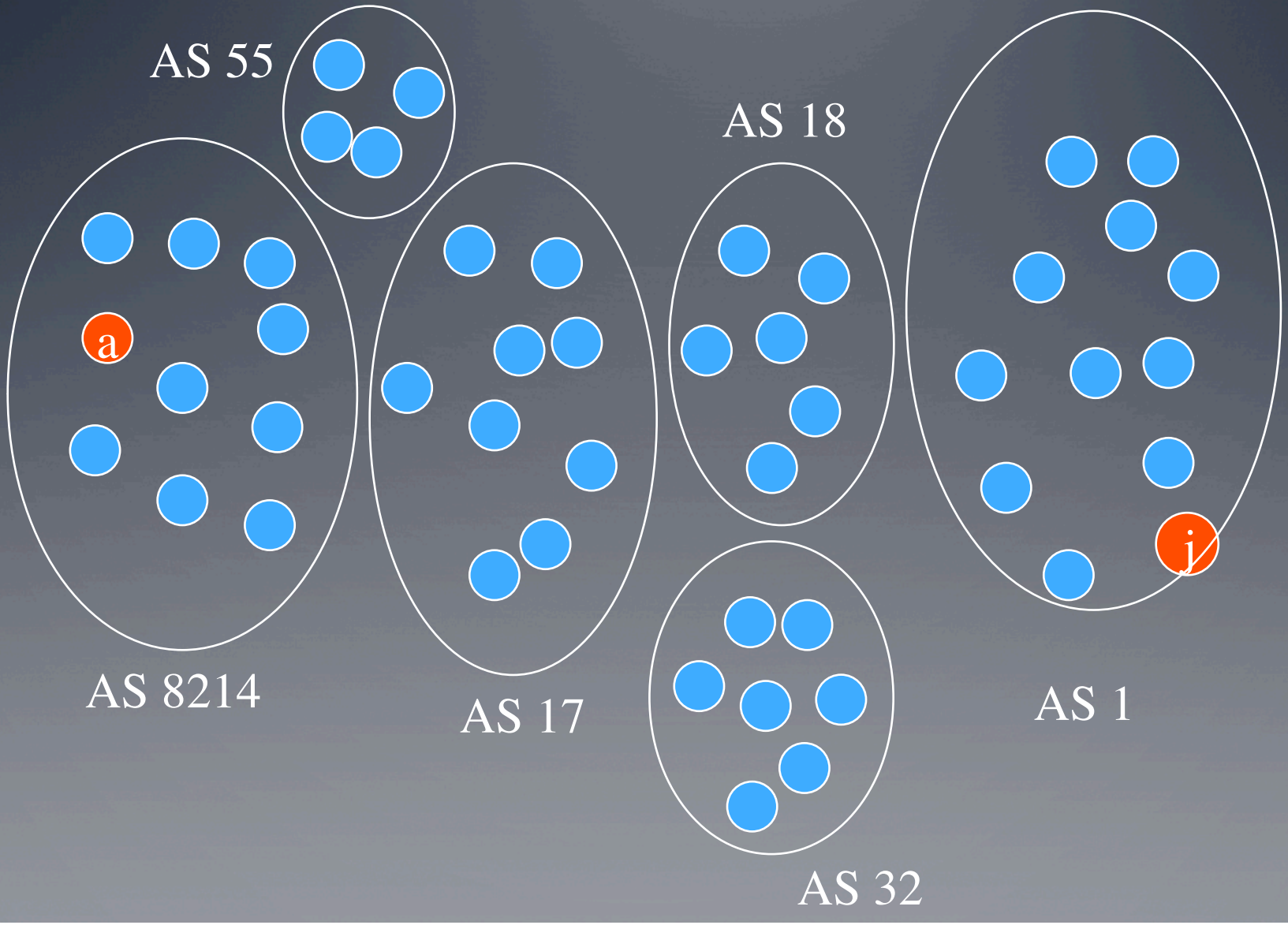
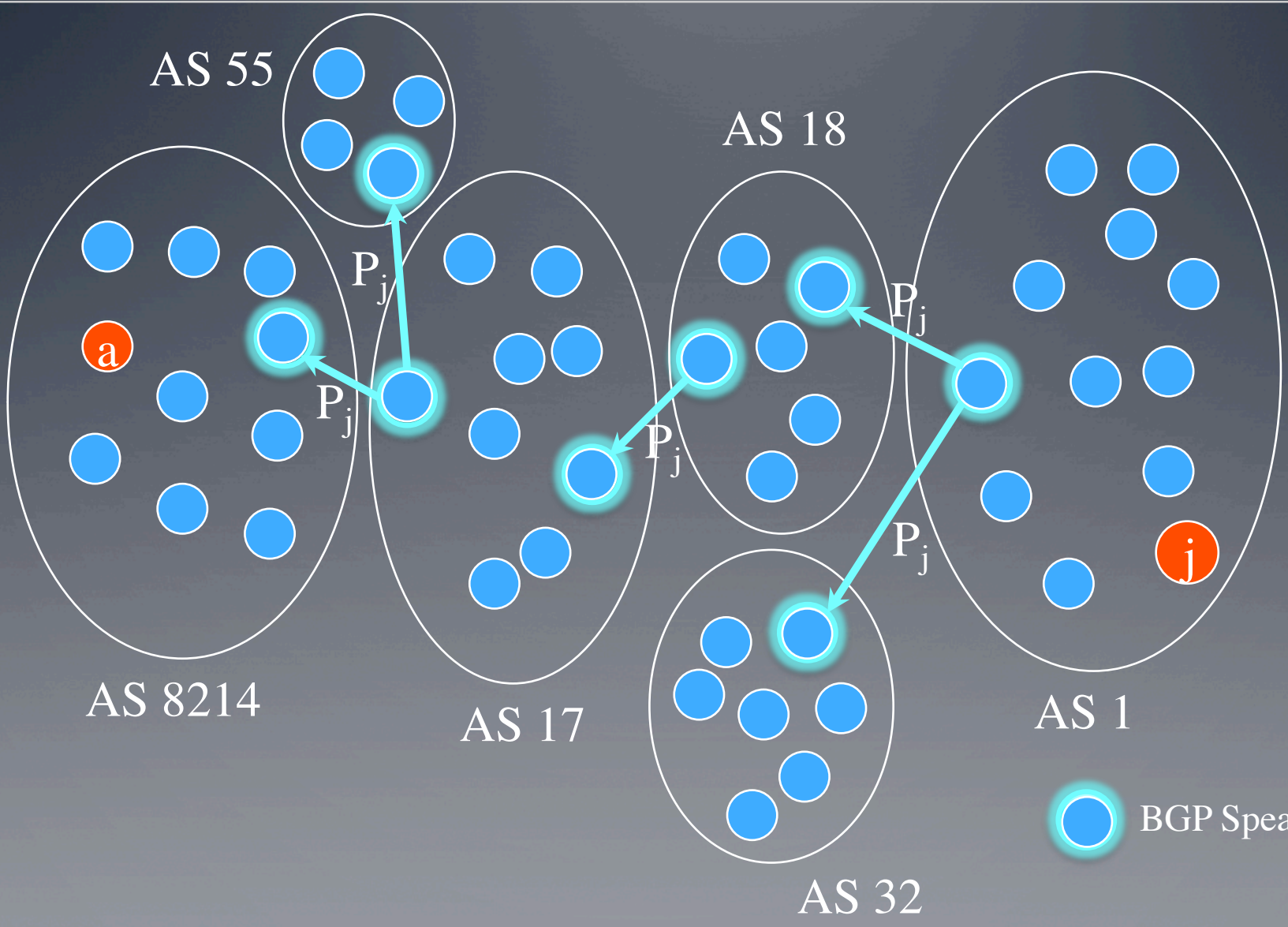
The Resource PKI: A Public Key Infrastructure for IP Addresses & Autonomous Systems

