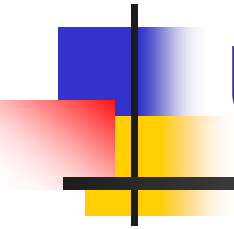


Update on Resource Certification

Geoff Huston, APNIC

Mark Kosters, ARIN

IEPG, March 2008

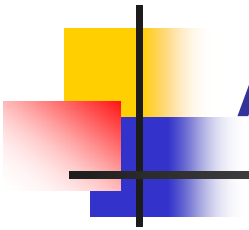
Address and Routing Security

What we have had for many years is a relatively insecure inter-domain routing system based on mutual trust that is vulnerable to various forms of disruption and subversion

And it appears that the operational practice of bogon filters and piecemeal use of routing policy databases are not entirely robust forms of defense against these vulnerabilities

So it appears to look at something that is a little more robust and offers a little more in terms of detection of subversion of the routing system

From the RIR perspective we've been looking at this topic for over a decade



Address and Routing Security

The basic routing payload security questions that need to be answered are:

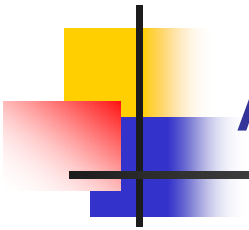
- Is this a **valid address prefix**?
- **Who** injected this address prefix into the network?
- Did they have the necessary **credentials** to inject this address prefix?
- Is the forwarding path to reach this address prefix an **acceptable representation** of the network's forwarding state?

Can these questions be answered reliably, cheaply and quickly?

Laying the Foundation in a PKI

Use a dedicated public key infrastructure to allow any relying party to be able to validate attestations about addresses and their use:

- the **authenticity of the address object** being advertised
- **authenticity of the origin AS**
- the **explicit authority** from the address to AS that permits an originating routing announcement



A Starting Point for Routing Security

Adoption of some basic security functions into the Internet's routing domain:

- Injection of reliable trustable data
  - A Resource PKI as the base of validation of network data
- Explicit verifiable mechanisms for integrity of data distribution
  - Adoption of some form of certified authorization mechanism to support validation of credentials associated with address and routing information

X.509 Extensions for IP Addresses

- RFC3779 defines extension to the X.509 certificate format for IP addresses & AS number
- The extension binds a list of IP address blocks and AS numbers to the subject of a certificate
- These extensions may be used to convey the issuer's authorization of the subject for exclusive use of the IP addresses and autonomous system identifiers contained in the certificate extension
- The extension is defined as a critical extension
  - Validation includes the requirement that the Issuer's certificate extension **must** encompass the resource block described in the extension of the certificated being validated

What is being Certified

For example:

APNIC (the “Issuer”) certifies that:

the certificate “Subject”

whose public key is contained in the certificate

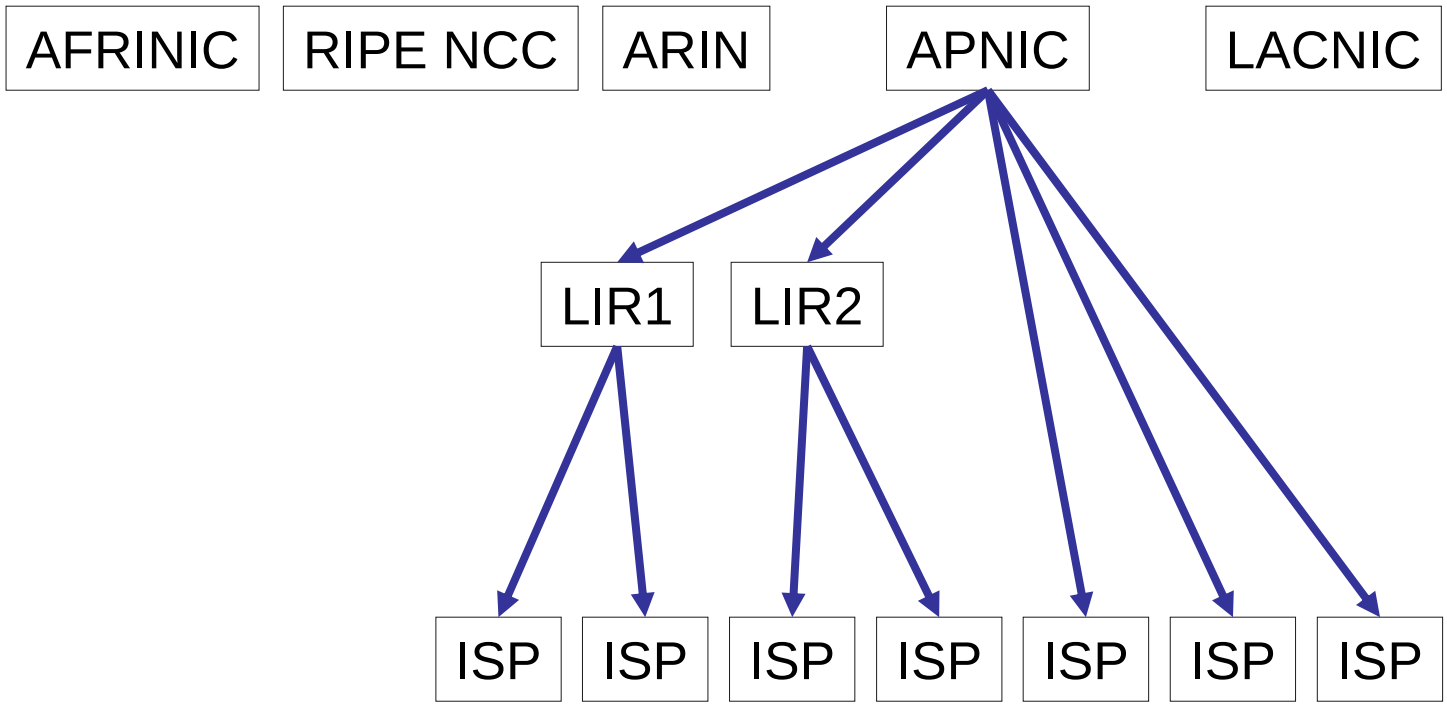
is the current controller of a set of IP address and AS resources

