Resource Certification

Overview

- What are we talking about?
  - Certification of Numbering Resources – Introduction
- Why are we talking about it now?
- (Second) Thoughts
- The way forward

What is this about?

Excerpt from Geoff Huston's talk
"Using Resource Certificates"
at RIPE 53, Amsterdam

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

What would be good …

- 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 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:

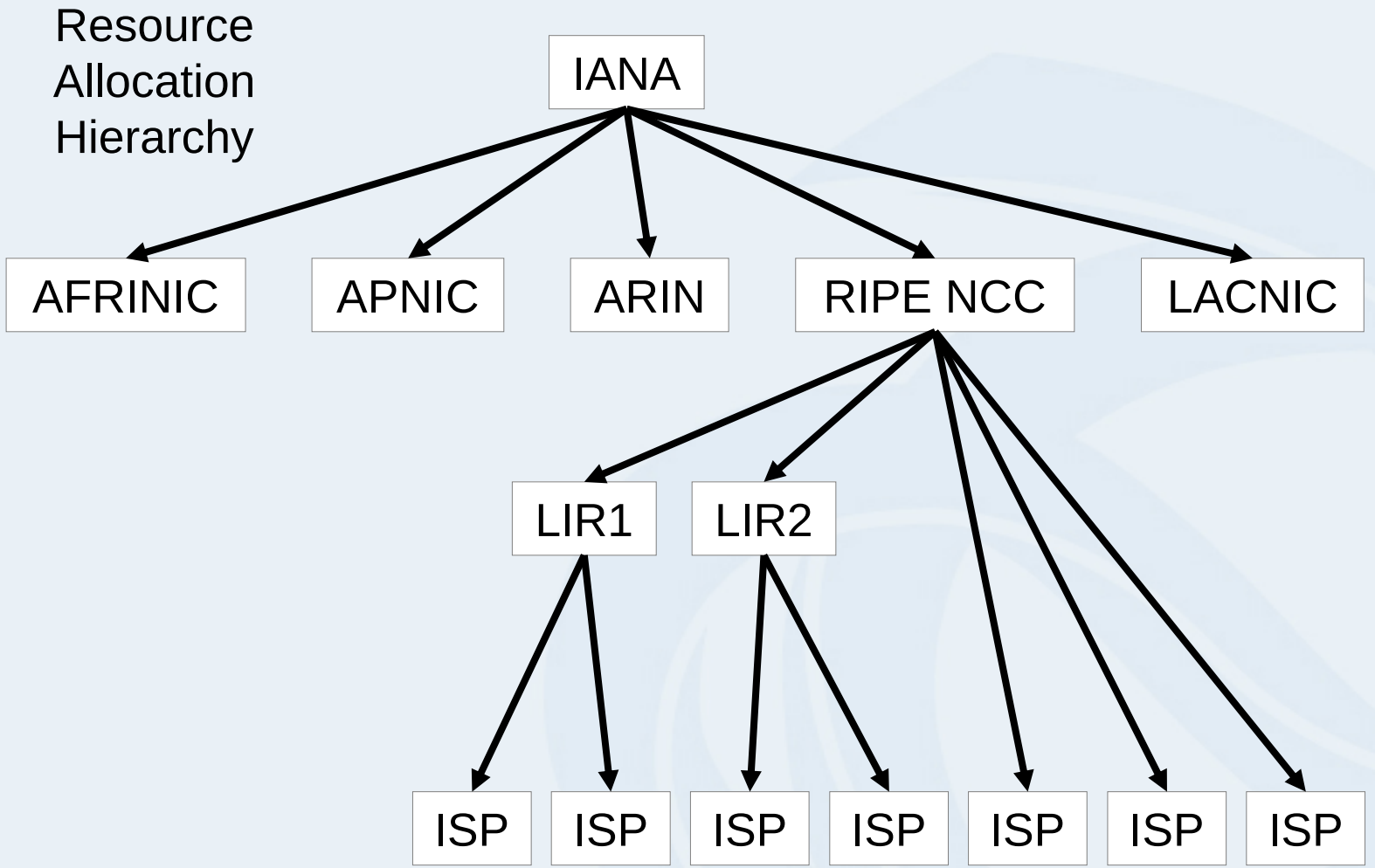
the certificate's Subject

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

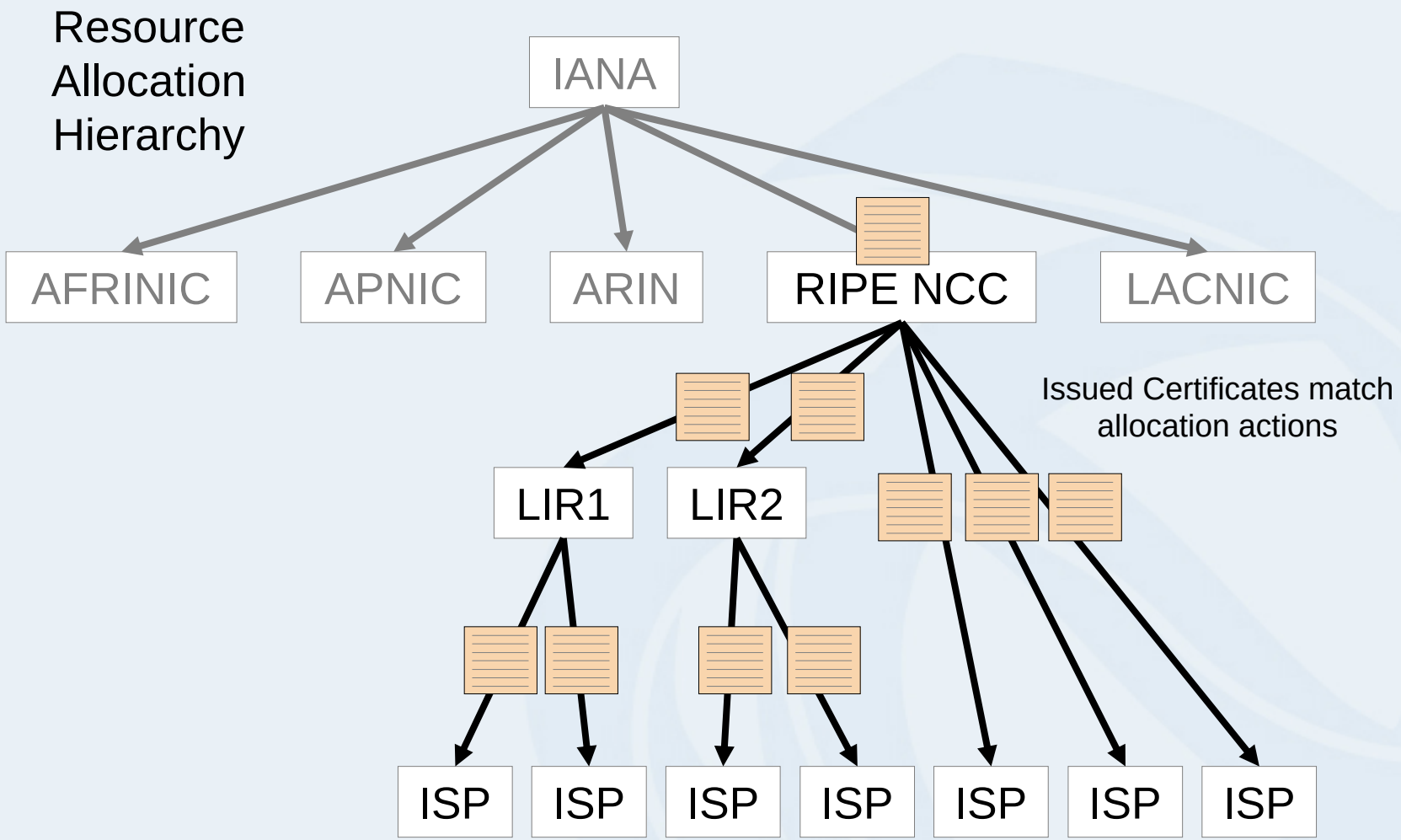
is the current controller of a collection of IP address and AS resources