Richard Barnes
BBN Technologies

How Internet Routing Works



BGP Advertisements



The BGP Security Problem

- BGP is critical infrastructure for Internet inter-domain routing
- Benign configuration errors have wreaked havoc for portions of the Internet address space
- The current system is highly vulnerable to human errors, as well as a wide range of attacks
- At best, BGP uses point-to-point keyed MAC & no automated key management
- Solutions must take into account the realities of Internet topology, size, update rates, ...

Current approaches

- Point-to-point BGP security
  - Doesn’t address bad announcements that are properly originated
- Route filtering
  - Need good inputs to build good filters
- Route information databases
  - Need authentication that route information is authentic

BGP Incidents

- Regular benign and malicious errors
  - Spammers hijacking prefixes to source mail
  - Leaks of the full routing table
- A few large-scale events every year
  - Sep 2005: Bolivian ISP announces /8s for AT&T, XO, BellSouth
  - Feb 2008: Pakistan Telecom announces YouTube /24
    - YouTube drops off net for 2 hours
  - Apr 2010: CHINANET announces bogus routes to around 37,000 prefixes

BGP Security Goals

- **Origin Validation:** Verify that the AS that originates a route is actually authorized to do so
  - The advertised prefix and origin ASN have been properly allocated
  - The holder of the prefix has authorized the AS to route it
- **Path Validation:** Verify that BGP announcement has actually transited each AS in the AS_PATH
- Origin validation prevents redirection **to** an unauthorized party
- Path validation prevents redirection **through** an unauthorized party

Solution Constraints

- ISPs and subscribers should want improved BGP security, but who will pay, and who will benefit?
- Changes to router software and/or hardware are very difficult to effect
  - Router vendors need to be persuaded this is a good way to spend scarce development resources
  - ISPs need to be convinced that they should buy and deploy new routers, or upgrade existing routers
- Improvements that do not require changes to routers are much more likely to be deployed!
- The RPKI project is a first step towards improved routing security

RPKI Project Strategy

- The RPKI project attempts to create an infrastructure to address this problem
- Develop an architecture, standards and software to support secure routing in the public Internet
  - Architecture relies on an X.509-based PKI to bind resources with resource holders
  - Certificates use RFC 3779 extensions to represent address space and AS number resources
  - PKI parallels the extant resource allocation scheme
  - Standards pursued in the IETF, in the Secure Inter-Domain Routing (SIRD) WG
- Encourage appropriate organizational entities to develop the software and deploy the PKI and associated infrastructure

Resource Certification

- Resource certification is the issuance of public key certificates to holders of Internet number resources
  - IP address space (both IPv4 and IPv6)
  - Autonomous System numbers (AS #'s)
- These certificates, used in conjunction with other digitally signed objects, provide a basis for improving routing security in the public Internet
- This presentation offers an overview of the Resource Public Key Infrastructure (RPKI) being developed in the Secure Inter-domain Routing (SIDR) Working Group of the Internet Engineering Task Force (IETF)

What is the RPKI?

- The RPKI is a global, X.509-based PKI in which certificates are issued to holders of IP (v4/v6) address space and AS #'s
- The certificates issued in the RPKI do NOT attest to the identity of the private key holder
  - They serve as capabilities (authorization tokens)
  - None of the certificates have meaningful DNs
- The RPKI has an unusual relying party model
  - Almost every relying party (ISP) is also a certification authority (CA)
  - Every ISP will process every certificate & CRL, at least daily, perhaps more often

