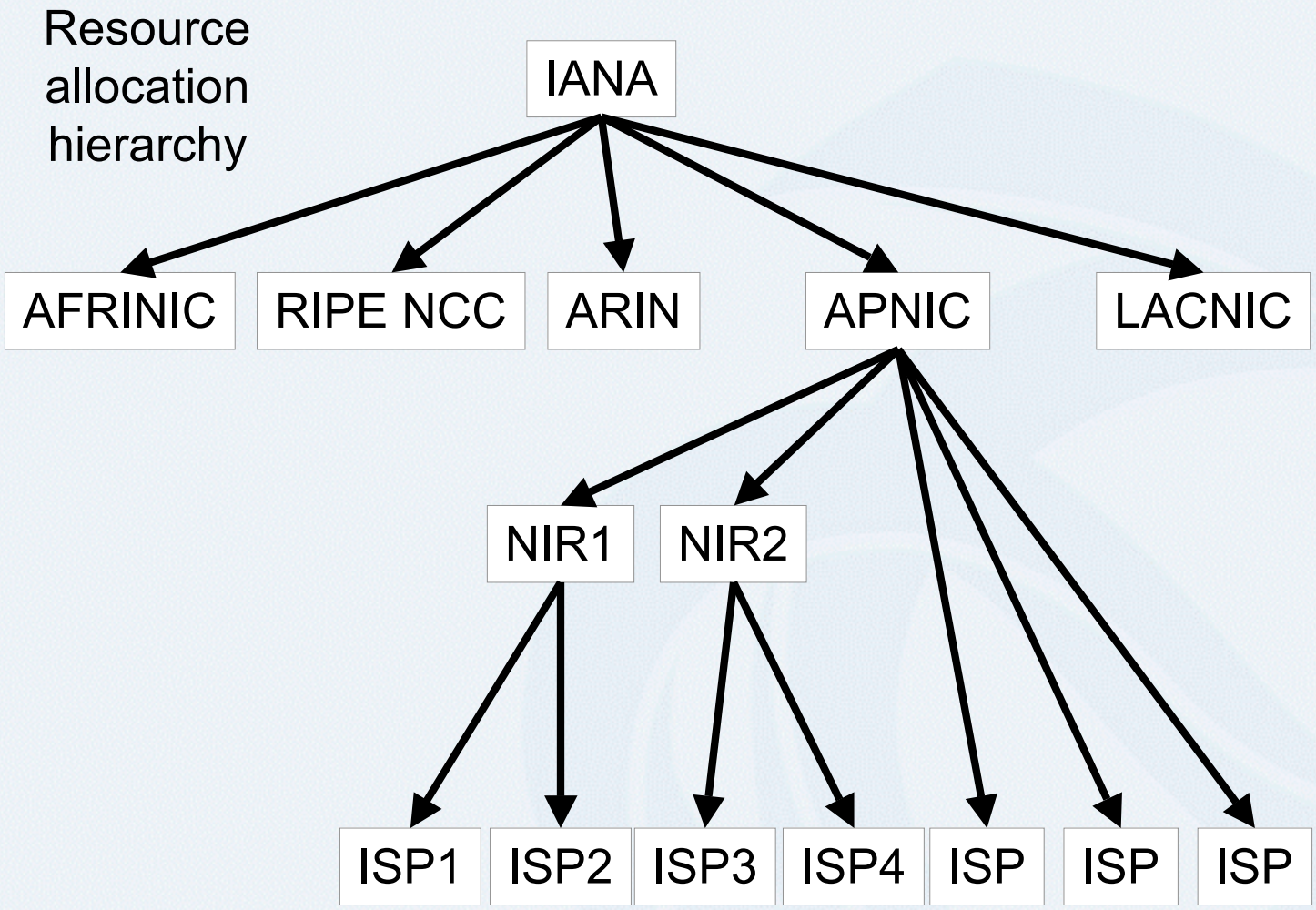
Resources for this work

- APNIC's allocation database
- Public / private key technology
- X.509 v3 certificate technology
- IP resource extensions to X.509 v3 certificates
- PKI models and trust relationships