that are listed in the certificate extension

APNIC does NOT certify the identity of the subject, nor their good (or evil) intentions!

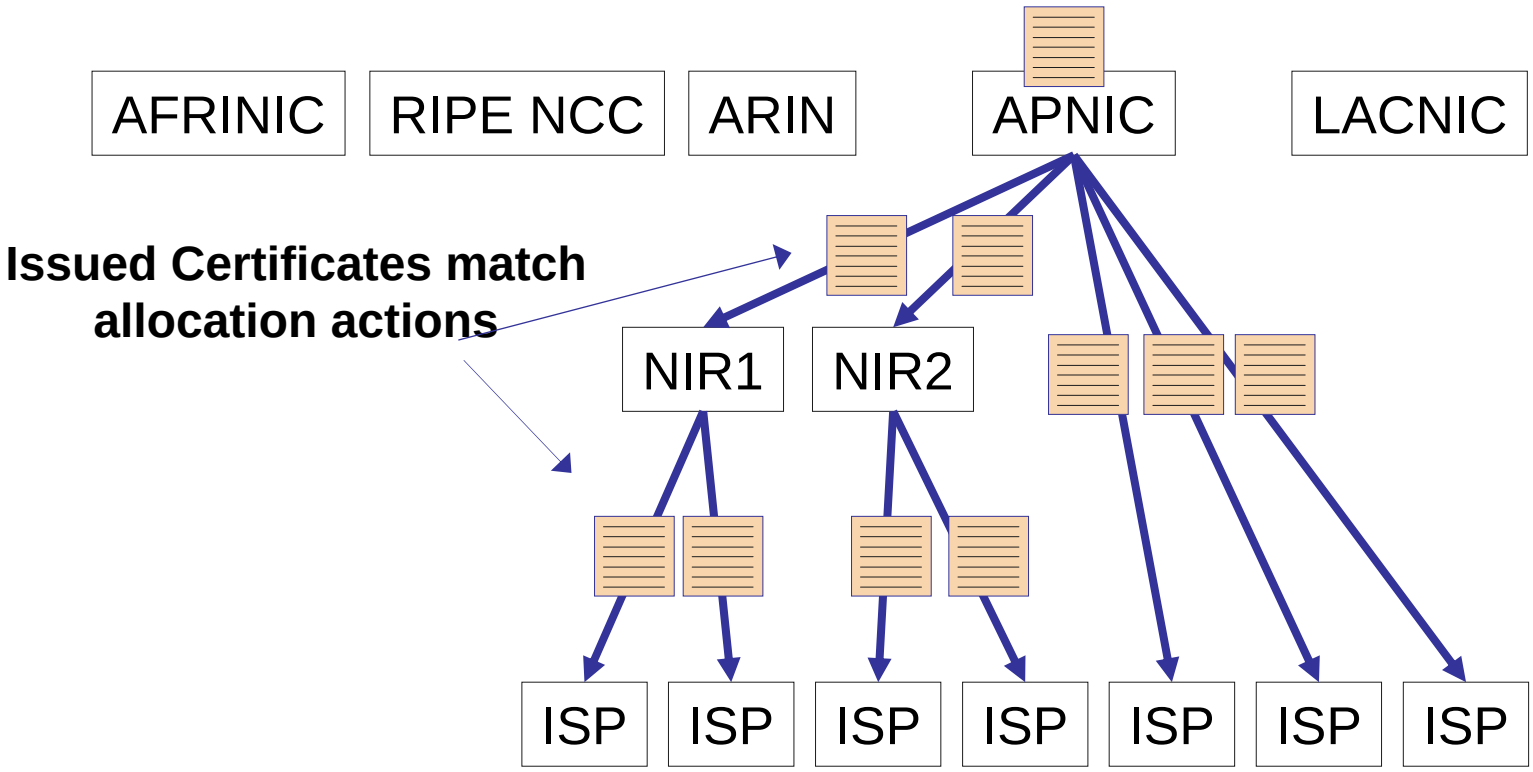