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

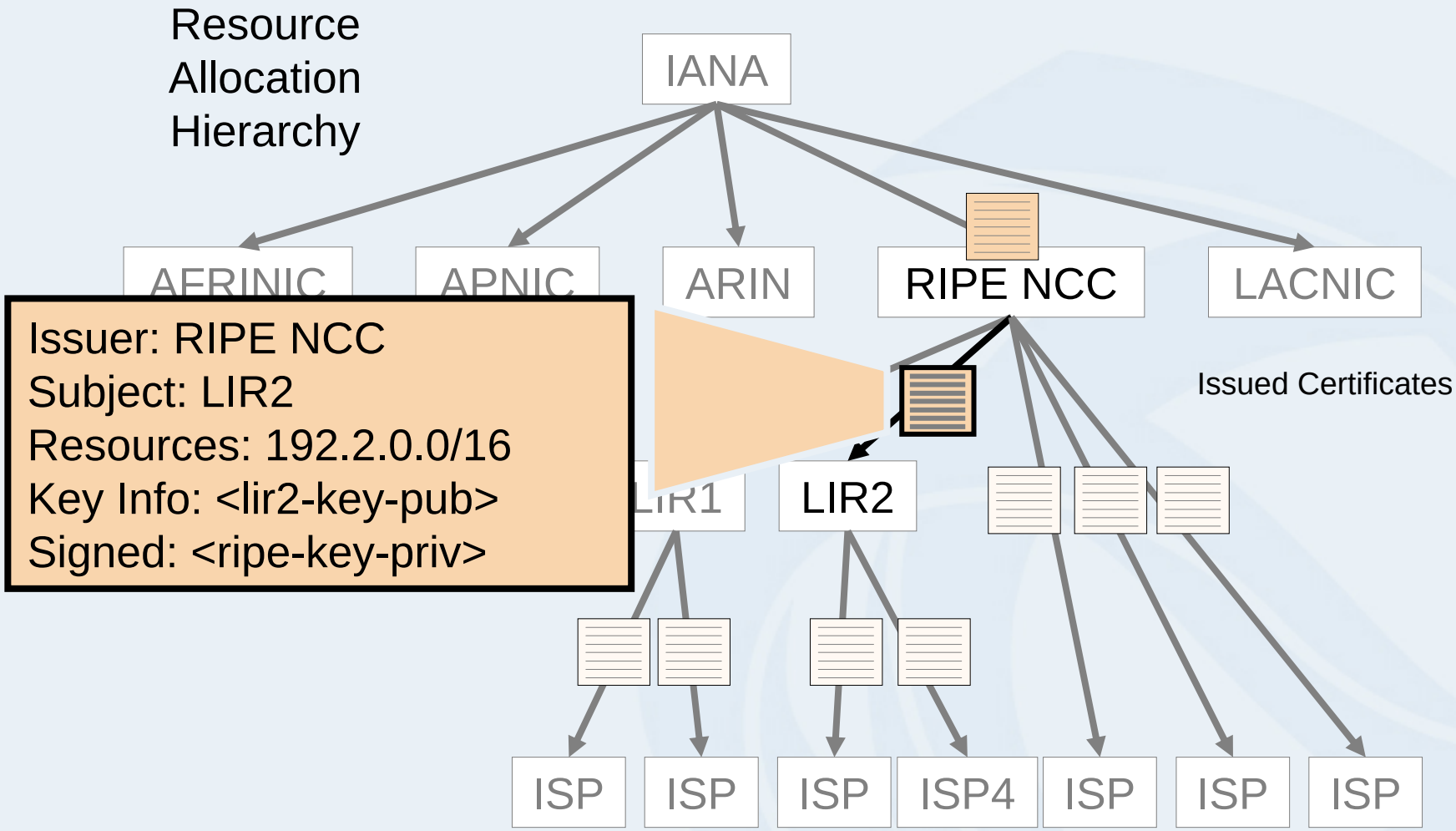
Resource Certificates