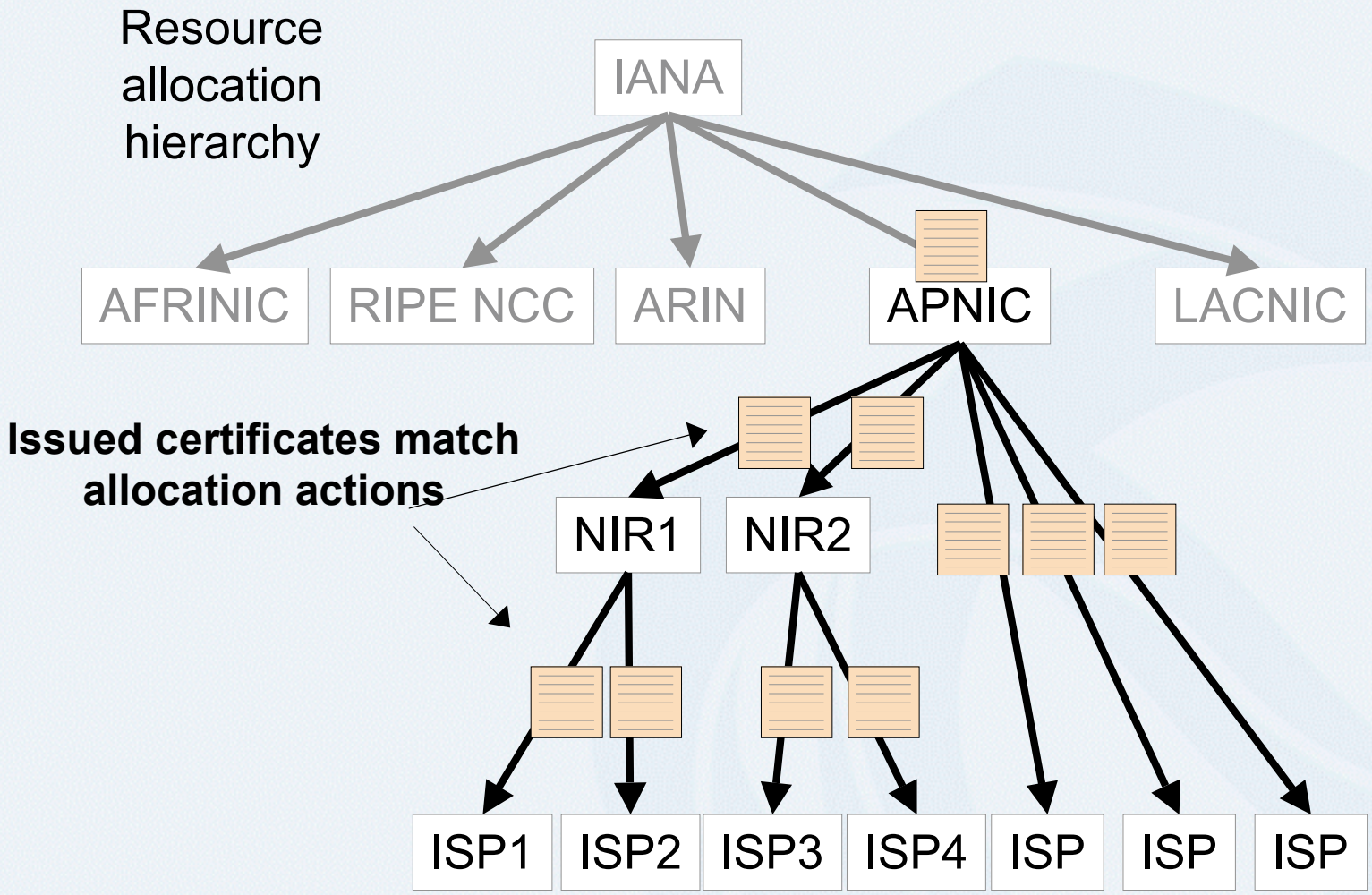
The overall objective

- To support a PKI that mirrors the existing resource allocation state
  - Every resource allocation can be attested by a matching certificate that binds the allocated resource with the resource issuer and recipient
- To use these resource certificates to make signed assertions that can be validated through this PKI