Resource Certificates

Resource
Allocation
Hierarchy



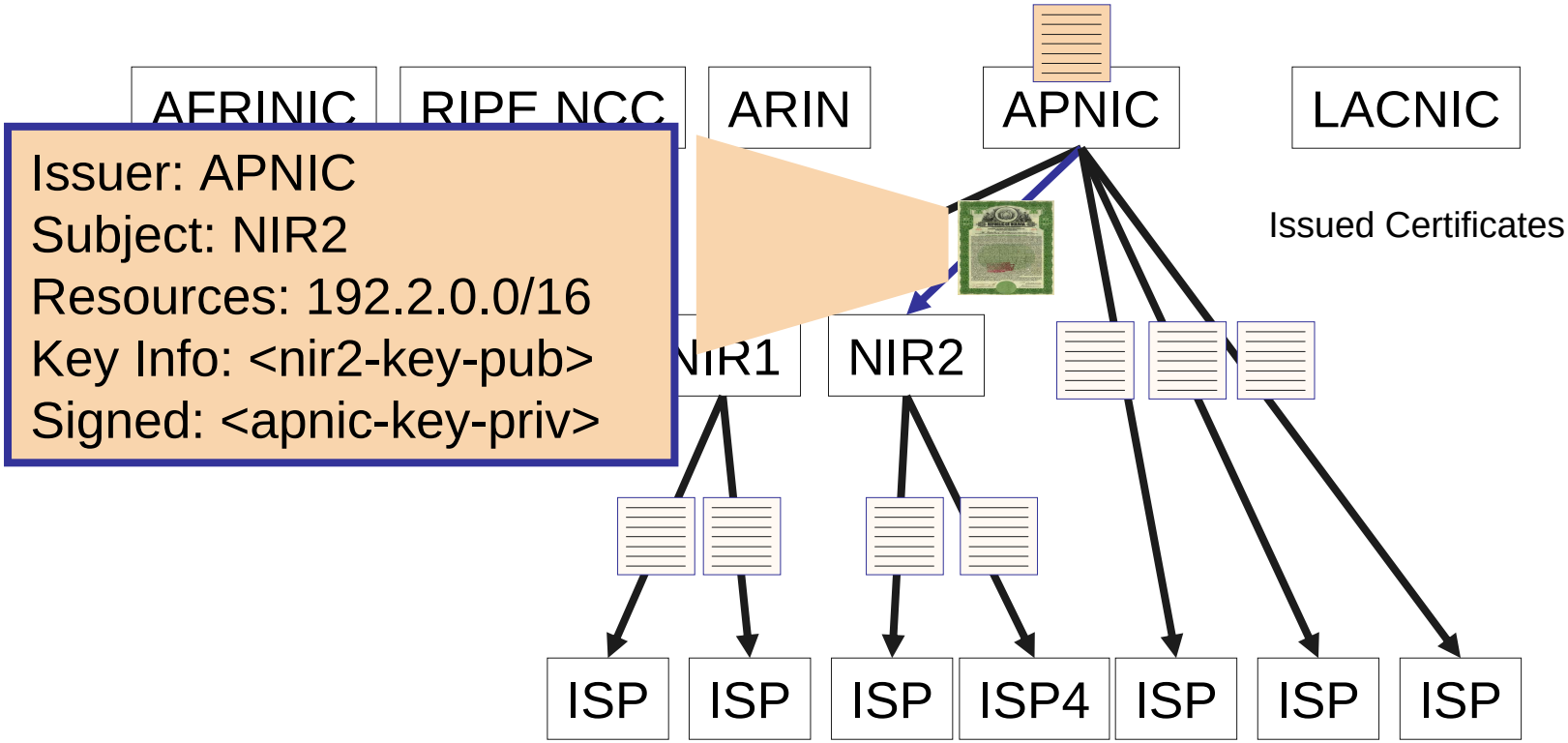
Resource Certificates

Resource
Allocation
Hierarchy



