The Resource Public Key Infrastructure

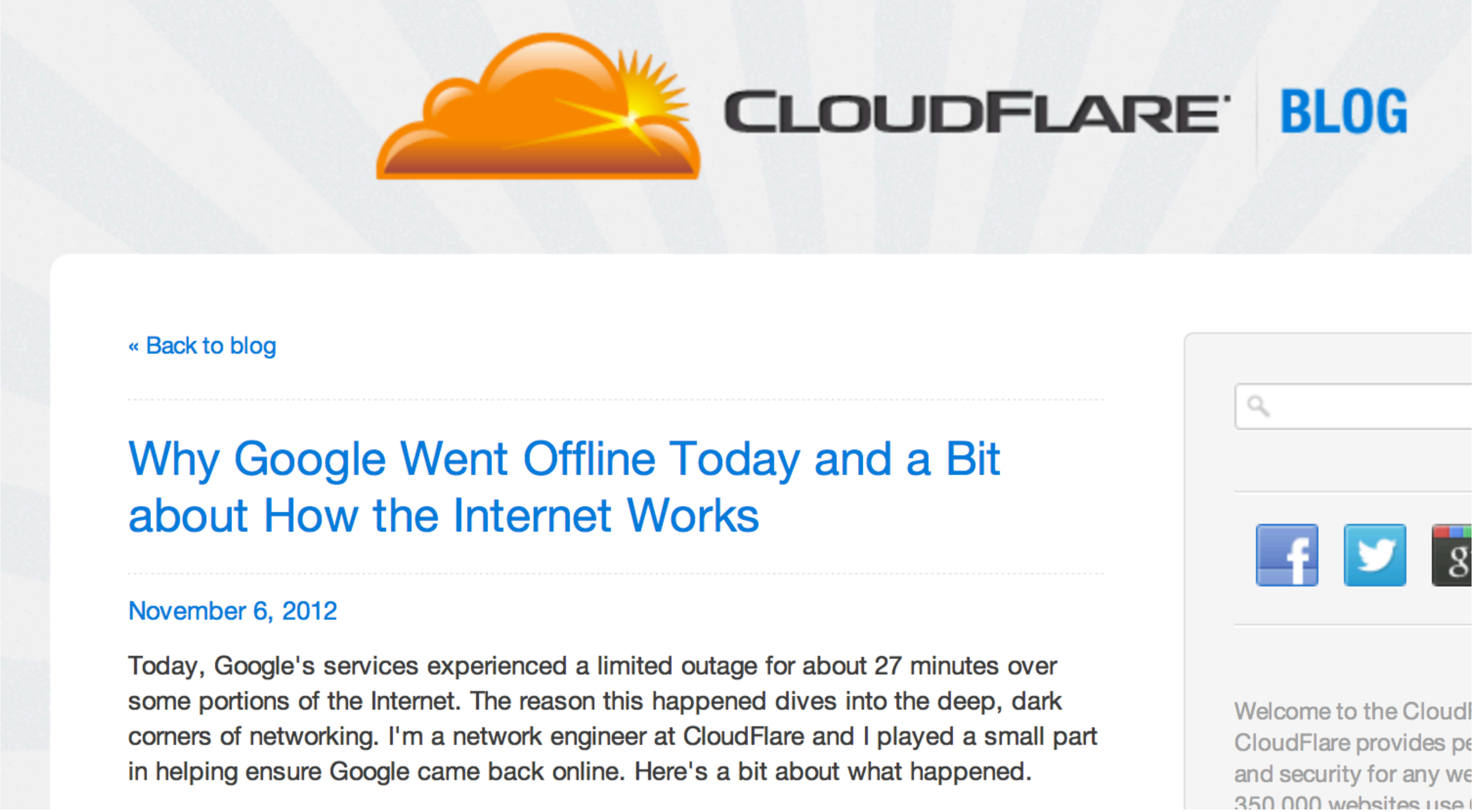
Geoff Huston

APNIC

Today's Routing Environment is Insecure

- Routing is built on mutual trust models
- Routing auditing requires assembling a large volume of authoritative data about addresses and routing policies
  - And this data does not readily exist
- We have grown used to a routing system that has some "vagueness" at the edges
- But this is not good enough...