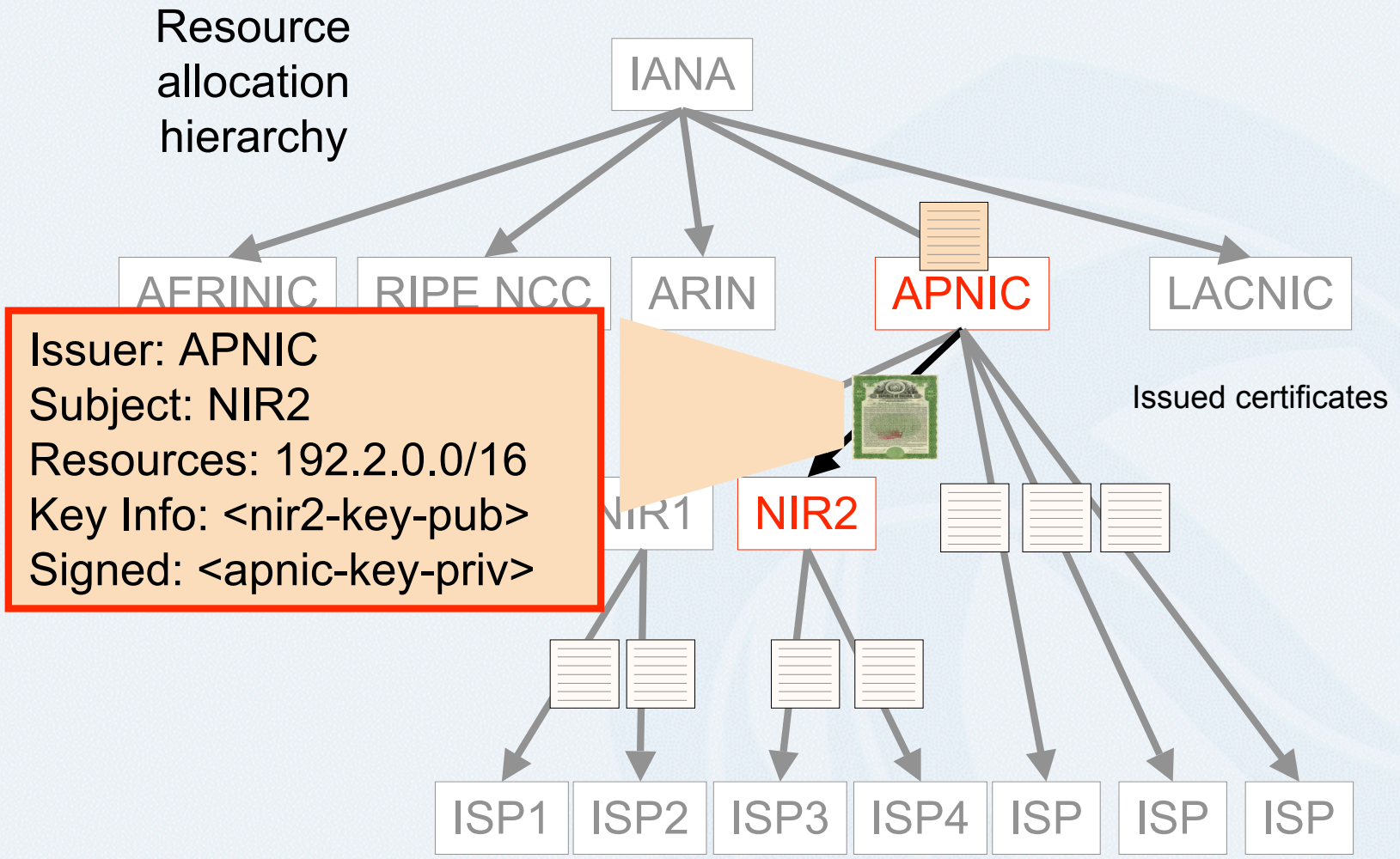
Resource certificates



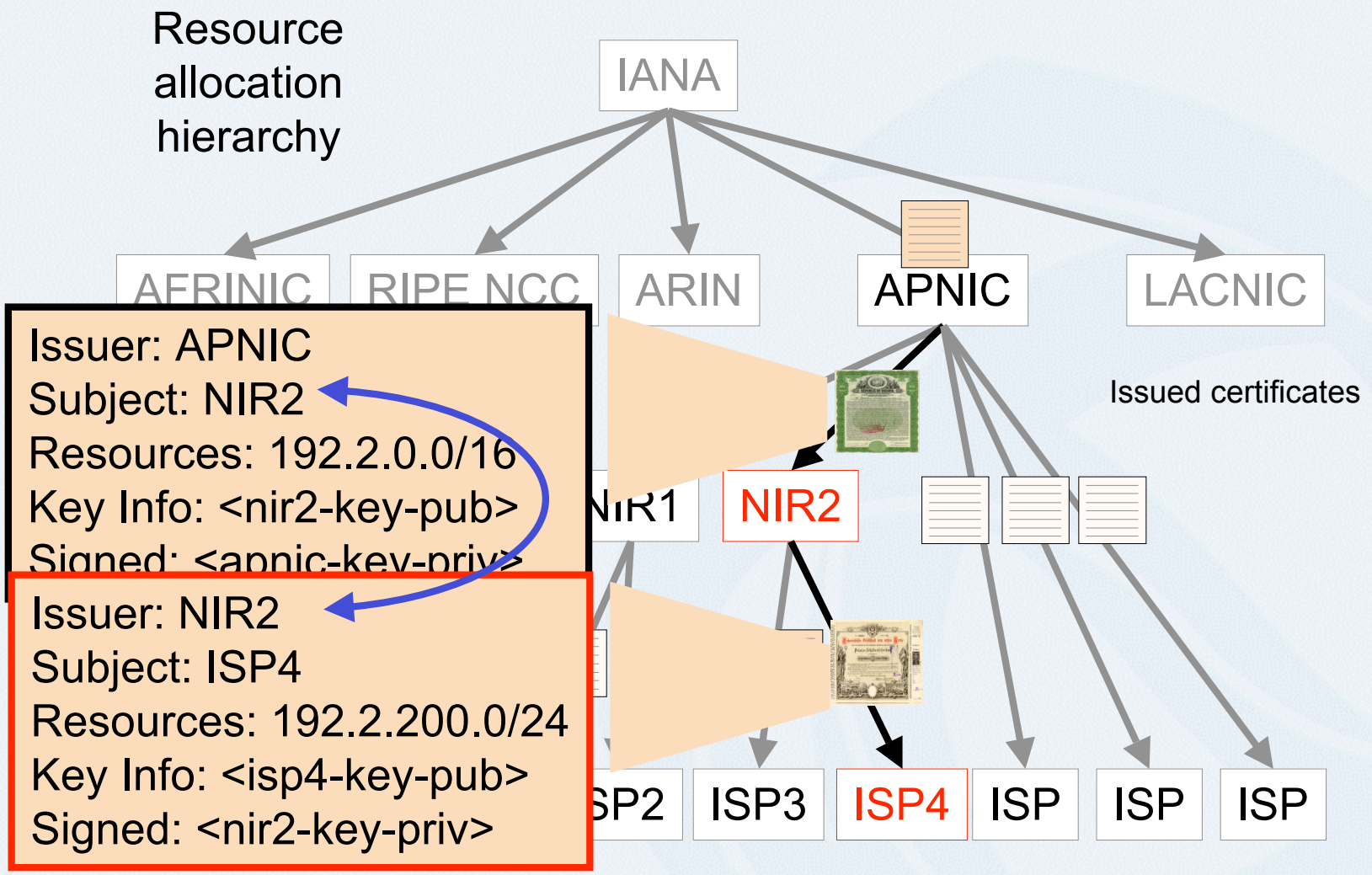
Resource certificates



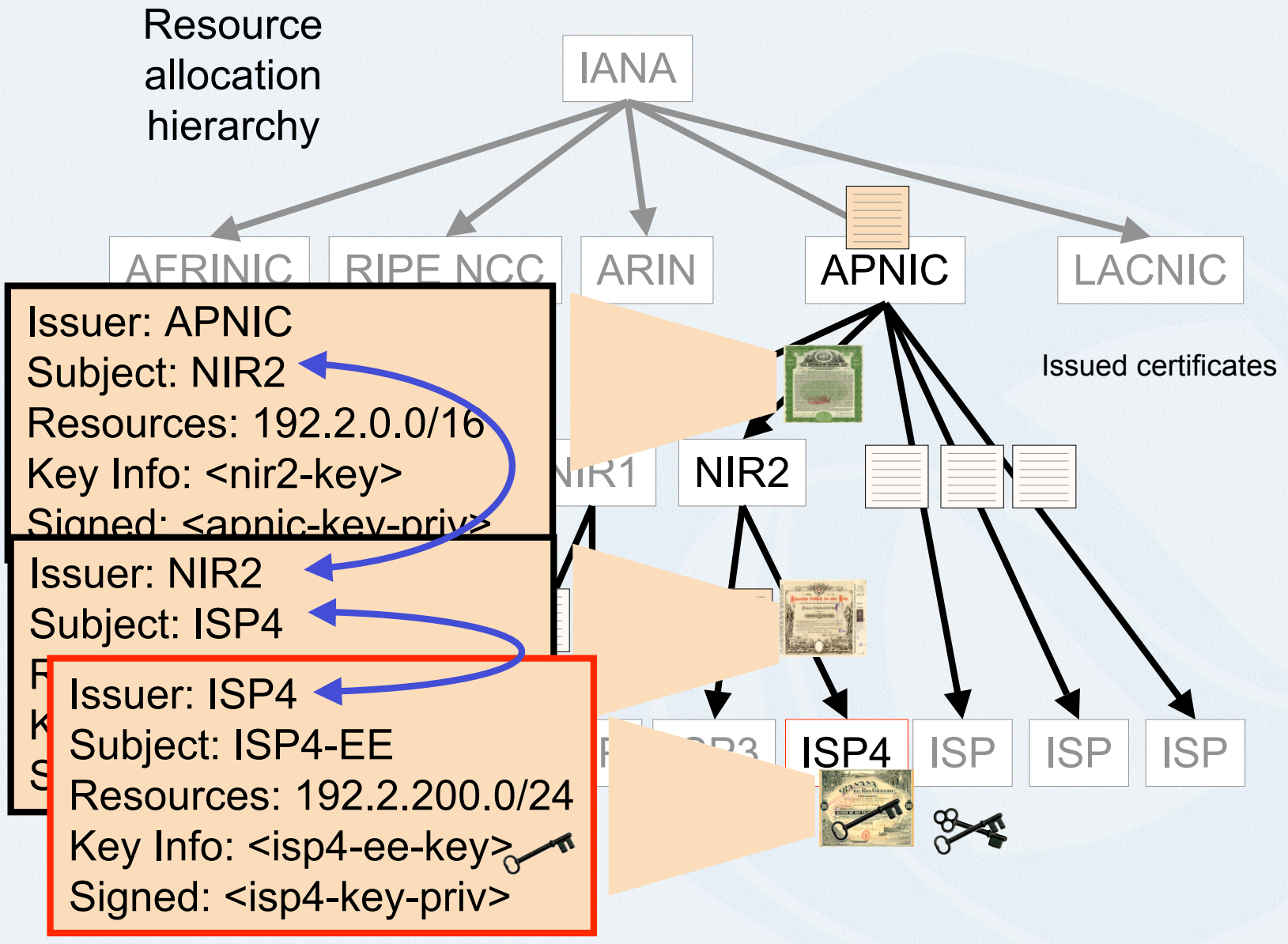
Resource certificates



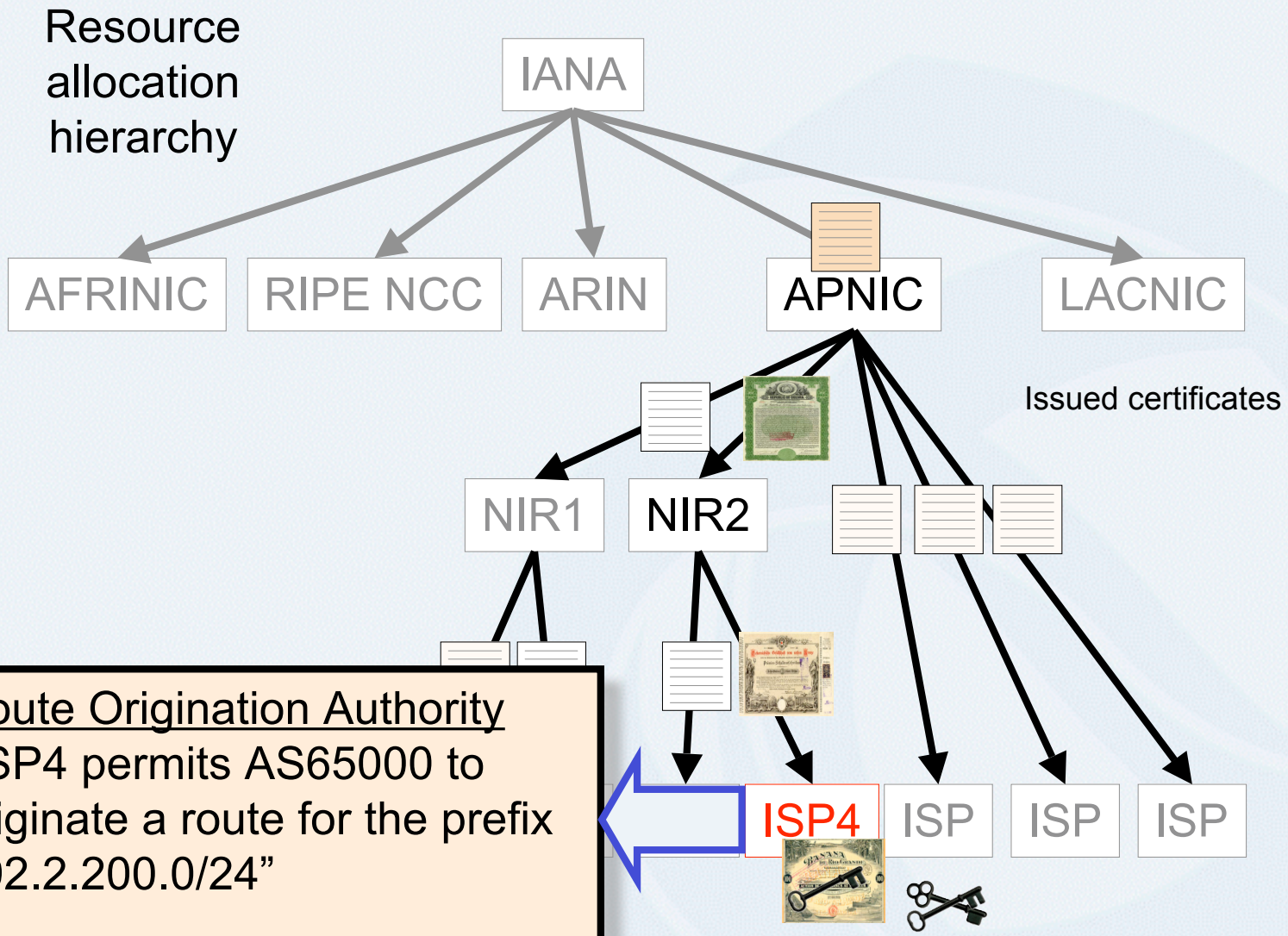
Resource certificates



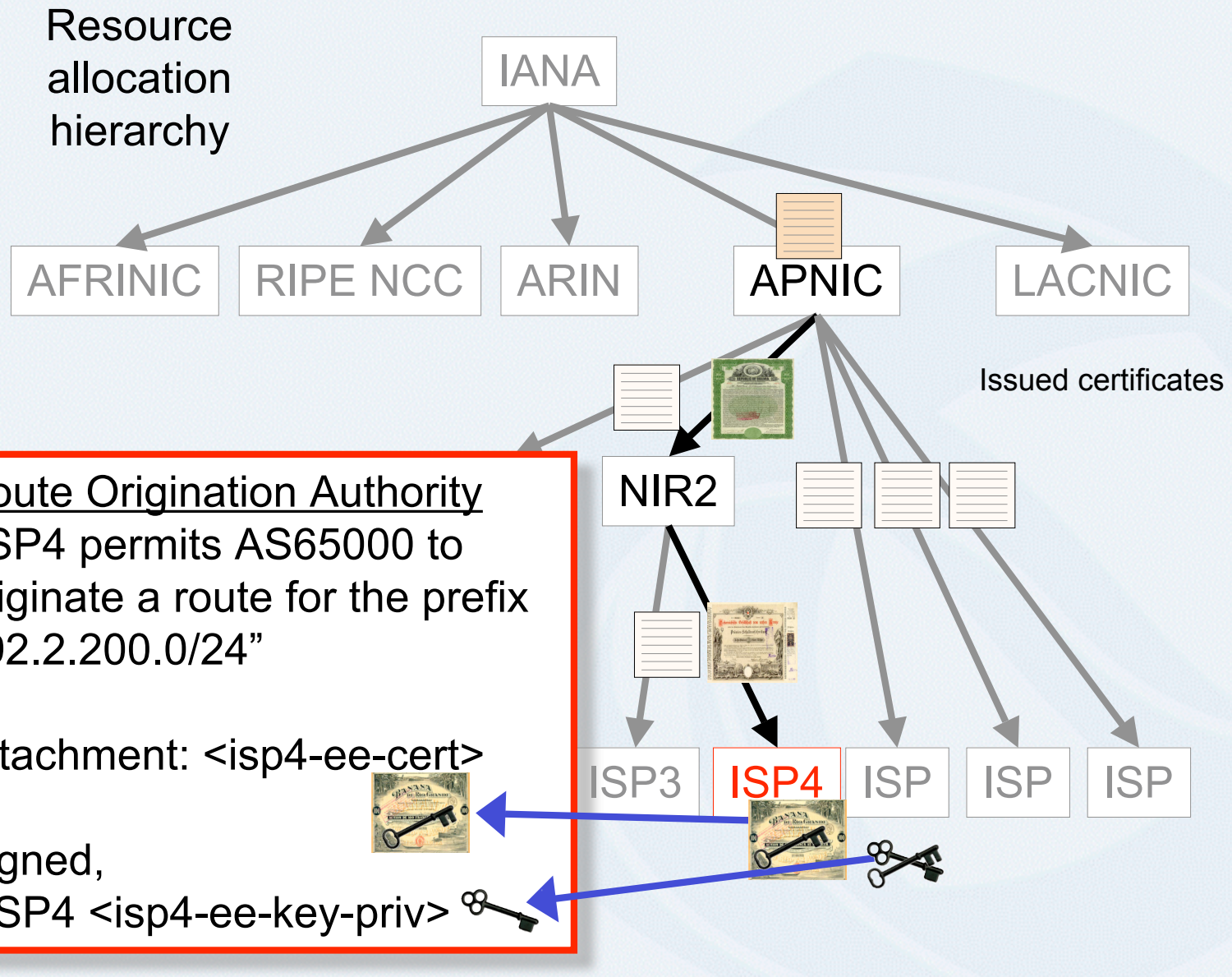
Resource certificates



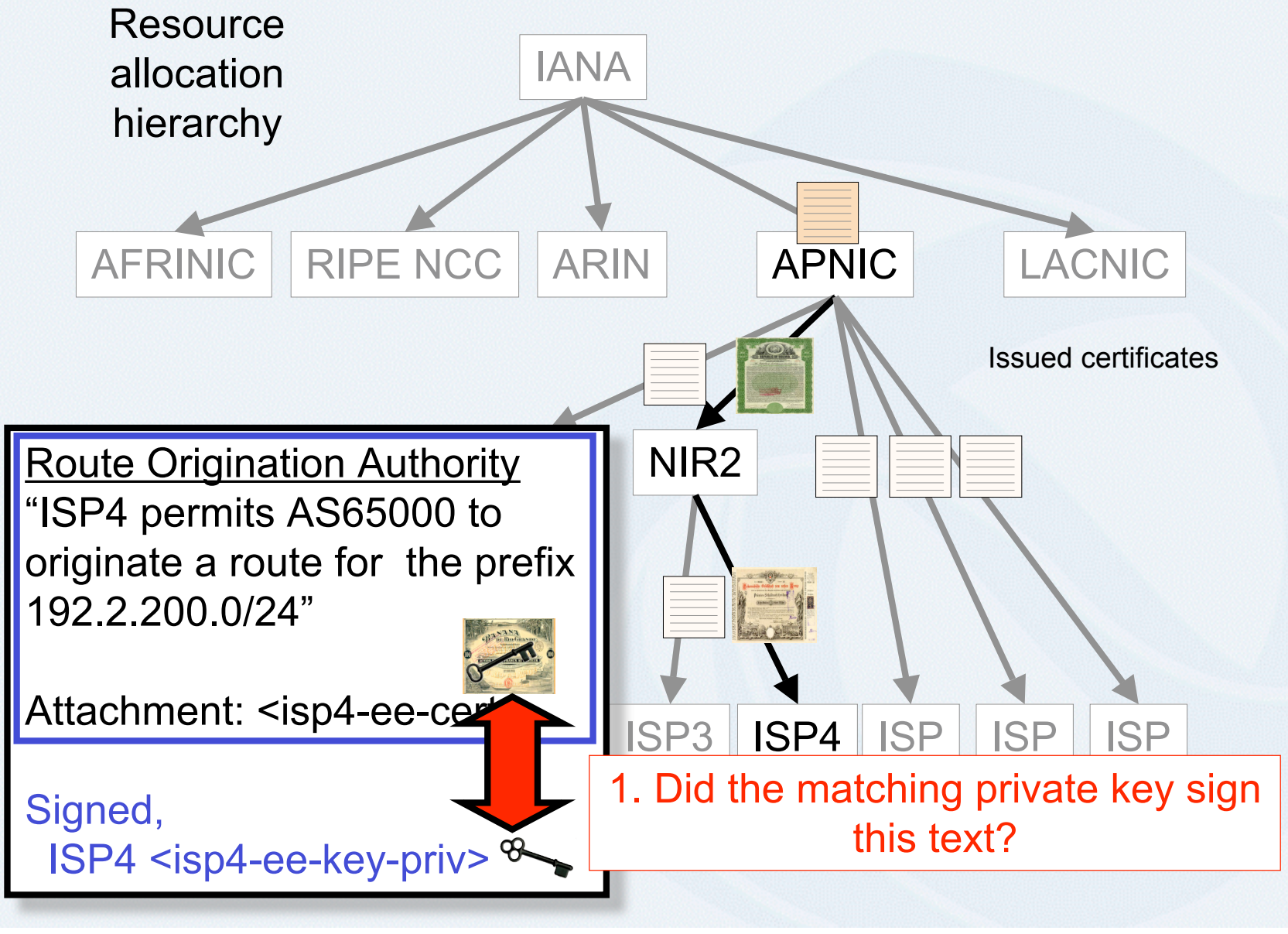
Use: Routing authority



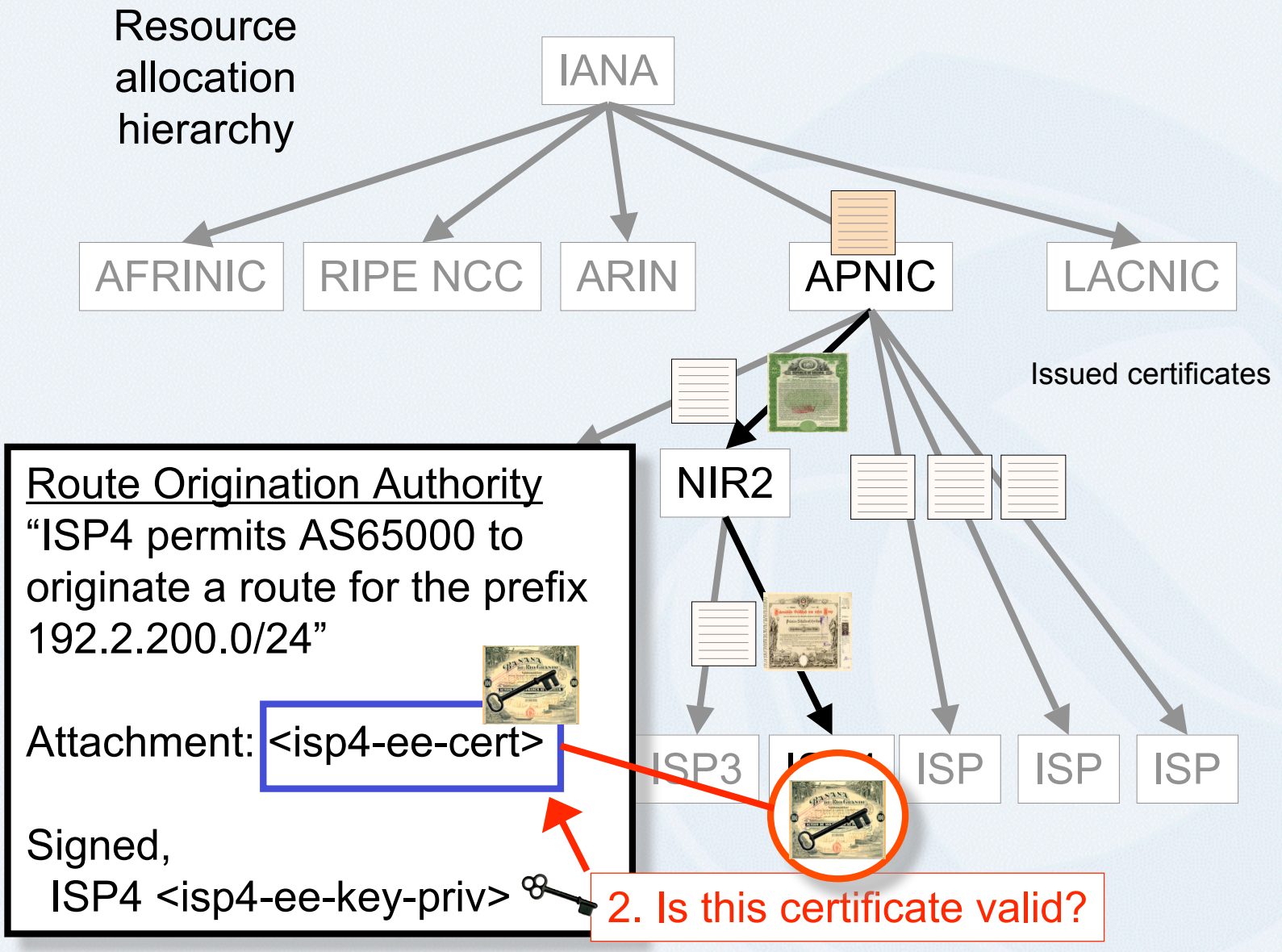
Signed objects



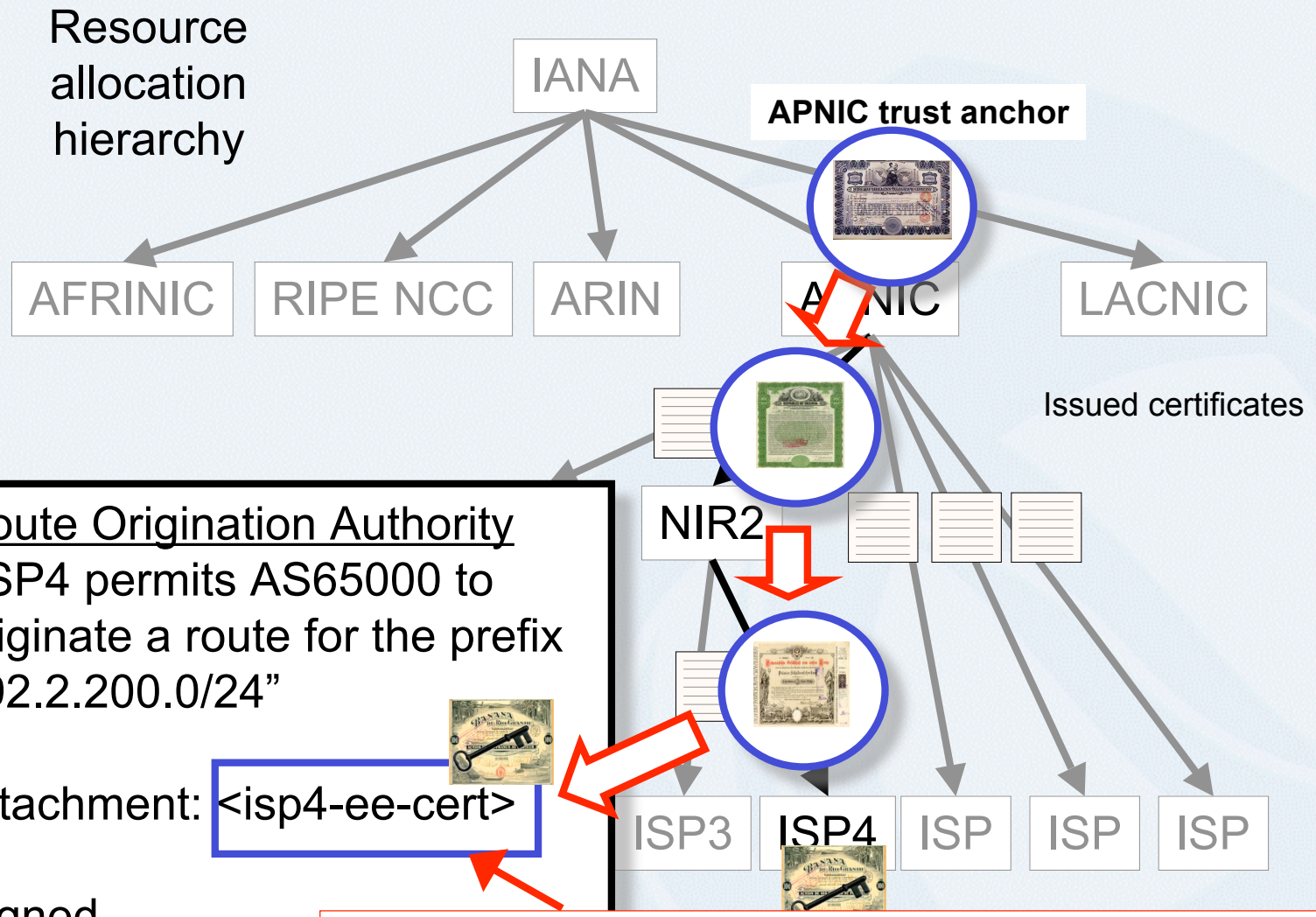