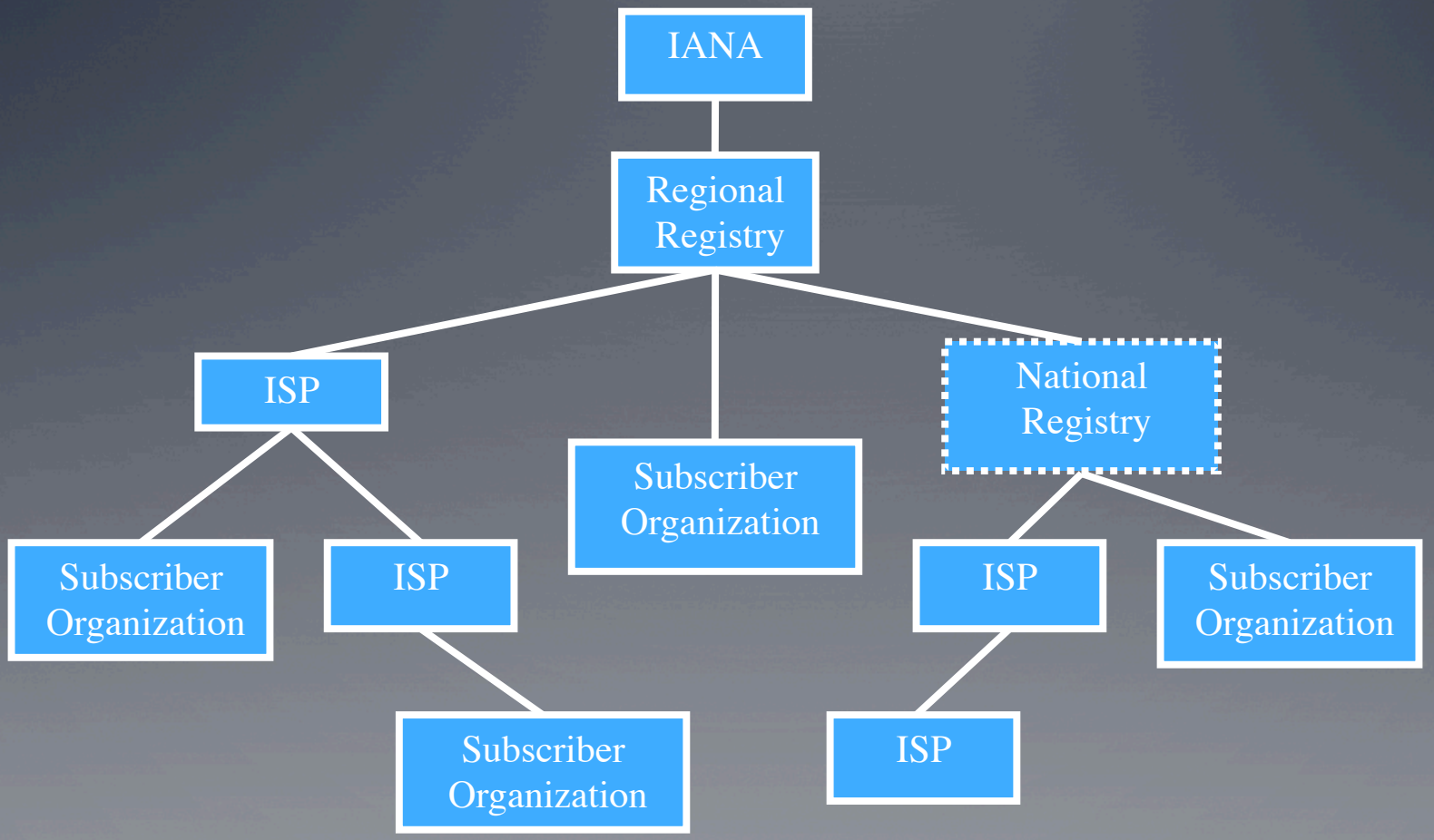
Motivations for the RPKI

- Inter-domain routing in the public Internet (BGP-based routing) is very insecure
- The Pakistan Telecom hijacking of YouTube address space illustrates how (even benign) BGP errors can cause problems
- Ultimately, changes to router software & hardware will be required to address all of the vulnerabilities, but an incremental approach is needed in the near/mid term
- As IPv4 address space becomes scarce, trading will result, and a “title” system for address space is critical to the creation & operation of an orderly “market”