Earlier this week...



« Back to blog

Why Google Went Offline Today and a Bit about How the Internet Works

November 6, 2012

Today, Google's services experienced a limited outage for about 27 minutes over some portions of the Internet. The reason this happened dives into the deep, dark corners of networking. I'm a network engineer at CloudFlare and I played a small part in helping ensure Google came back online. Here's a bit about what happened.

Welcome to the Cloudf
CloudFlare provides pe
and security for any we
350,000 websites use

Telling “Good” from “Bad” in Routing

Can we set up a mechanism to allow an automated system to validate that the use of an address in routing has been duly authorized by the holder of that address?

Telling “Good” from “Bad” in address use

Can we set up a mechanism to allow an automated system to validate where **attestations about** an address in **any context** has been duly authorized by the holder of that address?

Telling “Good” from “Bad”

This looks a lot like an application of public/private key cryptography, with “authority to use” conveyed by a digital signature

- Using a private key to sign the authority, and the public key to validate the authority
- If the private key was held by the address holder then we have the notion of binding the control over an address to holding the private key
- We can use a conventional certificate infrastructure to support public key validation at the scale of the Internet
- But how can we inject trustable authority into this framework?

Trustable Credentials

How can we inject trustable authority into this framework?

Trustable Credentials

How can we inject trustable authority into this framework?

Bind the Registry and the key structure together:

- Use the existing address allocation hierarchy
  - IANA, RIRs, NIRs & LIRs, End holders
- Describe this address allocation structure using digital certificates
- The certificates do not introduce additional data – they are a representation of registry information in a particular digital format

Resource Certificates

- A resource certificate is a digital document that binds together an IP address block with the IP address holder's public key, signed by the certification authority's private key
- The certificate set can be used to validate that the holder of a particular private key is held by the current legitimate holder of a particular number resource – or not!

- Community driven approach
  - Collaboration between the RIRs since 2006
  - Based on open IETF standards
    - Based on work undertaken in the Public Key Infrastructure (PKIX) and Secure Inter-Domain Routing (SIDR) Working Groups of the IETF