Signed object validation



Signed object validation

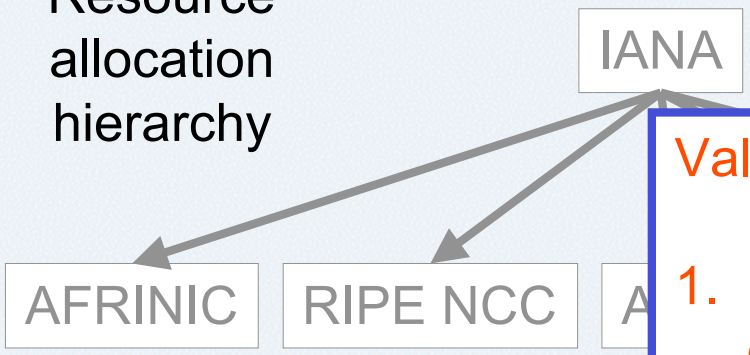


Signed object validation



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/avP4OU4CC3QMhU98tw2BqOTY
             HZvqXfAOVhjD4Apx4KjiAyr8tfeC7ZDhO+fpvsydV2XXtHIvjwjcL4GvM/gES6dJ
             KJYFWWlrPqQnfTFMm5oLWBUhNjuX2E89qyQf2YZVizITTNg3ly1nwqBoAqmmDhDy
             +nsRVAxax7II2iQDTr/pjI2VWfe4R36gbT8oxyvJ9xz7I9IKpB8RTvPVO2I2HbMI
             1SvRXMx5nQOXyYG3Pcxo/PAhbBkVkgfudLki/IzB3j+4M8KemrnVMRo=