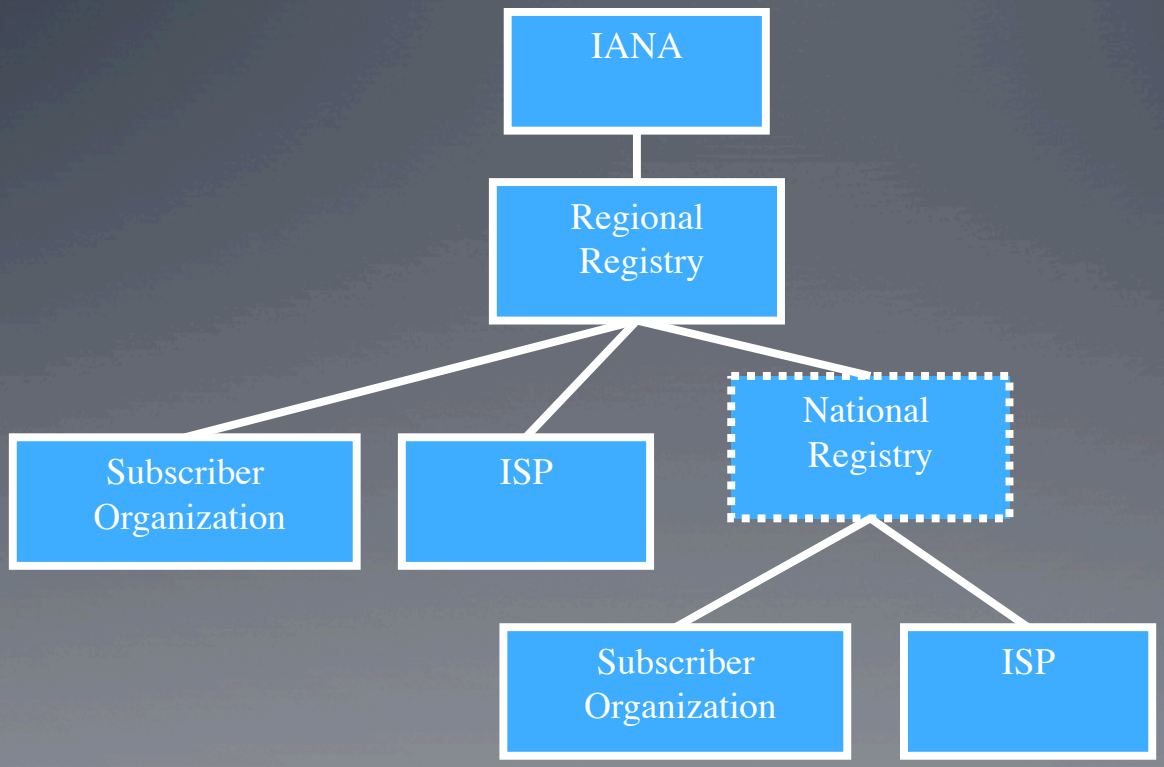
Aspects of the RPKI

- The RPKI is a complex infrastructure with many aspects
  - Certification authorities, relying parties, a repository system
  - A profile for X.509 certificates & CRLs
  - Certificate extensions (RFC 3779) to represent address space and AS #'s
  - Definitions for application-specific digitally signed objects (e.g., ROAs and manifests)
  - An operations model for ISPs to use the RPKI
  - A definition for how routers use RPKI data to improve BGP routing security

Address Allocation Hierarchy



AS Number Assignment Hierarchy



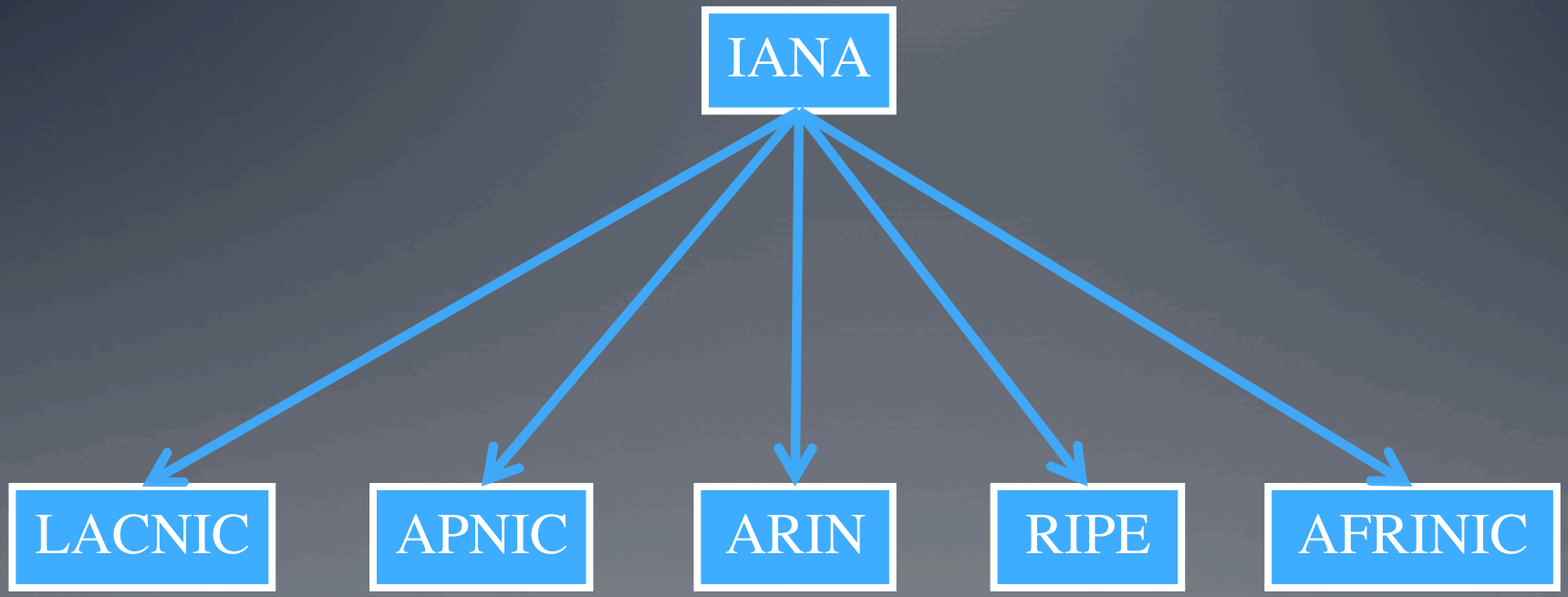
RPKI Elements (1/2)

- All certificates are “resource certificates”
  - Attest to holdings of address space and/or AS numbers
  - They do NOT identify the private key holder
  - Every resource holder is a CA
- End-entity (EE) certificates
  - Used to verify application-specific signed objects, e.g., ROAs and manifests (see later)
  - Nominal 1-1 correspondence with signed objects enables simple revocation (via CRL)
  - Most EE certificates follow a one-time-use model, so the private key can be discarded immediately after signing