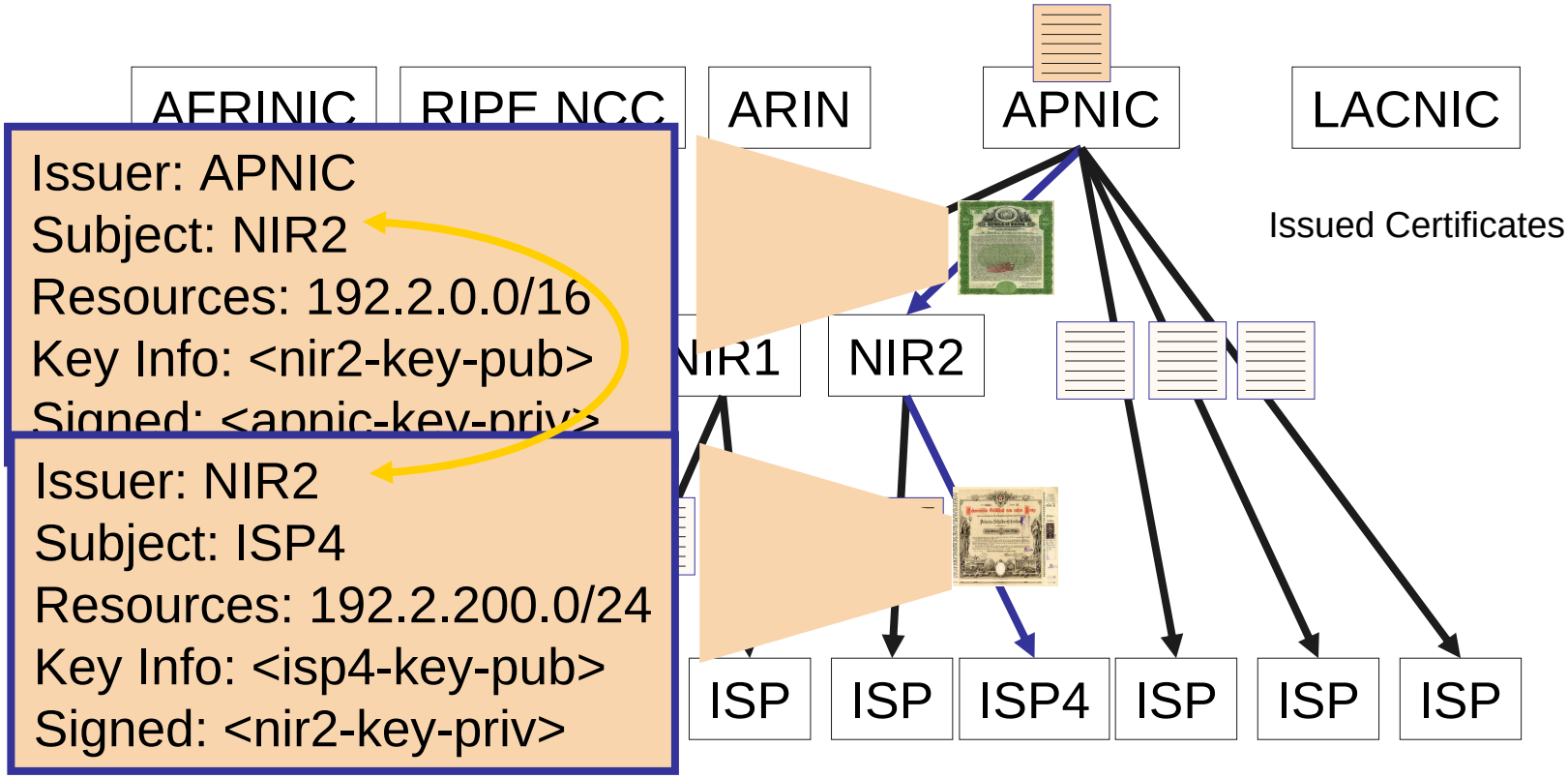
Resource Certificates

Resource
Allocation
Hierarchy



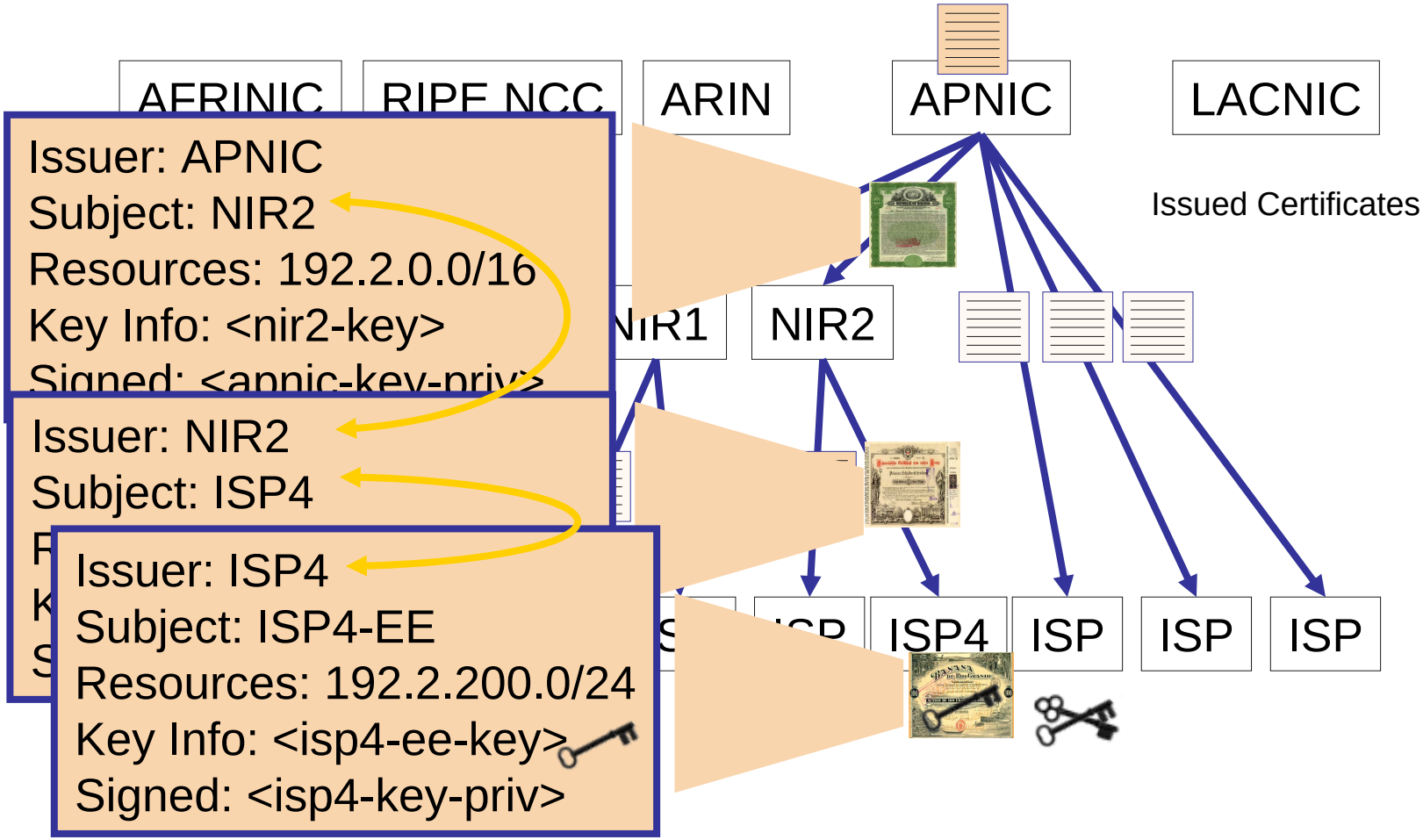
Resource Certificates

Resource