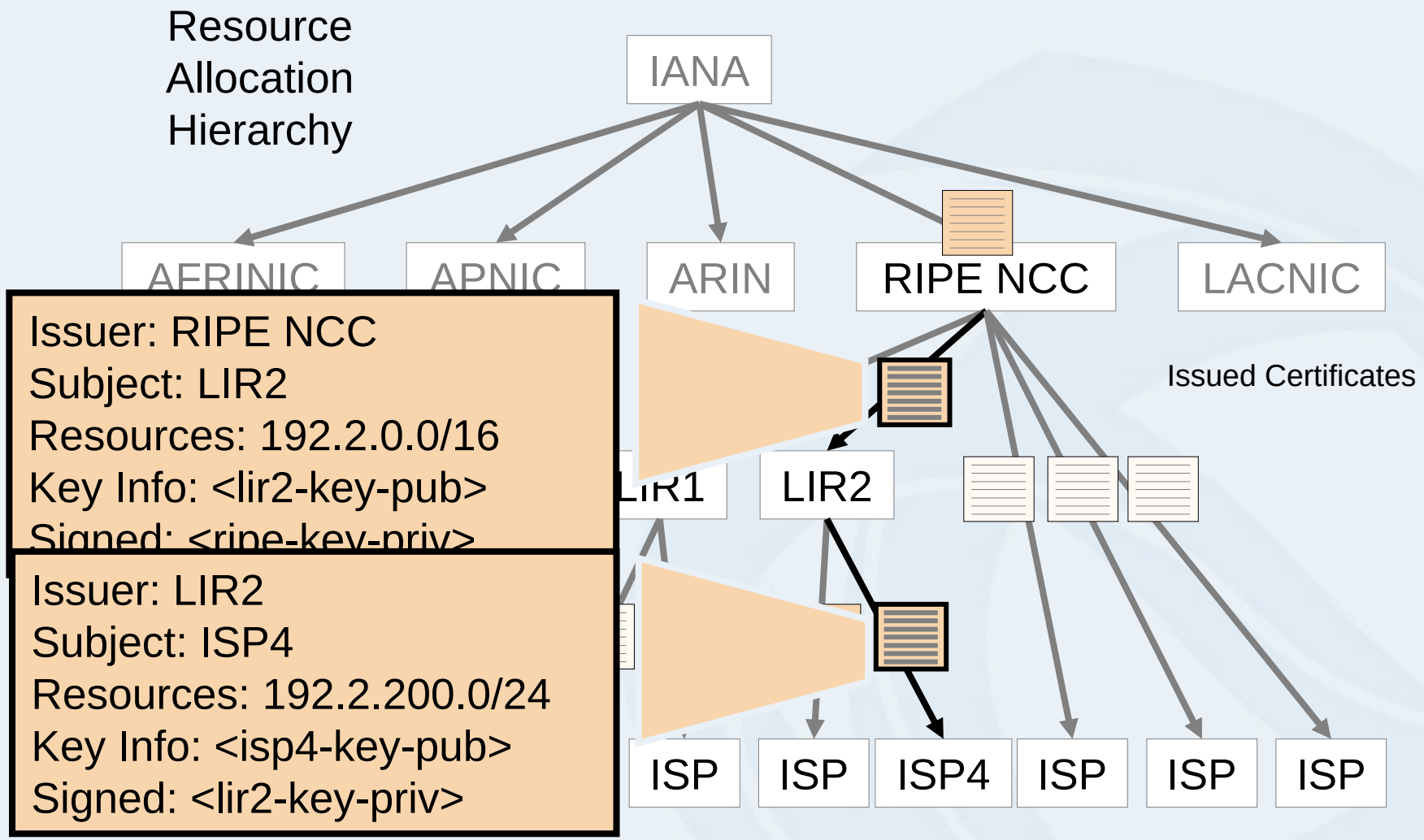
Resource Certificates



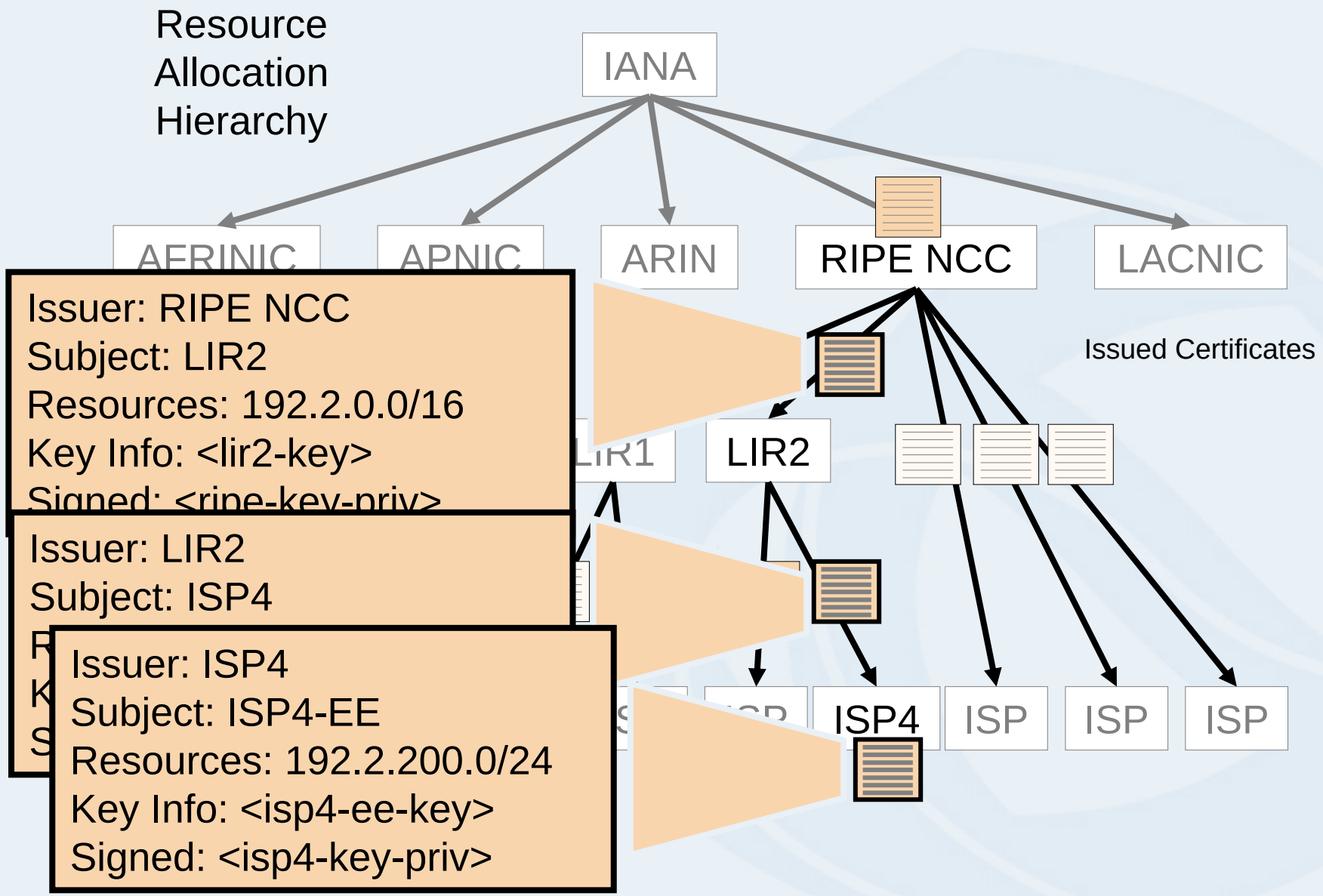