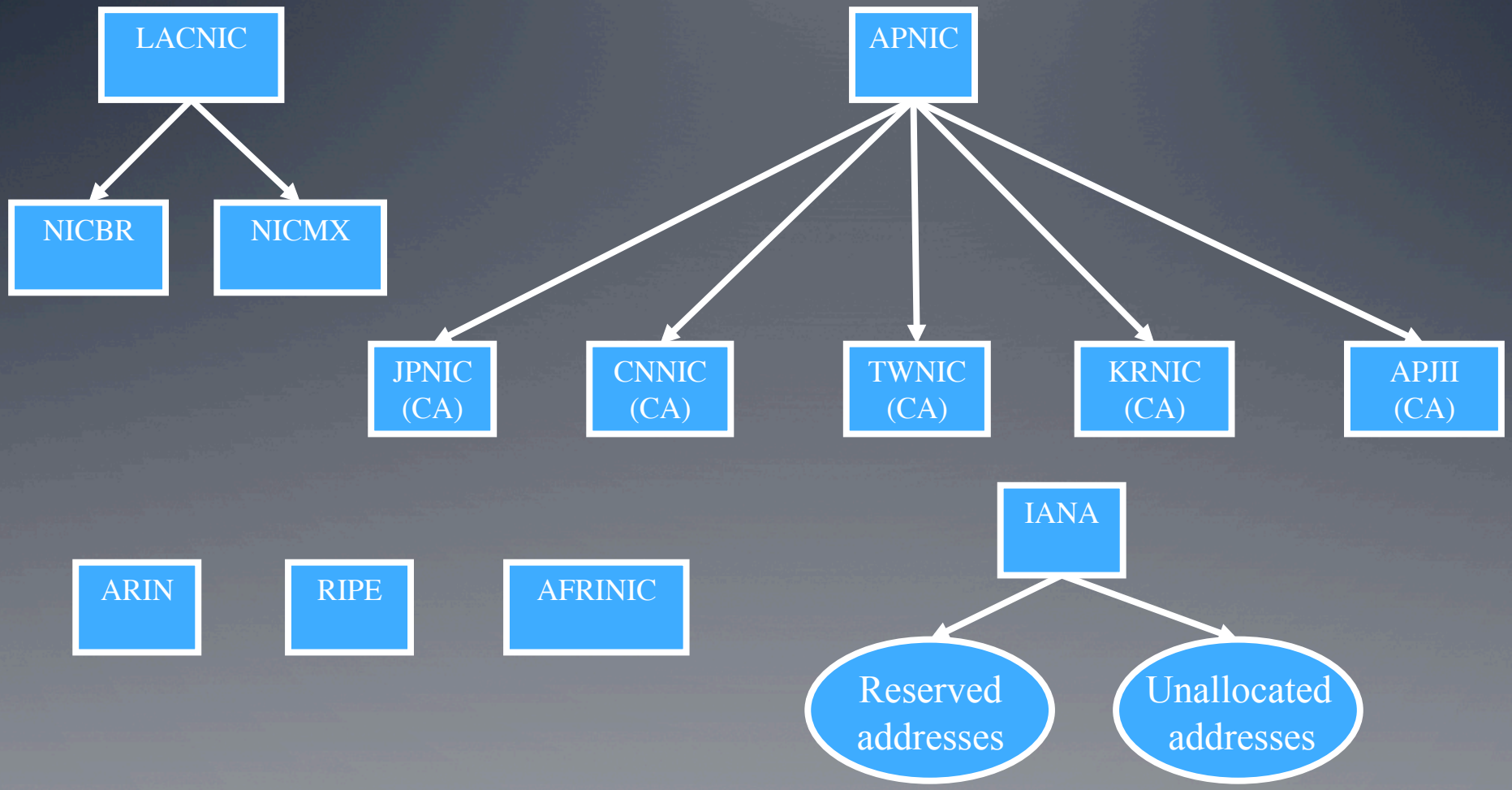
RPKI Elements (2/2)

- Route Origination Authorizations (ROAs)
  - A signed object that identifies an AS authorized by the address space holder to originate route the address space in question
- Manifest
  - A signed object that enumerates file names and hashes to detect missing/replaced objects in the repository system
- Trust anchors
  - Ultimately, every relying party decides which CAs to trust
  - IANA is the obvious trust anchor for the RPKI, since it is the source of all resource allocations
  - The real world is messy …, but we will assume IANA is the TA for this presentation

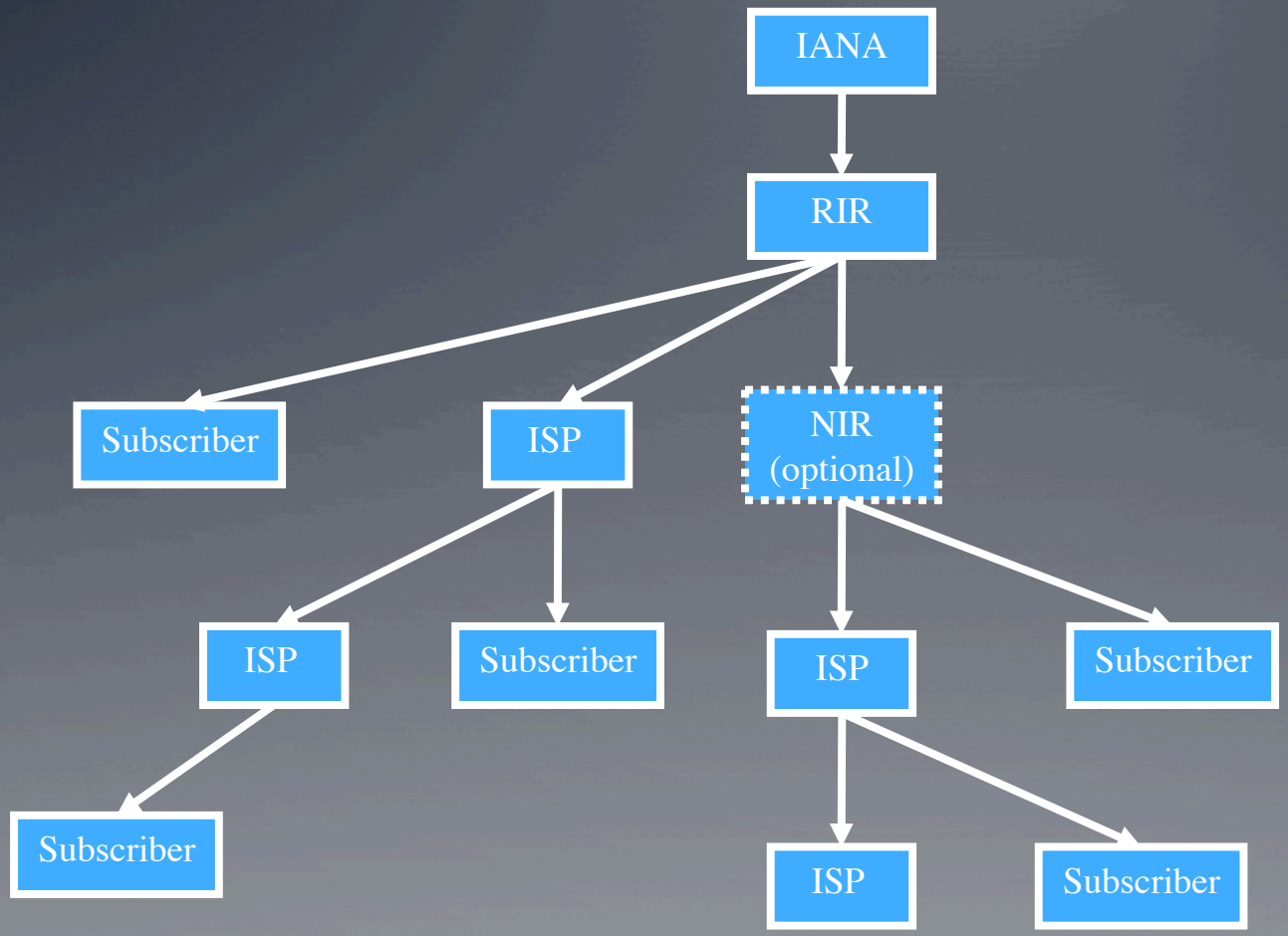
RPKI Tiers 1 & 2 (simple model)