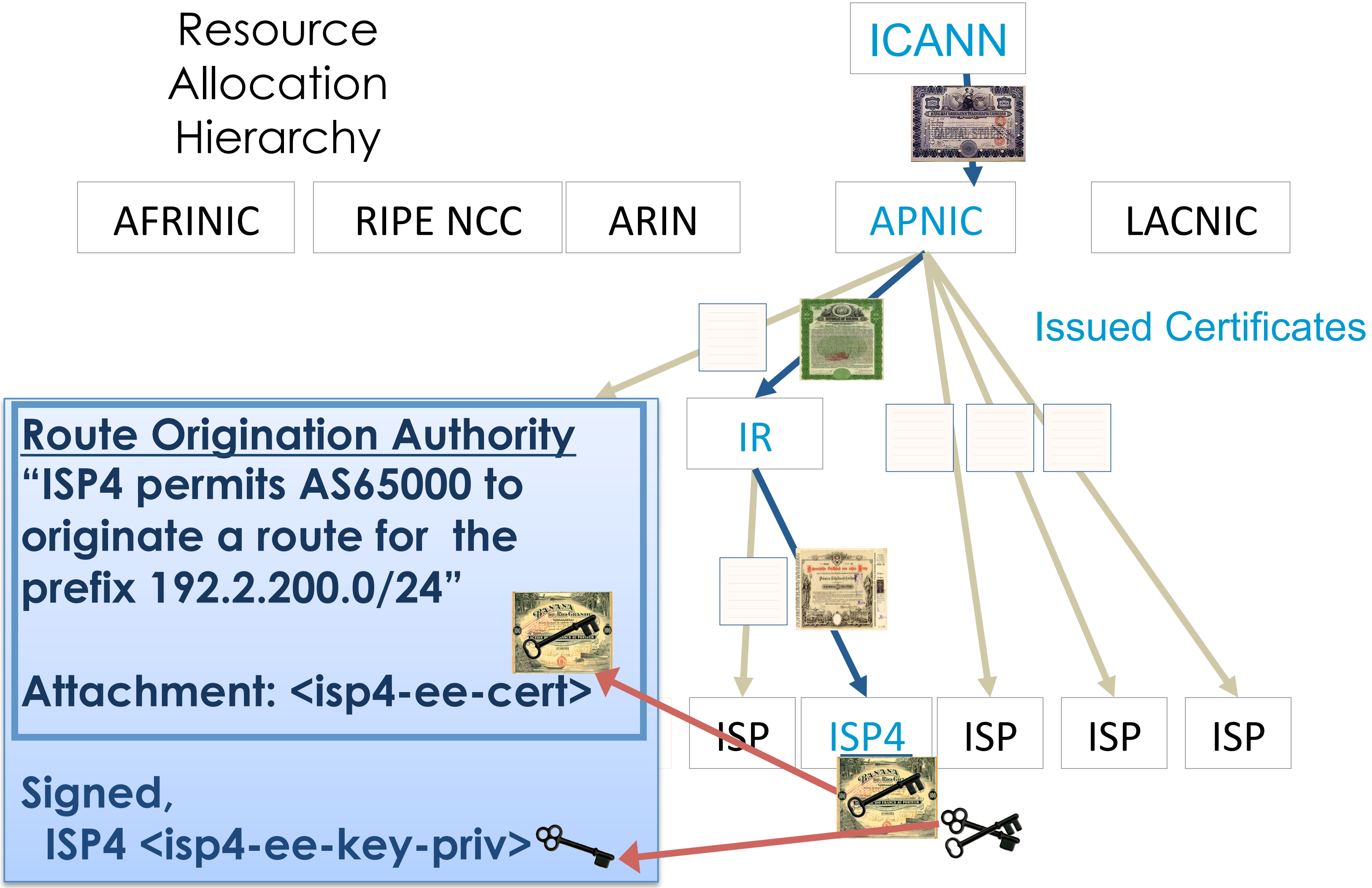
The RPKI Certificate Service

- Enhancement to the RIR Registry
  - – Offers verifiable proof of the number holdings described in the RIR registry
- Resource Certification is an opt-in service
  - – Number Holders choose to request a certificate
    - Derived from registration data

A Number Resource PKI

- The RPKI is a service that offers a means to validate attestations about addresses and their current holder
  - The ability to validate assertions about an entity being the holder of a particular address or autonomous system number
    - “I am the holder of 1.1.1.0/24”
  - The ability to make more reliable routing decisions based on signed credentials associated with route objects
    - “I authorise AS 23456 to originate a route to 1.1.1.0/24”