Resource Certificates



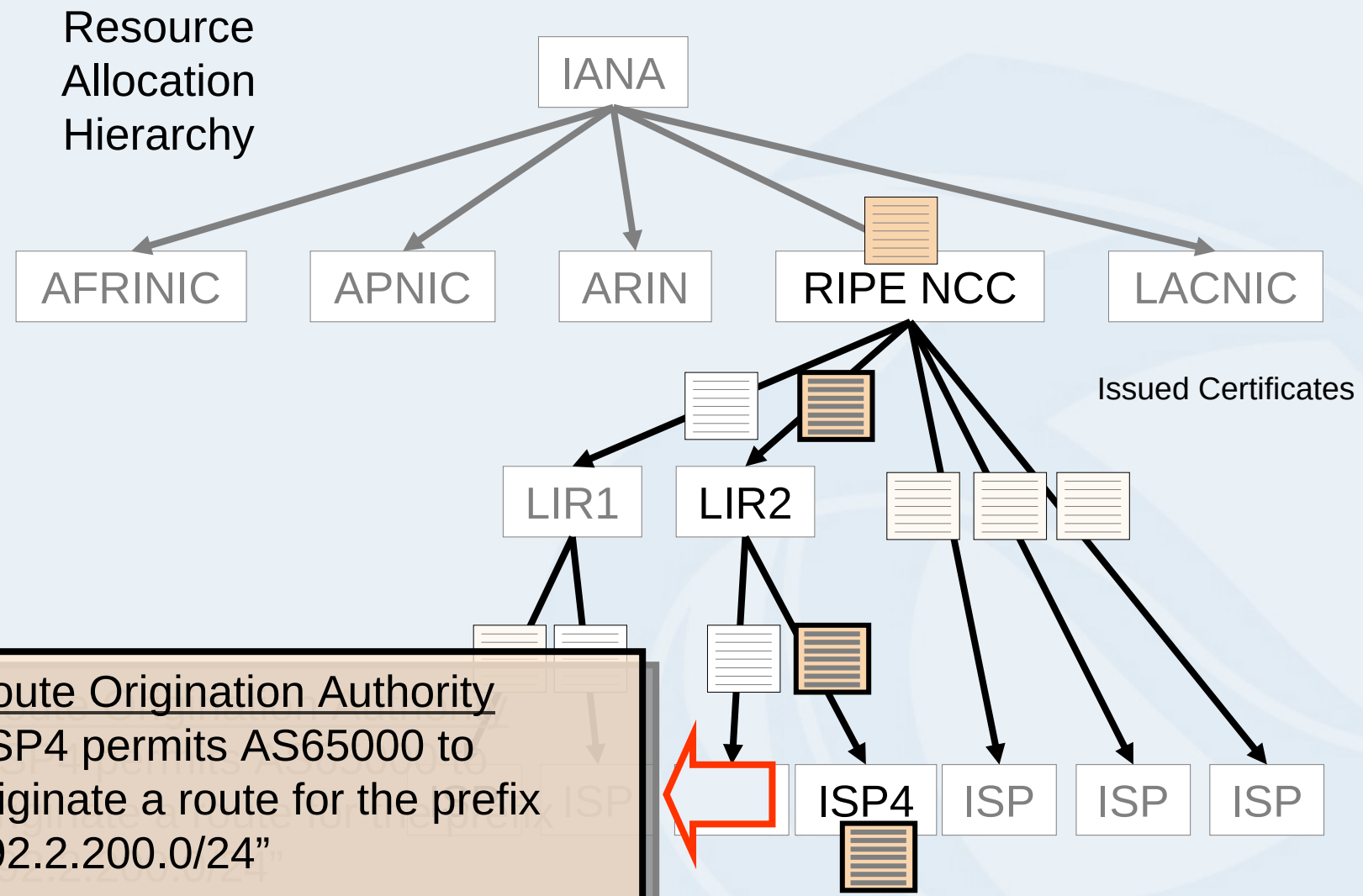
Resource Certificates



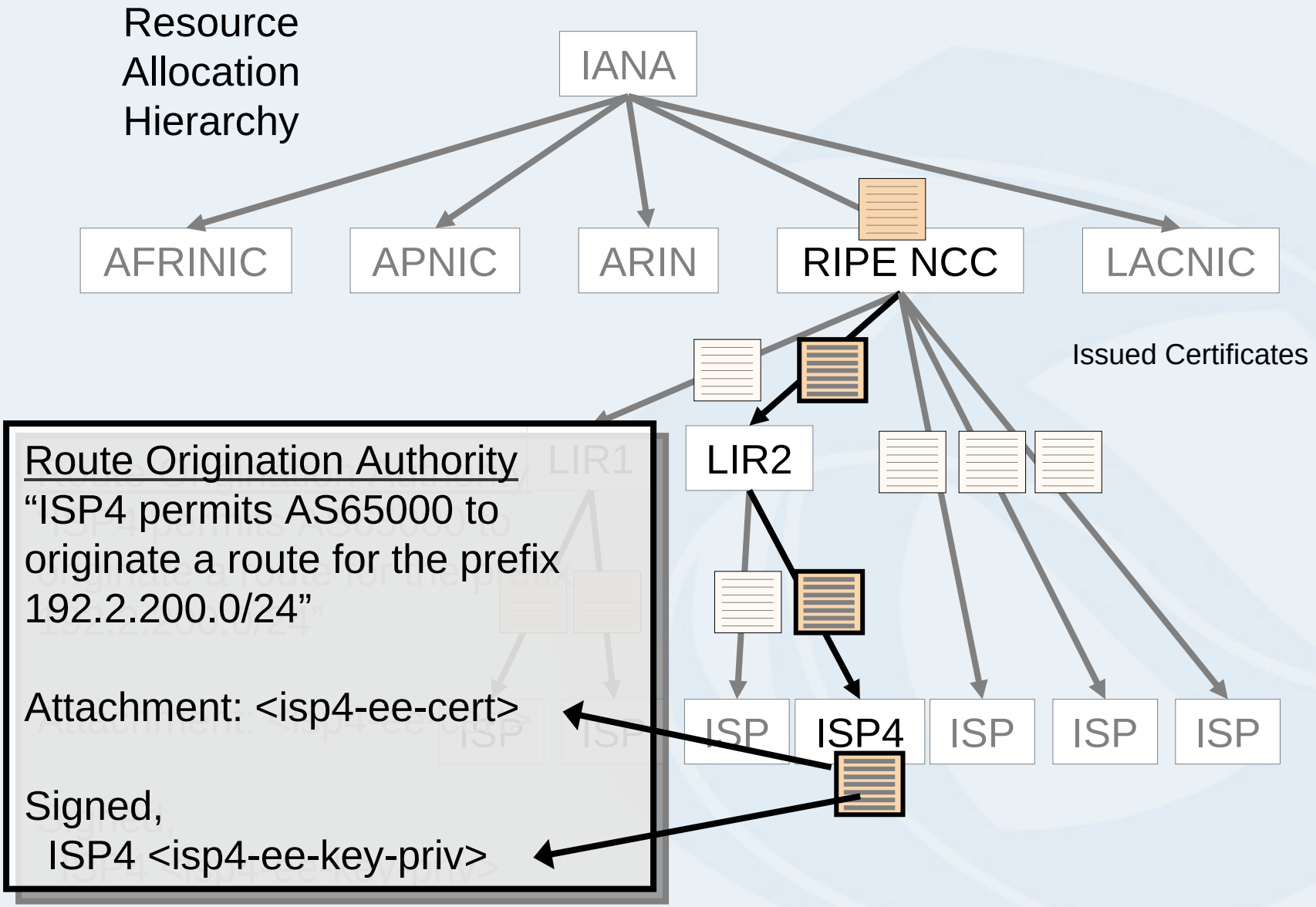