             -----END PKCS7-----
changed:     test@telstra.net 20060822
source:      APNIC
```

Signer's resource 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
            Ck01Op5Q/Hc4yxwhTamNXW-cDWtQcmvOVGjU
Key Usage: DigitalSignature, nonRepudiation
CRL Distribution Points:
            rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5
            Ck01Op5Q.crl
Authority Info Access: caIssuers -
            rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5
            Ck01Op5Q.cer
Authority Key Identifier:
            Key Identifier g(AKI): cbh3Sk-iwj8Yd8uqaB5Ck01Op5Q
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 activity 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 certificate extensions to OpenSSL for Resource Certificates (open source development activity, supported by ARIN)

Current activities

- 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:

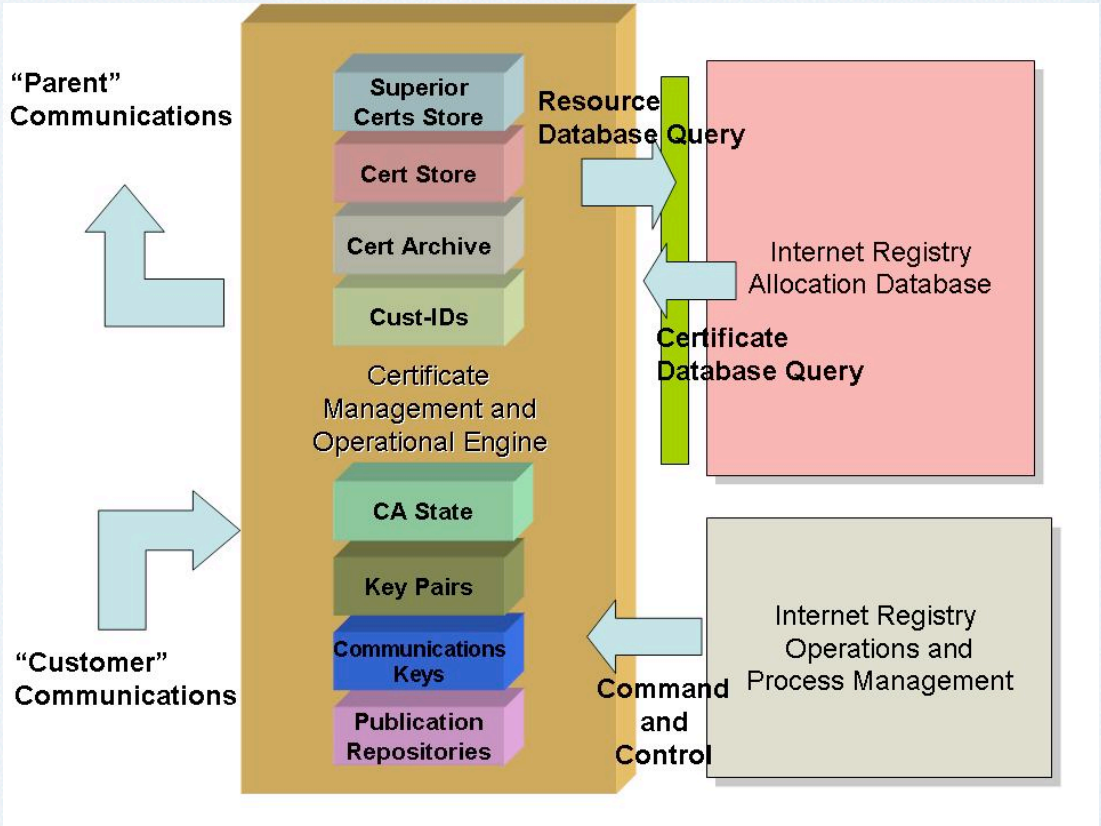
http://mirin.apnic.net/resourcecerts

Focus points for Q1 2007

- Can we design the certificate management subsystem to be an largely automated “slave” of the resource allocation function?
- Provide a toolset to allow IRs to manage certificate issuance
- Use the same toolset to provide ‘hosted’ certificate services

Focus points for Q1 2007

- Defining the components and interactions of a “certificate engine”



Focus points for Q1 2007

- Automated certificate issuance
  - Query / response interaction between registry and registry clients:
    - **List**: What resources have been allocated to me and what's the corresponding state of issued certificates?
    - **Issue**: Here is a certificate request – please issue me with a certificate that matches my allocated resource set
    - **Remove**: Please revoke certificates issued with this public key

Next steps

- Development of the Certificate Engine
- End entity Certificates
- Tools for relying parties
- Evaluation of progress

Thank you

http://mirin.apnic.net/resourcecerts

Questions?