ROA Validation



Resource
Allocation
Hierarchy

ICANN

AFRINIC

RIPE NCC

ARIN

APNIC

LACNIC

Issued Certificates

IR

ISP

ISP4

ISP

ISP

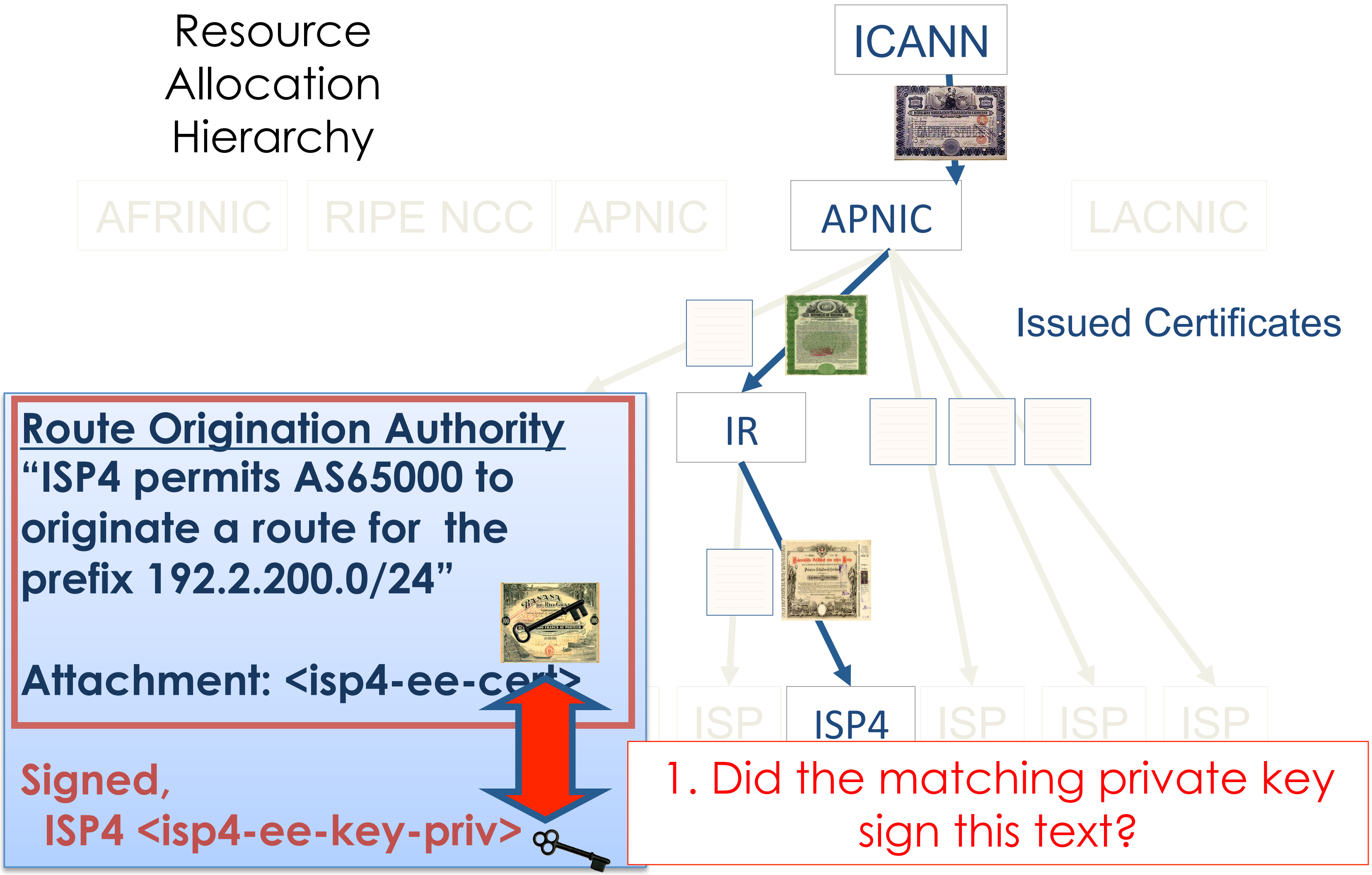
ISP