Resource Certificates



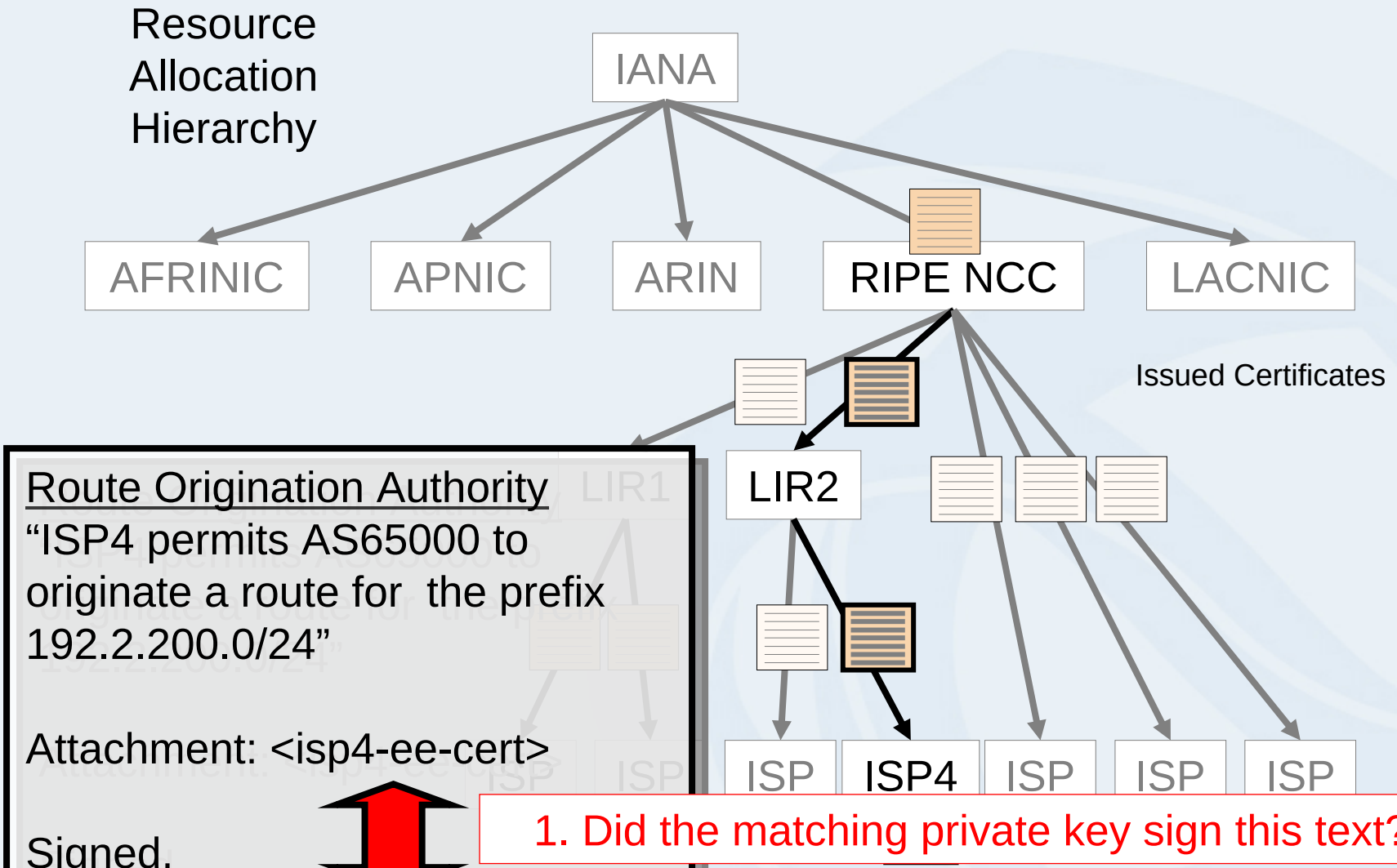
Base Object in a Routing Authority Context