Allocation
Hierarchy



Resource Certificates

Resource
Allocation
Hierarchy

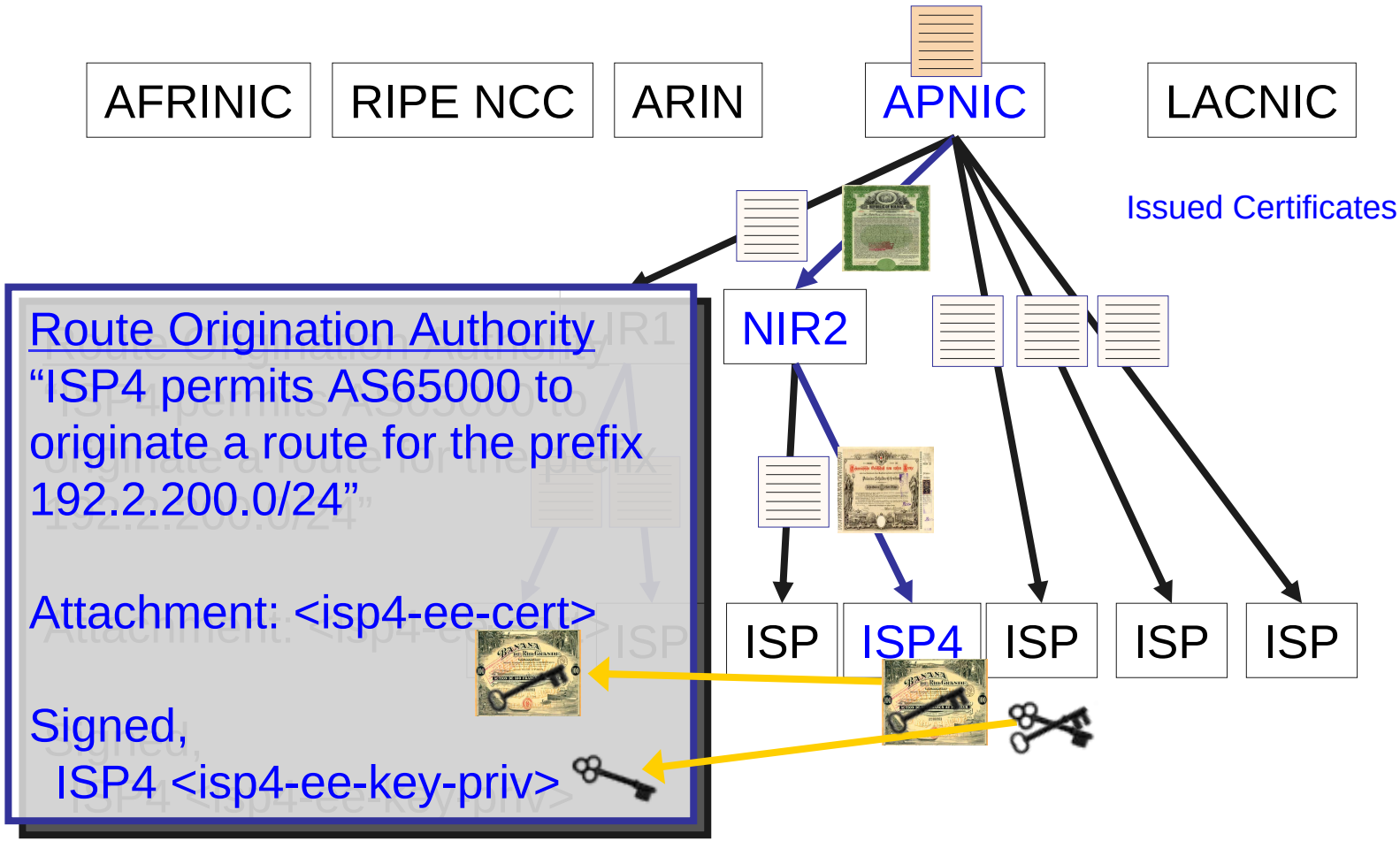


What could you do with Resource Certificates?