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>

ROA Validation



Route Origination Authority

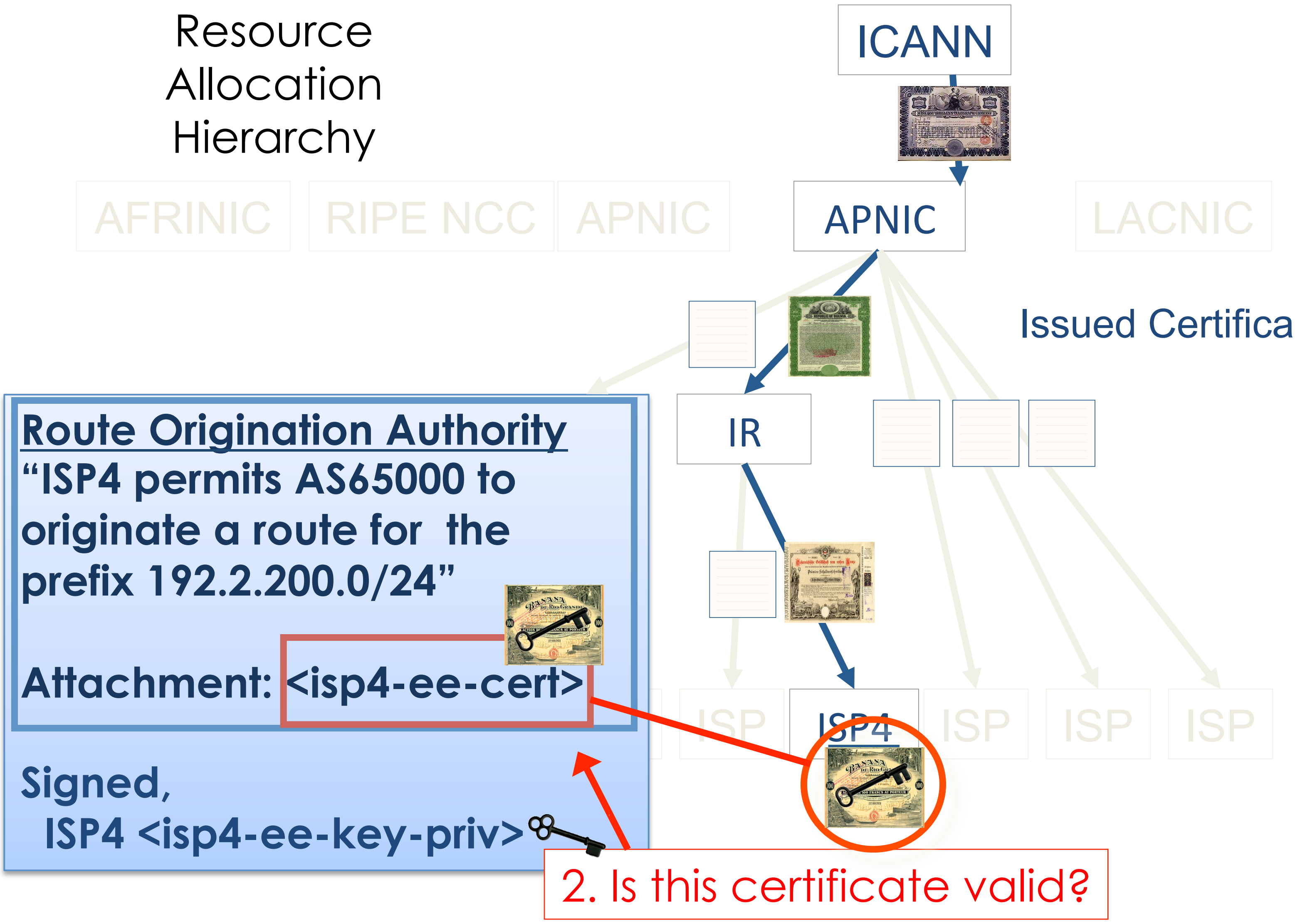
"ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24"