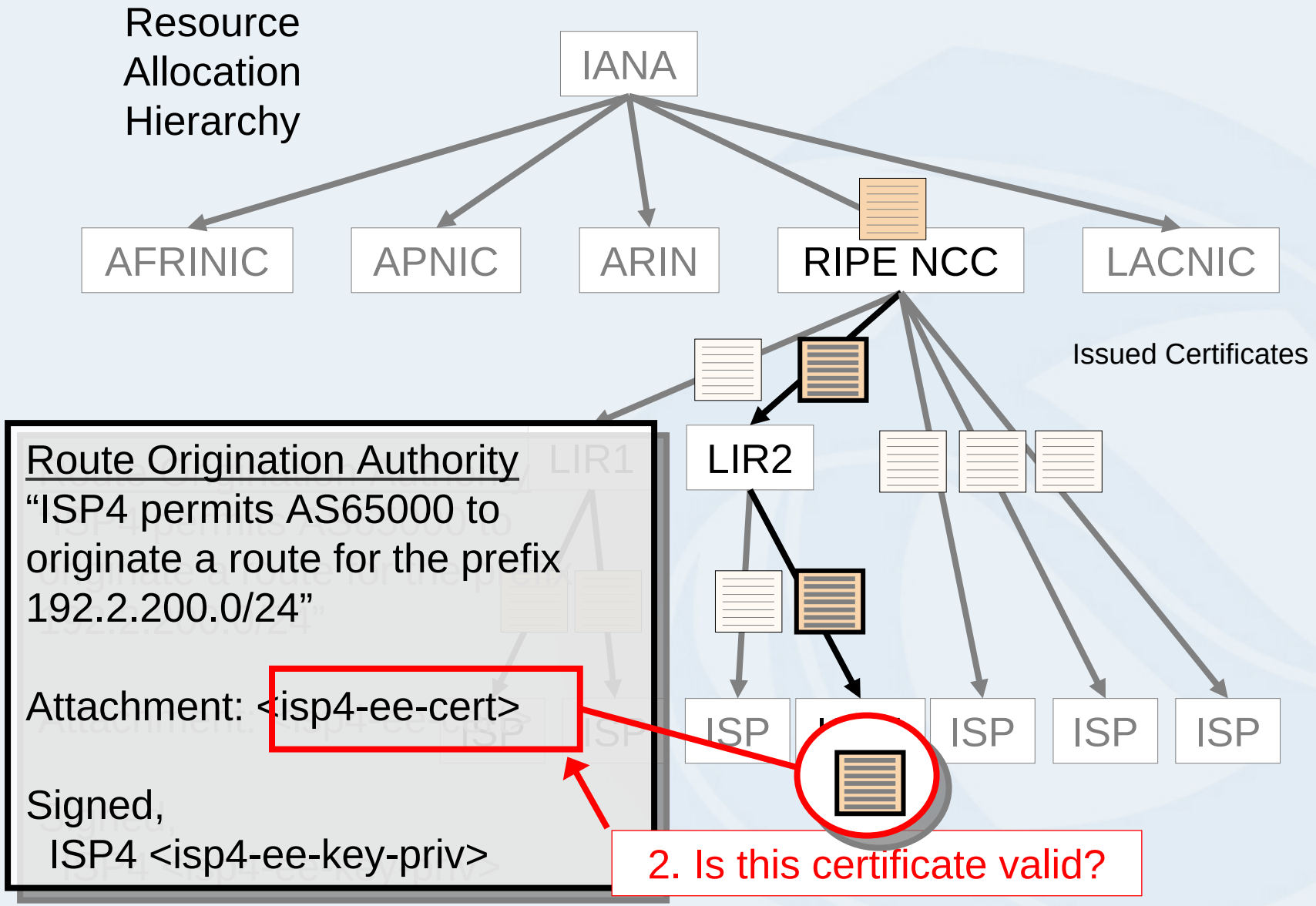
Signed Objects



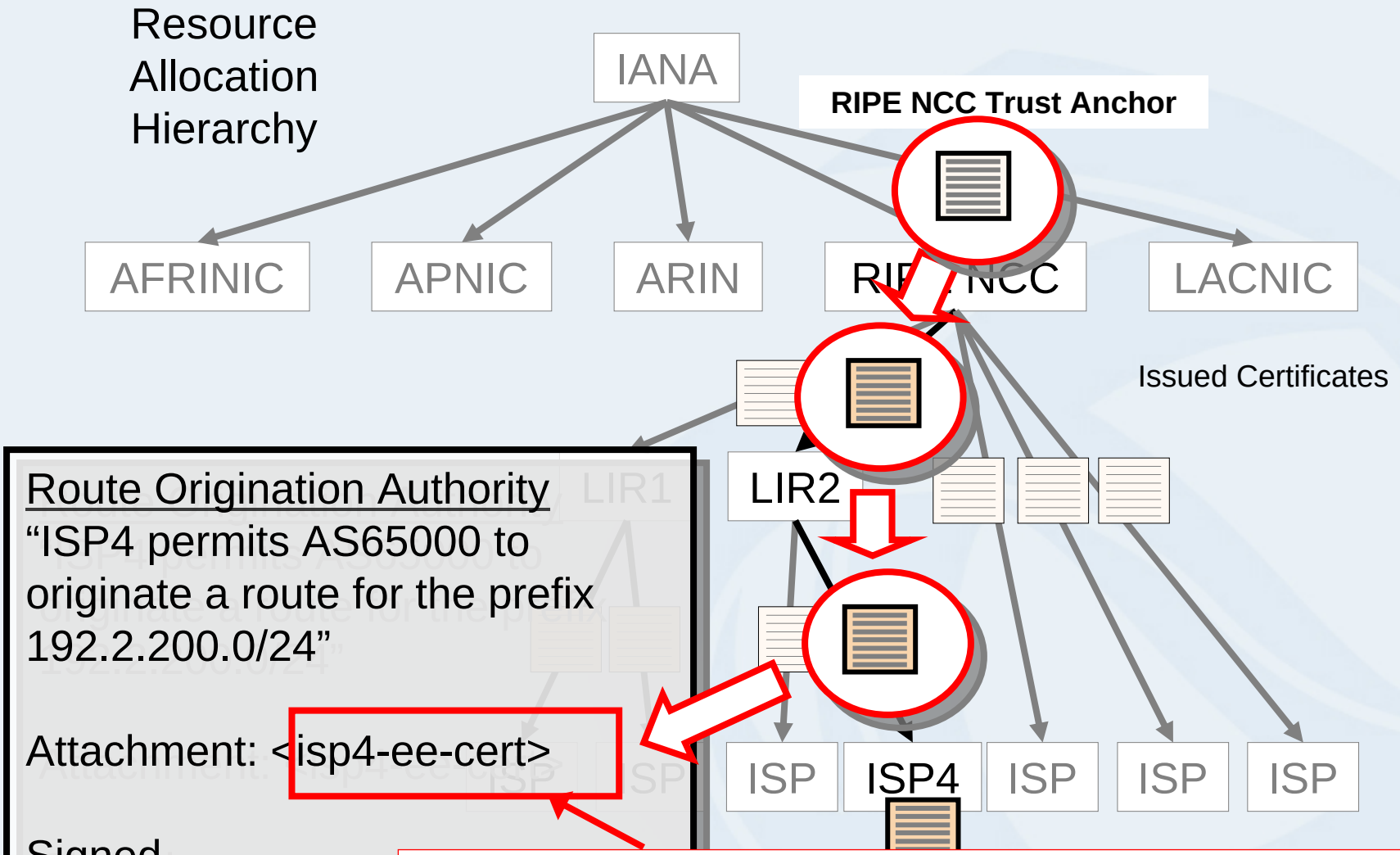
Signed Object Validation



Signed Object Validation

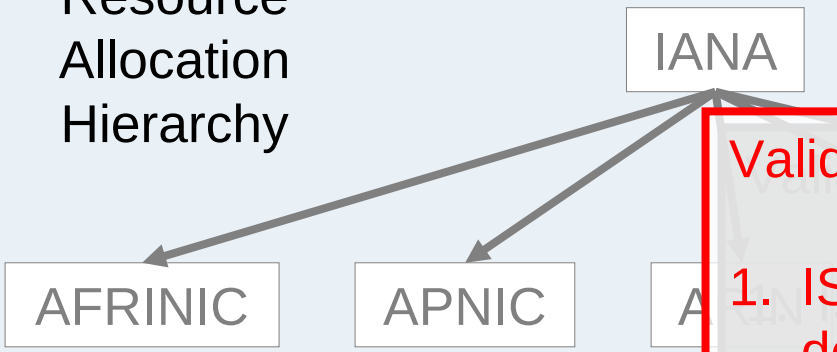


Signed Object Validation



