A PKI for IP Address Space and AS Numbers

Dr. Stephen Kent

Chief Scientist - Information Security

BBN

TECHNOLOGIES

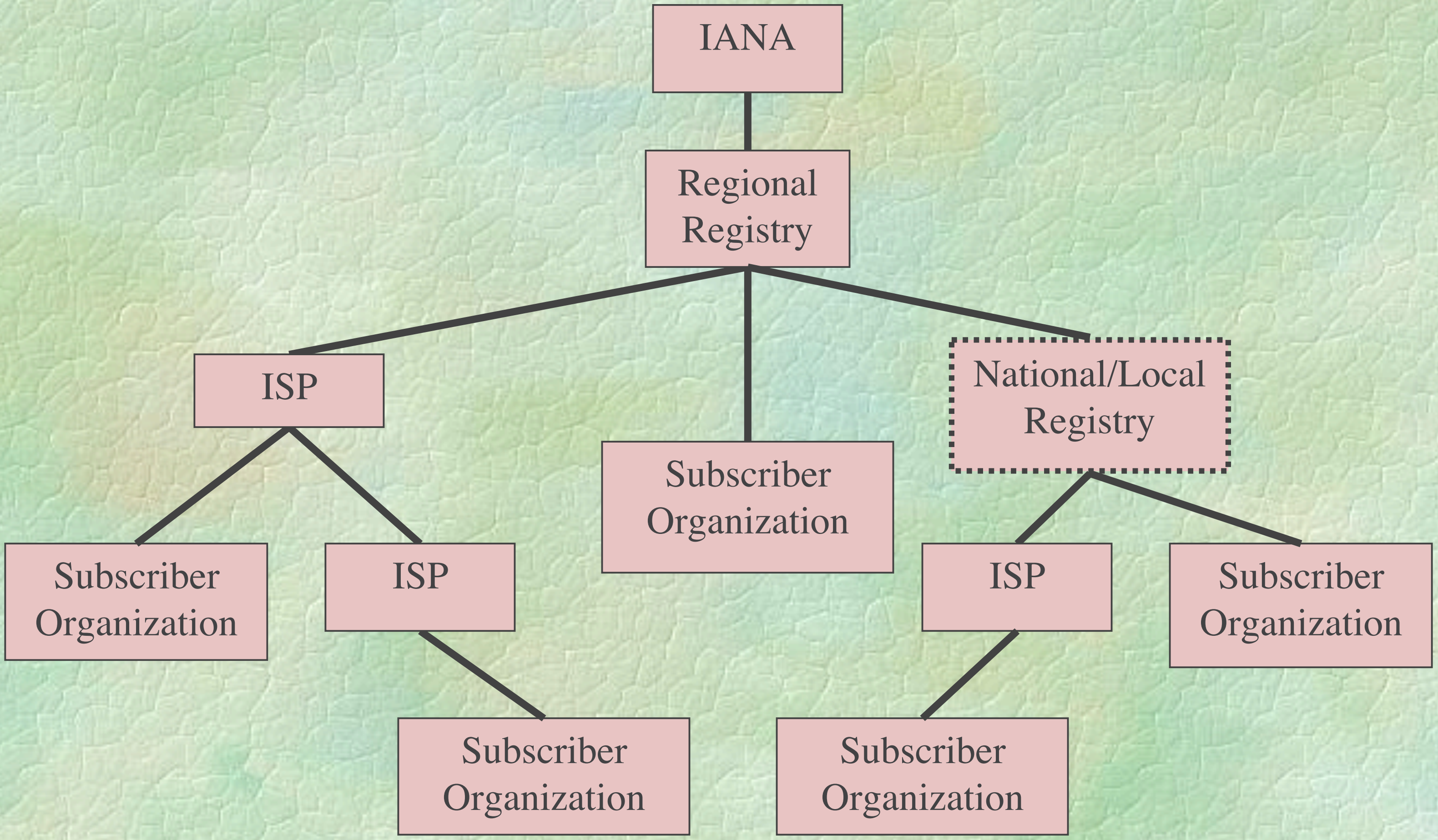
Why A PKI?

- All proposals for improving the security of BGP rely on a secure infrastructure that attests to address space and AS number holdings by ISPs and subscribers
- A PKI is a natural way to satisfy this requirement
- The proposed PKI provides a first step towards improved BGP security, offering a way to detect bogus route origination info in UPDATEs
- It also can help ISPs avoid "social engineering" attacks that attempt to trick them into issuing bogus routes