Attachment: <isp4-ee-cert>

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

1. Did the matching private key sign this text?

ROA Validation



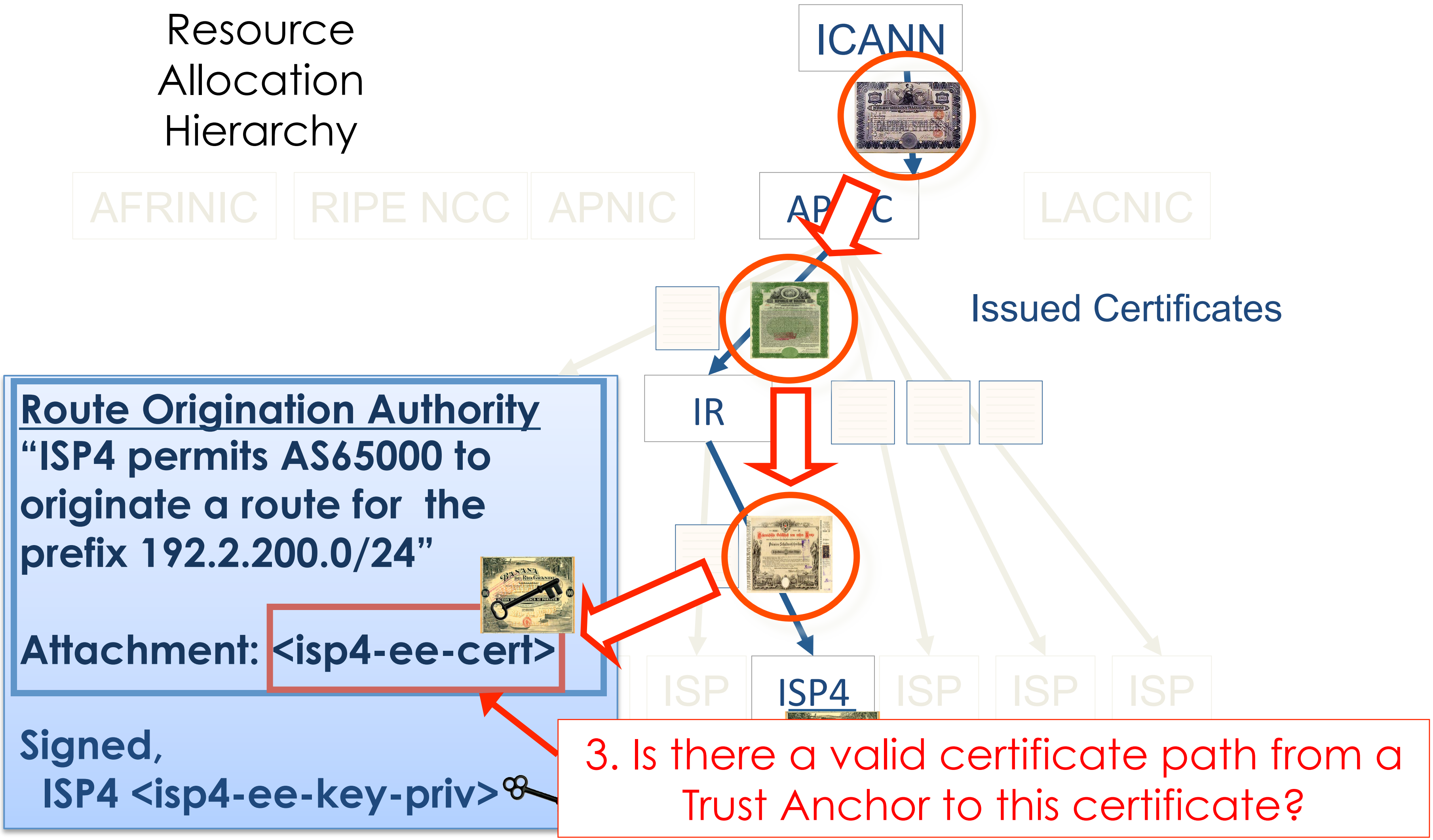
Route Origination Authority
"ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24"

Attachment: <isp4-ee-cert>

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

2. Is this certificate valid?

ROA 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>

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

Activities

- Open Standards
  - Resource Certificates
  - Resource Public Key Infrastructure
  - Certification Policies
  - Secure Origination Routing
  - Secure Path Routing

Activities

- Open Tools
  - RPKI Certification Authority toolset
  - RPKI validators
  - RPKI-to-router toolset
- Vendor Implementations
  - Secure Origination in BGP using RPKI

Current Activities

- Certificate Infrastructure
  - Integration of Certificate Issuance Systems into production services
  - Signing and validation service modules as plugin modules for other apps
  - Tools for the distribution and synchronization of the certificate store
- Secure Routing Systems
  - Specification of AS Path signing extensions to BGP