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>

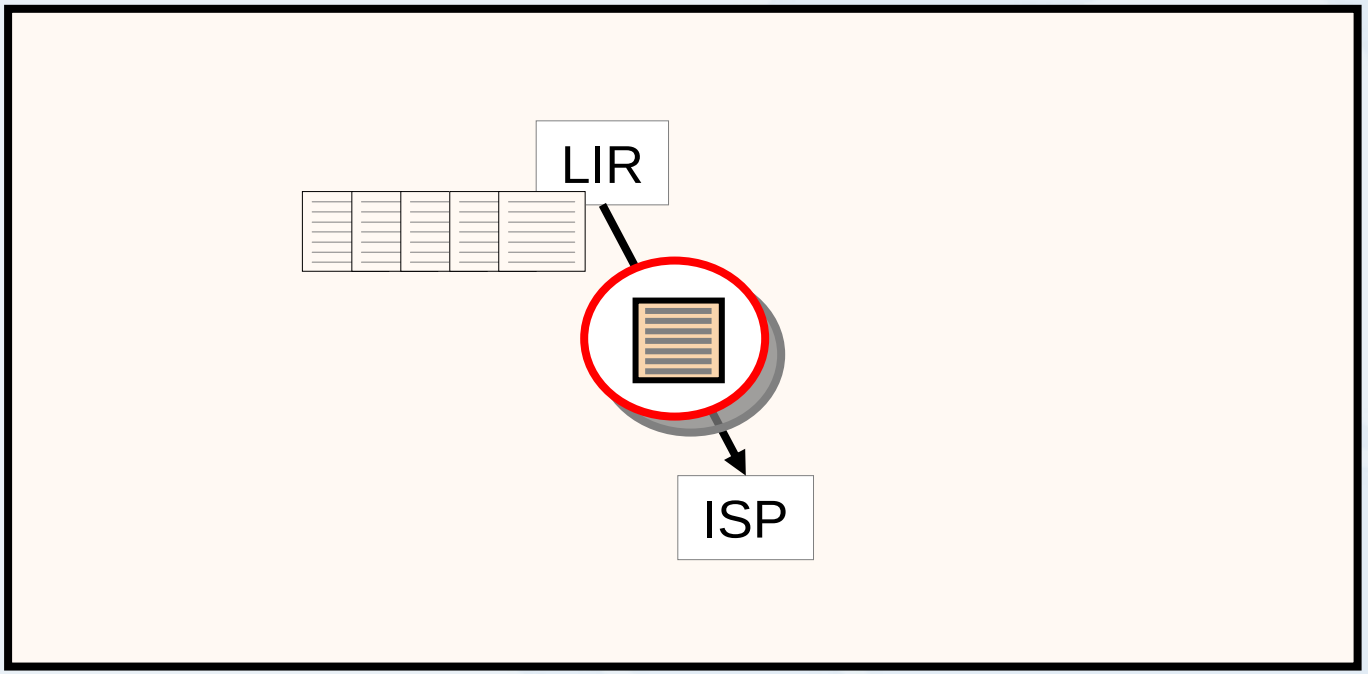
Validation Outcomes

1. ISP4 authorized this Authority document
2. 192.2.200.0/24 is a valid address
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