RPKI Tiers 2 & 3



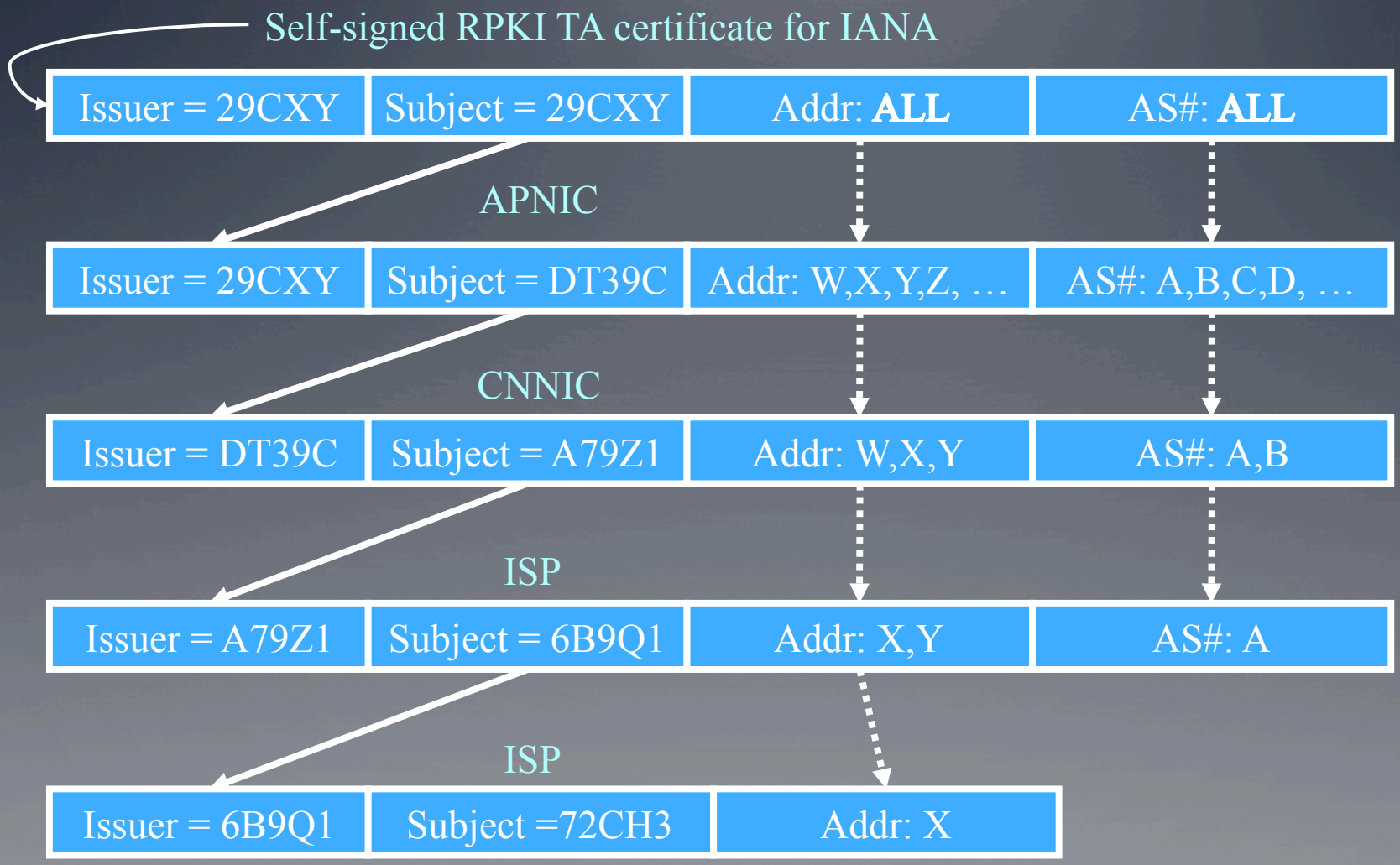
Address Space PKI Vertical Slice



Names

- Every entity has an X.500 distinguished name consisting of just one attribute (common name)
- The common name is an arbitrary character string, generated by the CA (not by the Subject)
- It is not intended to be meaningful!
  - To avoid liability for CAs
  - To help ensure that these certificate are NOT used for any other purposes (e.g., TLS, S/MINE, IPsec)