- You could sign routing origination authorities or routing requests with your private key, providing an authority for an AS to originate a route for the named prefix. A Relying Party can validate this authority in the RPKI
- You could use the private key to sign routing information in an Internet Route Registry
- You could attach a digital signature to a protocol element in a routing protocol
- You could issue signed derivative certificates for any sub-allocations of resources

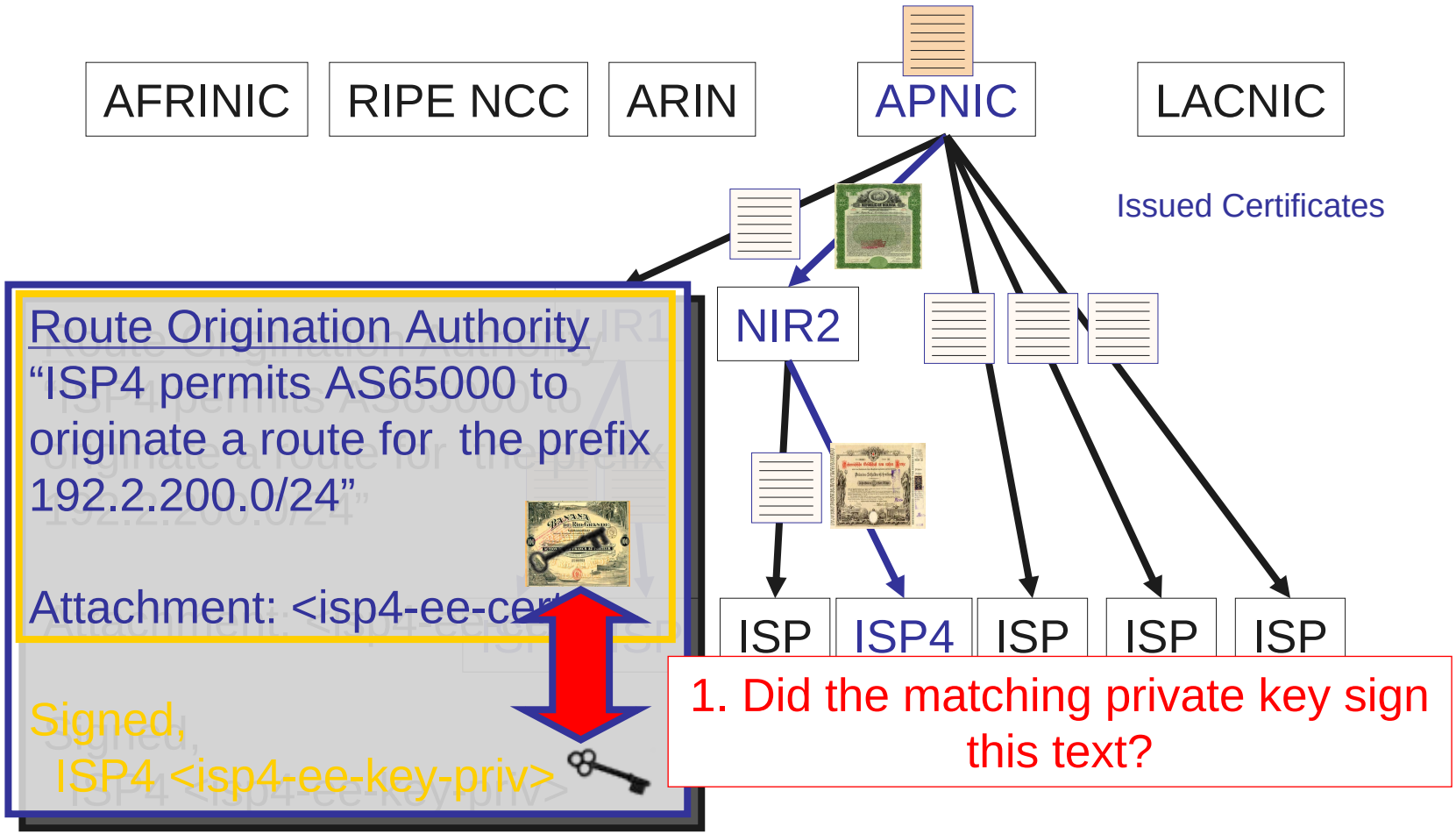
Signed Objects

Resource
Allocation
Hierarchy



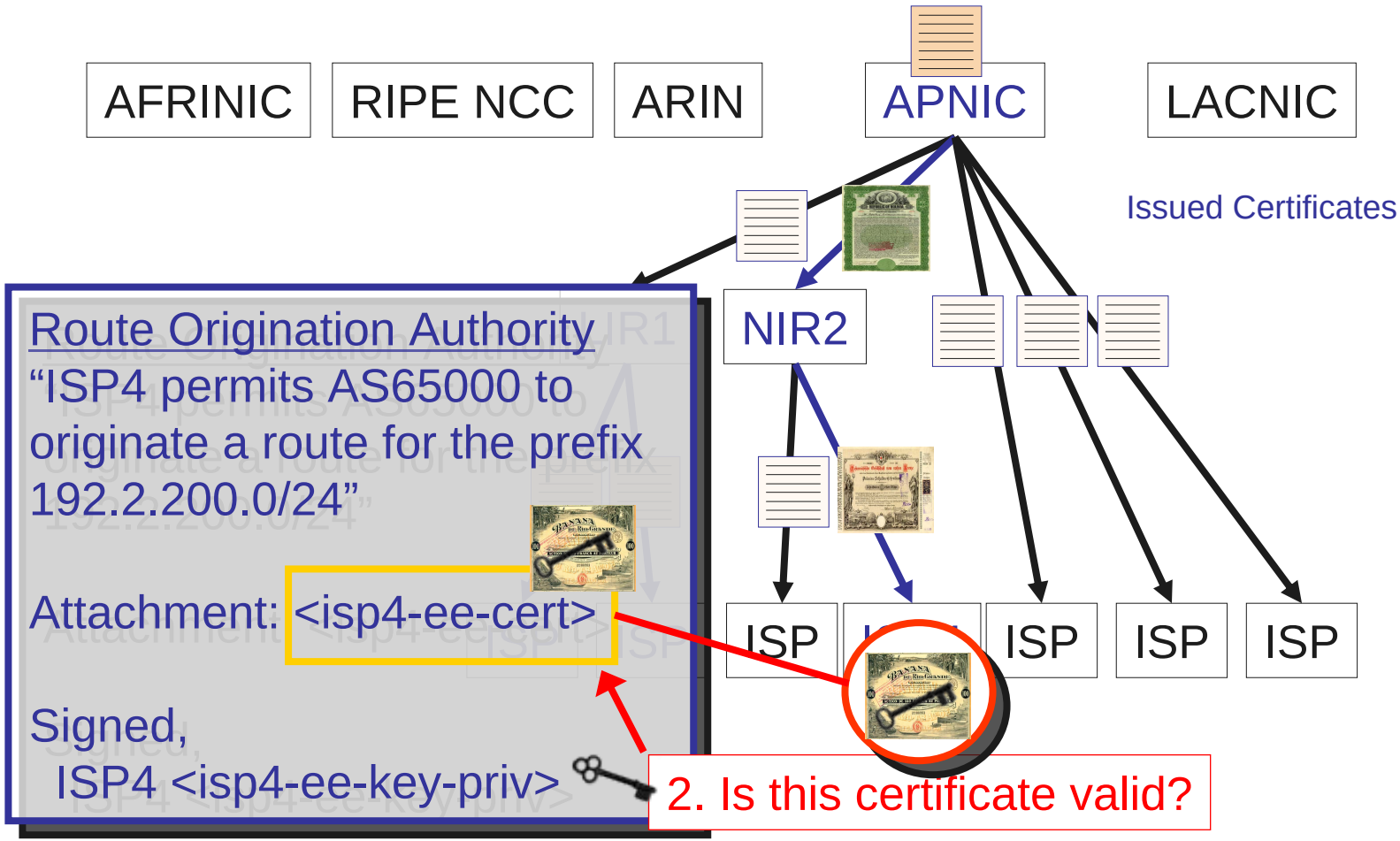
Signed Object Validation

Resource
Allocation
Hierarchy



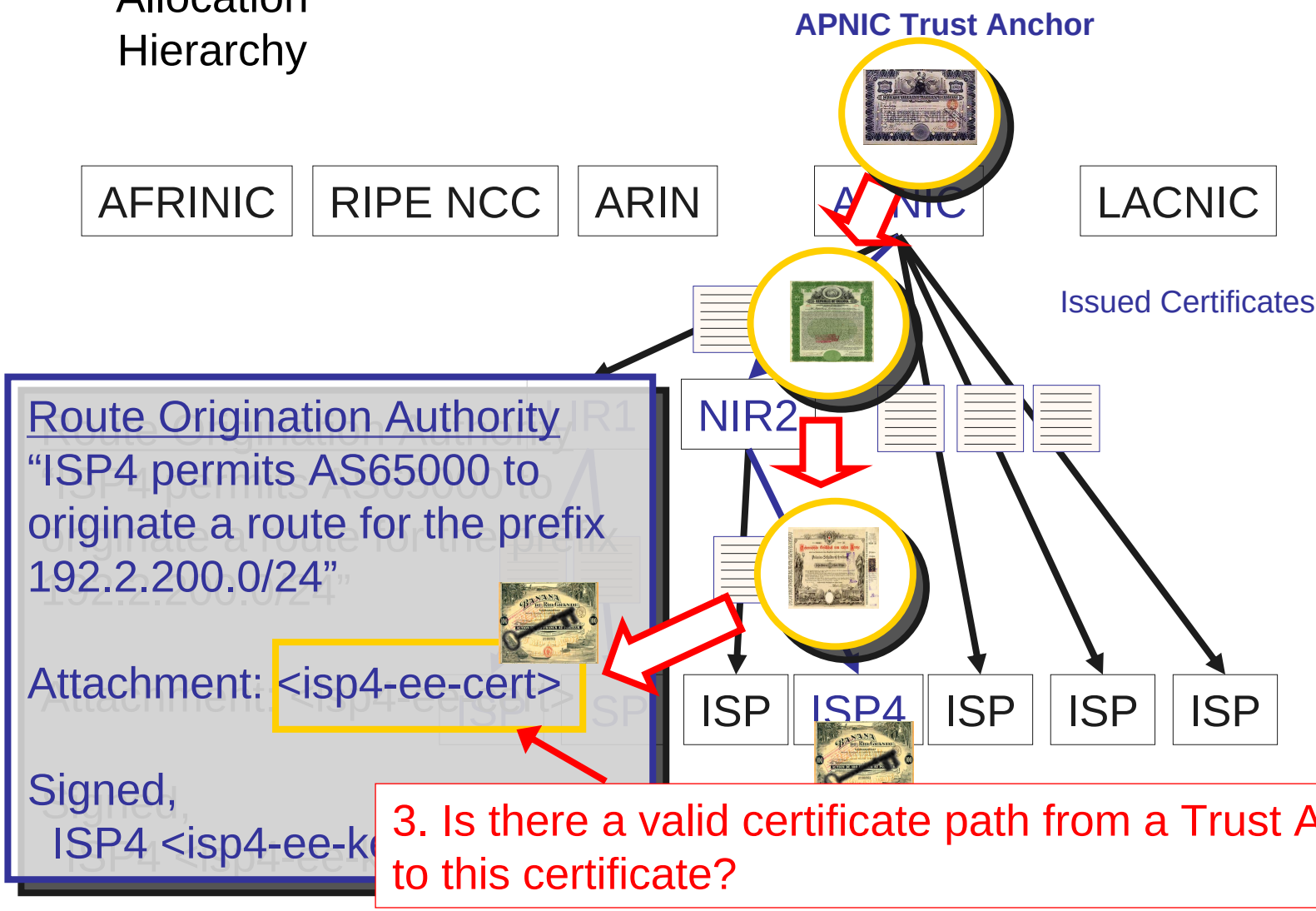
Signed Object Validation

Resource
Allocation
Hierarchy



Signed Object Validation

Resource Allocation Hierarchy



Signed Object Validation

Resource
Allocation
Hierarchy

AFRINIC | RIPE NCC | A

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

Managing Resource Certificates

- Resource Holders ‘enroll’ for certificates using existing trusted relationship between issuer and holder
- Exchange of credentials to establish a secure path between issuer and subject
- Subject and Issuer each operate instances of an “RPKI Engine” to manage certificate issuance actions
- Certificate Issuance reflects the current state of the issuer’s allocation database

Managing Resource Certificates

- Certificate management is an automated process driven by the issuer's allocation database state
- Uses a distributed publication repository system to allow:
  - CA's to publish certificates and CRLs
  - EE's to publish signed objects
- Relying Parties could maintain a local cache of the publication repository framework to allow local validation operations to be performed efficiently