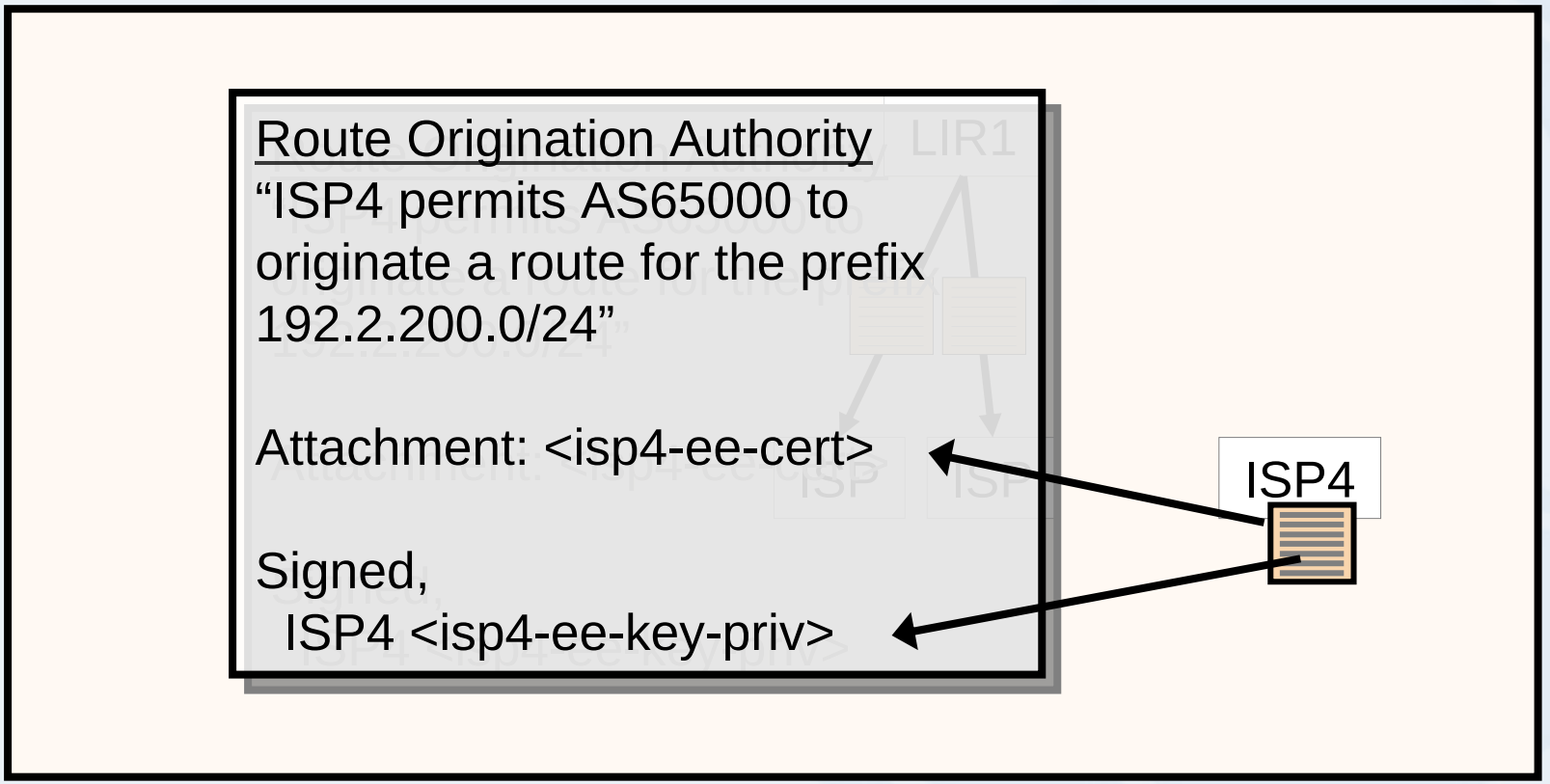
Maintain a certificate collection that matches the current resource allocation state



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

Thank you, Geoff…

- Why are we talking about this now?

RIPE NCC Services -- History

"No e-voting. No informal poll of what services are needed. RIPE NCC just keeps rolling along."

- We want to be transparent
- Explicit decisions needed
- We want to be sure of doing what members need…

- http://www.ripe.net/info/ncc/roles-responsibilities.html

Certification of Numbering Resources

- APNIC heading effort, presentation RIPE 51
- During 2006, ongoing effort to implement prototype tools
  - RIPE NCC contribution ~ 1 FTE

Next Step

- Ensure Context Match across RIRs
- …
- But wait!
- What are we doing?
- Are we having second thoughts?
- …

Next Step:
Let's take a Step Back!

- Why are we doing this?
- Assumptions
  - Resource Certification is preparing the way for Secure Routing
  - Resource Certification is good for RIPE DB "Data Quality"
- Are these valid?
- (Un)Intentional Consequences?

Paving the way for Routing Security

- Really?
- … or DNSsec Redux?
  - Resources spent
  - Activity successfully concluded
  - Deployment AWOL
- Will YOU deploy secure routing?
  - What will convince you?
  - What will hold you back?
- Are we running too fast?

Certification Good for Data Quality

- Why?
  - Will we be checking every allocation?
  - Will we be asserting holder identity?
  - Or will we rather certify what is already in our files?
- Certification is itself is not a Fine Tooth Comb
- “Combing Results” can be documented by a variety of means
- Certificates are just one possibility
- Cost/Benefit ratio attractive enough for this purpose?

Unintended Consequences

- If numbers were certified…
- Are we about to enable a marketplace?
  - "Numbers do not have monetary value!"
  - … or do they?
- Would that be Good? Or Bad?
  - Approaching the end of lifetime of IPv4
  - Would the role of RIRs change?
  - How?

The Way Forward

Strawman Proposal @ RIPE 53

- Continue prototype development
- Trial deployment in RIPE region in 2007
- Planning for two additional FTE for integration in business processes and systems
- Install Evaluation Task Force
  - Scope:
    - Follow developments
    - Participate in Trial
    - Advise on impact
    - Formulate report as input for RIPE 55

Task Force Report

- 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

Decision Time

- Decide @ RIPE 55 about operational use
  - Agree administrative details
  - Discuss policy changes
  - Changes & amendments to Service Contracts

Questions?