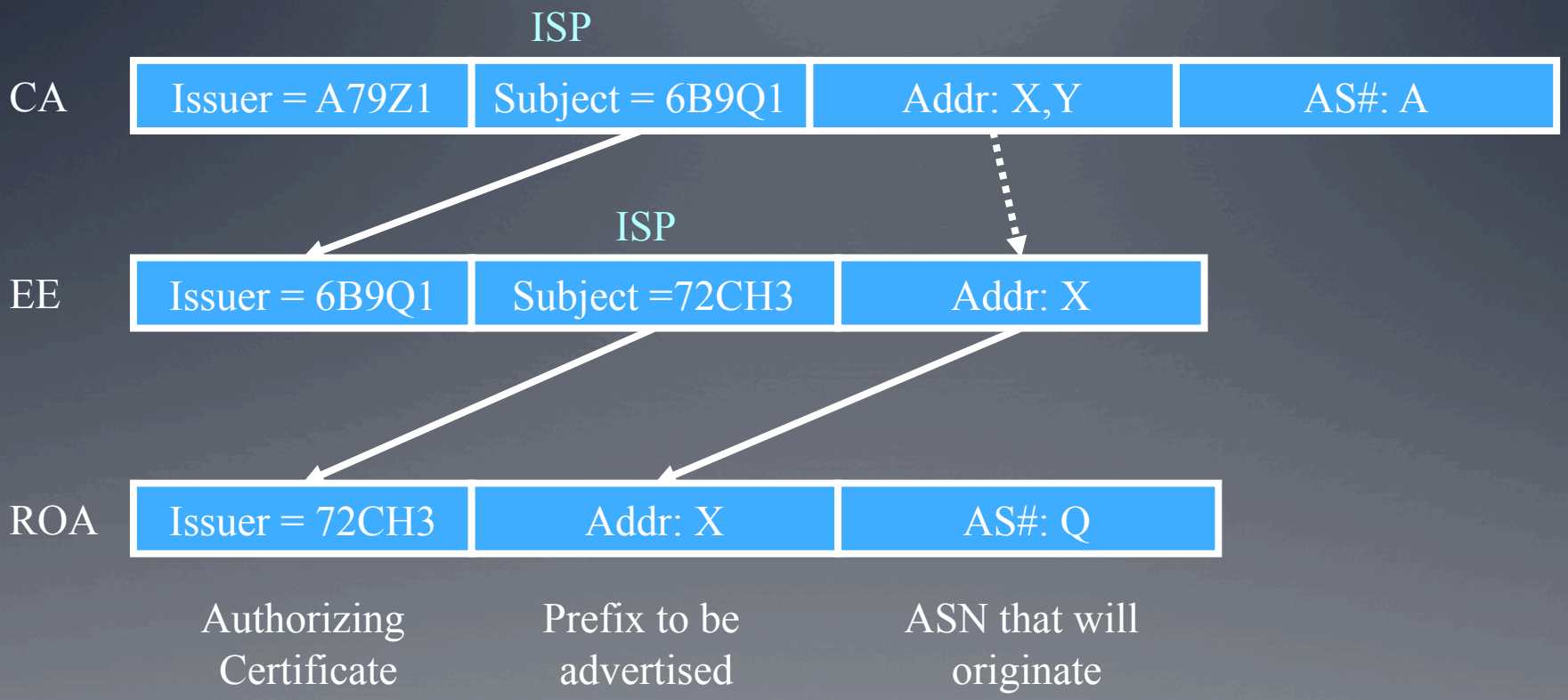
Certificate Chain Example



Route Origination Security

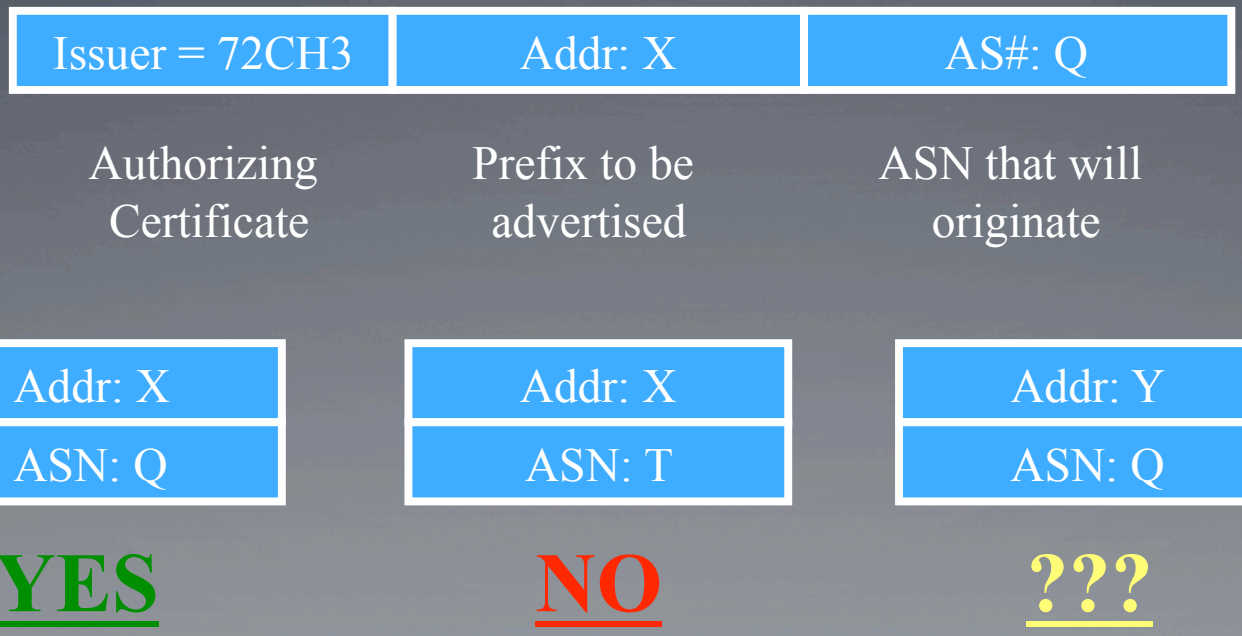
- A Route Origination Authorization (ROA) is an object signed by an address space holder to identify an ISP (by AS #) that is authorized to originate a route for one or more prefixes
- A ROA is verified using an EE certificate issued by the CA associated with the address space in question
- An ISP can verify a ROA and use it to validate the origin of a route in a BGP UPDATE message