Progress Report

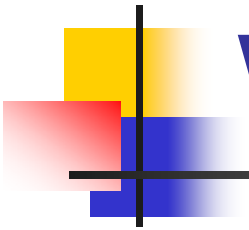
- Specifications submitted to the SIDR WG of the IETF:
  - Specification of a profile for Resource certificates
  - Specification of the distributed publication repository framework
  - Specification of the architecture of the RPKI
  - Specification of profiles for Route Origination Authorization objects (ROAs) and Bogon Origination Attestation objects (BOAs)
  - Specification of the Issuer / Subject resource certificate provisioning protocol

Progress Report

- Implementation Progress
  - Four independent implementation efforts for various aspects of the RPKI are underway at present
  - Tools for Resource Certificate management
    - Requests, Issuance, Revocation, Validation
  - Issuer / Subject certificate provisioning protocol
  - Functional RPKI Engine instance for an RIR integrated into one RIR's production environment
  - Relying Party local cache management
  - RPKI validation tools

Intended Objectives

- Create underlying framework for route security measures
- Assist ISP business process accuracy with Peering and Customer Configuration tool support
- Improve the integrity of published data through the signing and verification capability in Whois, IRR and similar
  - Possibility of removing dependency on where the data was originally published as the derivation of trust in the accuracy of the data, and replace it with the capability to validate the published data, independent of trust in the original publication point, and irrespective of where and how the data has been stored



What this does NOT do

- Act as a replacement for sBGP, soBGP, pgBGP, ...