Signing ROAs



ROA = Route filter

- ROA specifies a prefix and an ASN
- Any advertisement for that prefix **must** have that ASN as the first hop in the AS_PATH

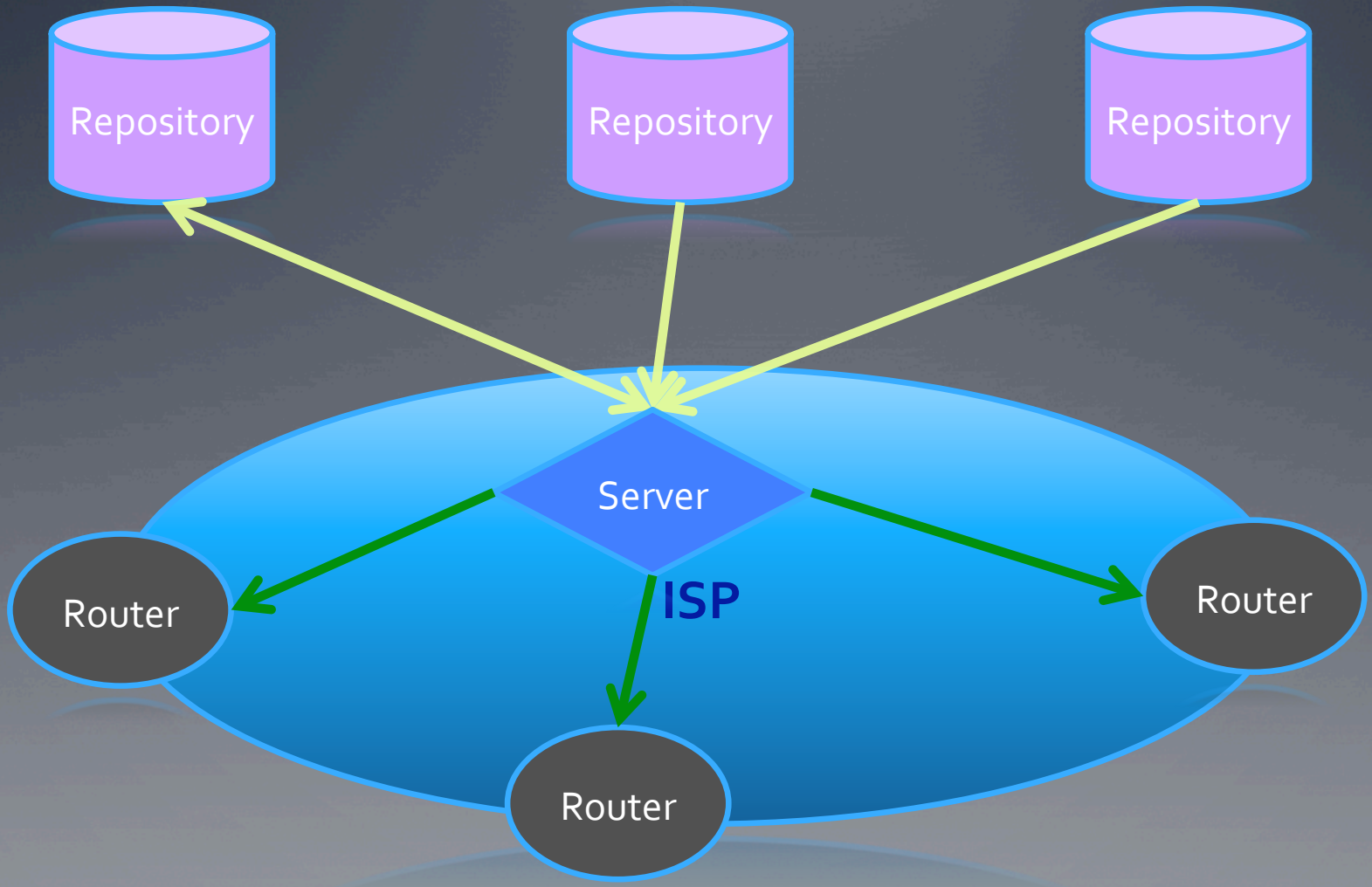


RPKI Operations Model

- Each ISP uploads new certificates, CRLs, ROAs, and manifests, to a repository as needed
- Each ISP downloads all certificates, CRLs, ROAs, and manifests from all repositories (at least daily)
- Relying party software (e.g., in a server) verifies these digitally signed objects, and extracts the ROA data
- Servers distribute the ROA data to BGP routers, enabling these routers to check the origin AS in BGP UPDATE messages

An ISP could, instead, use the validated ROA data to generate route filters for its routers

RPKI Operations Model



Deployment Timeline

- Architecture documents are nearing completion in the IETF SIDR working group
- Cisco and Juniper both have prototype servers that
  - Read and validate RPKI certificate and ROAs
  - Generate route filters
  - Distribute route filters to routers
- All five RIRs are expected to begin issuing certificates on **1 January 2011**
- Some things you can experiment with right now:
  - Use RIPE LIR portal to make certificates and ROAs
  - Use open tools to verify ROAs and generate route filters
    - https://subvert-rpki.hactrn.net/

Summary

- The RPKI provides a basis for improved BGP routing security
  - It enables an ISP to make a local decision about the validity of the origin AS asserted in a BGP UPDATE message, based on authenticated, authoritative data
  - Later enhancement to BGP may extend this sort of validity checking to the entire route expressed in a BGP UPDATE message
- The architecture described here is being deployed by all 5 regional registries, and major router vendors (Cisco and Juniper) are preparing software to make use of the RPKI data

Questions?