  - It is intended to provide a validation framework that could support these secure BGP proposals
- Process routing updates and make unvalidated destinations unreachable
  - That’s something that is a local policy preference setting

Current Activity

- ARIN
  - Working through ISC and PSG.NET for code and design work
  - Engine to be placed in the public domain
  - Hope to have pilot service up to test by the end of the year

Current Activity (cont)

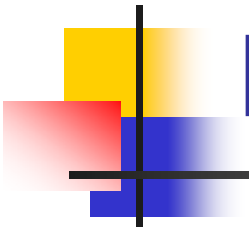
- APNIC
  - Has a working RPKI CA placed into its production platform (Feb 2008)
  - In house development of Perl based implementation of RPKI engine largely complete, with Perl interface to OpenSSL libraries, to be published as an open source software suite
  - Working on hosting services for clients for 2Q 2008 production delivery

Current Activity (cont)

- BBN
  - Resource certificate validation engine (java implementation)
- RIPE NCC
  - In house development of CA/RA manager tool suite

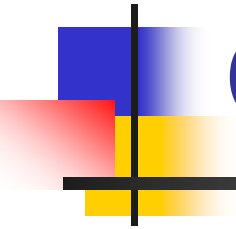
Next Technical Steps

- Tools for ‘hosted’ RPKI services
  - Allow an ISP or an LIR to outsource Resource Certificate management services to an external agency
- Tools to manage attestation and authority generation and signing for end entities
- Relying Party tools to assist in validation functions
- Tools to support RIR functions
- Addition of digital signatures to IRR objects ?
- Specification of use of RPKI by BGP speakers ?



References

- IETF SIDR Working Group
  - http://tools.ietf.org/wg/sidr/
- Working project documentation at:
  - http://mirin.apnic.net/resourcecerts/wiki/index.php/Main_Page
- ISC (funded by ARIN) subversion reference at:
  - http://subvert-rpki.hactrn.net/



Questions?