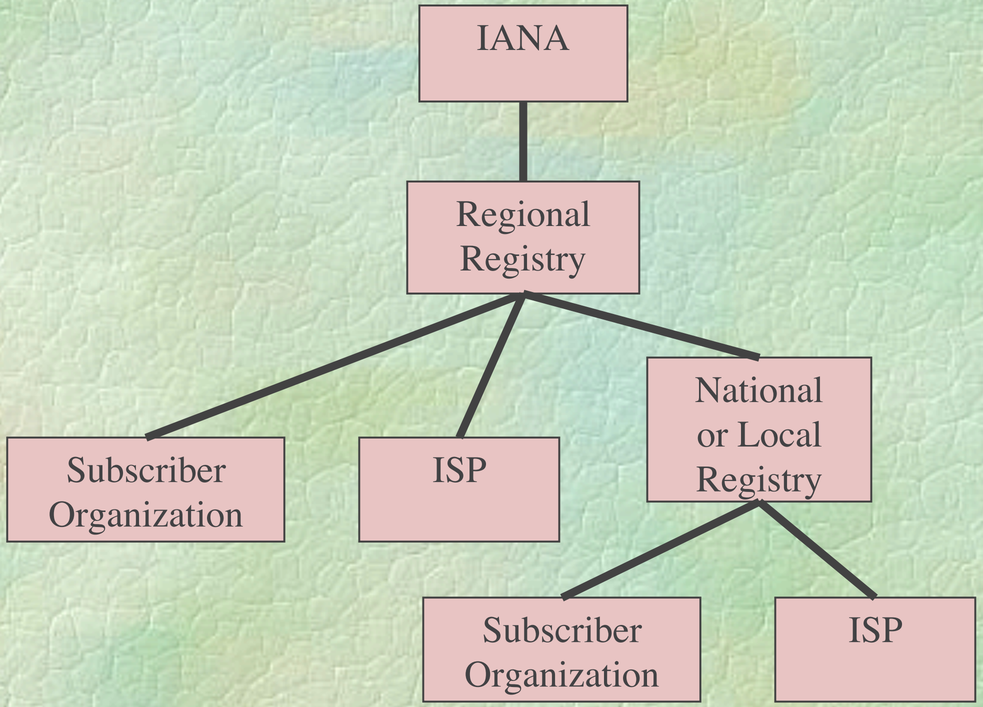
What Does the PKI Look Like?

- The PKI consists of three parts:
  - X.509 certificates that attest to address space and AS number holdings
  - Route Origination Authorizations (ROAs) that allow an address space holder to identify the AS(es) it authorizes to originate routes to its holdings
  - A repository system for these certificates, CRLs, and ROAs
- The PKI makes use of the existing address space and AS number allocation system
- This PKI also embodies the "principle of least privilege," which minimizes the impact of errors or security compromise at each entity in the PKI

Address Allocation Hierarchy



AS Number Assignment Hierarchy



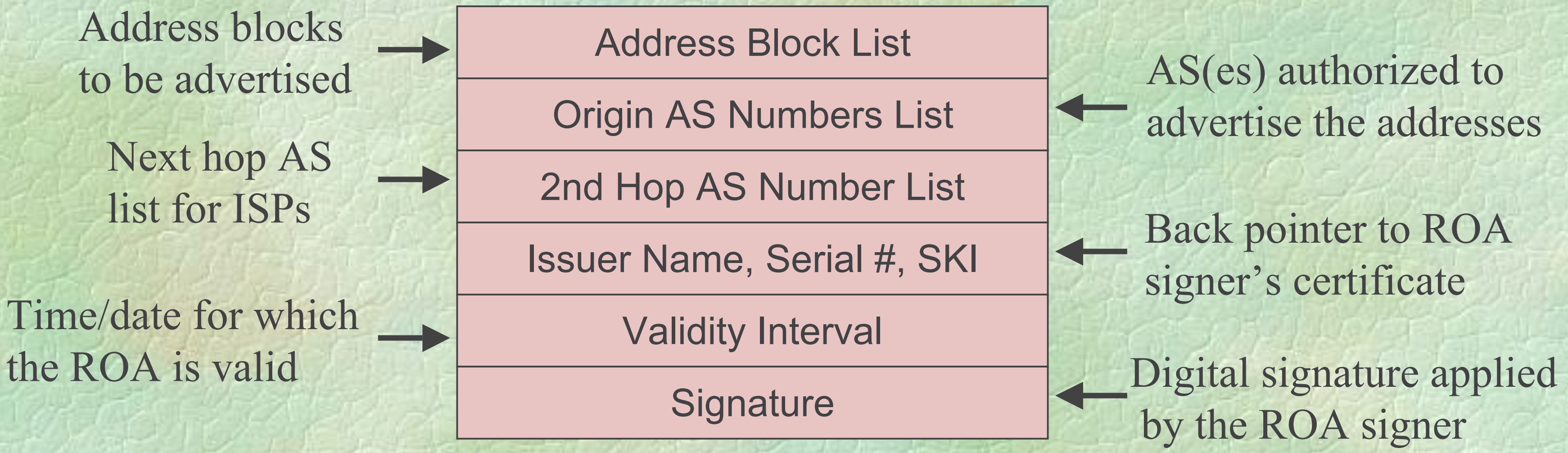
How Does the PKI Work?

- The root issues certificates to the 5 RIRs, and each RIR issues certificates to local/national registries (if applicable) and to ISPs and subscribers
- ISPs issue certificates to downstream providers and to subscribers
- At each tier, each organization issues certificates that match the address space (and AS number) allocations it records in its databases
- All resource holders are certification authorities (CAs)
- The PKI uses two X.509 extensions (defined by RFC 3779) to represent the address and AS number data
- Each certificate path represents sub-allocation by the organizations noted above, a subset constraint that can be verified by ISPs downloading these certificates

Route Origination Authorization

- The initial goal of the PKI is to enable ISPs to verify route origination data
- To support this goal, each address space holder needs to digitally sign a ROA, enumerating the AS(es) authorized to advertise routes on behalf of the address space holder
- An end-entity (shadow) certificate is introduced under each ISP & subscriber CA to facilitate ROA verification
- Since each ISP is an address space holder, it would sign a ROA authorizing itself to advertise the addresses it holds
- An ISP can optionally list next hop ASes for its address space holdings, to provide greater route security coverage, consistent with the notion that an ISP knows the immediate neighbors it authorizes to advertise routes

ROA Format



Address Block List

Origin AS Numbers List

2nd Hop AS Number List

Issuer Name, Serial #, SKI

Validity Interval

Signature

Address blocks to be advertised

AS(es) authorized to advertise the addresses

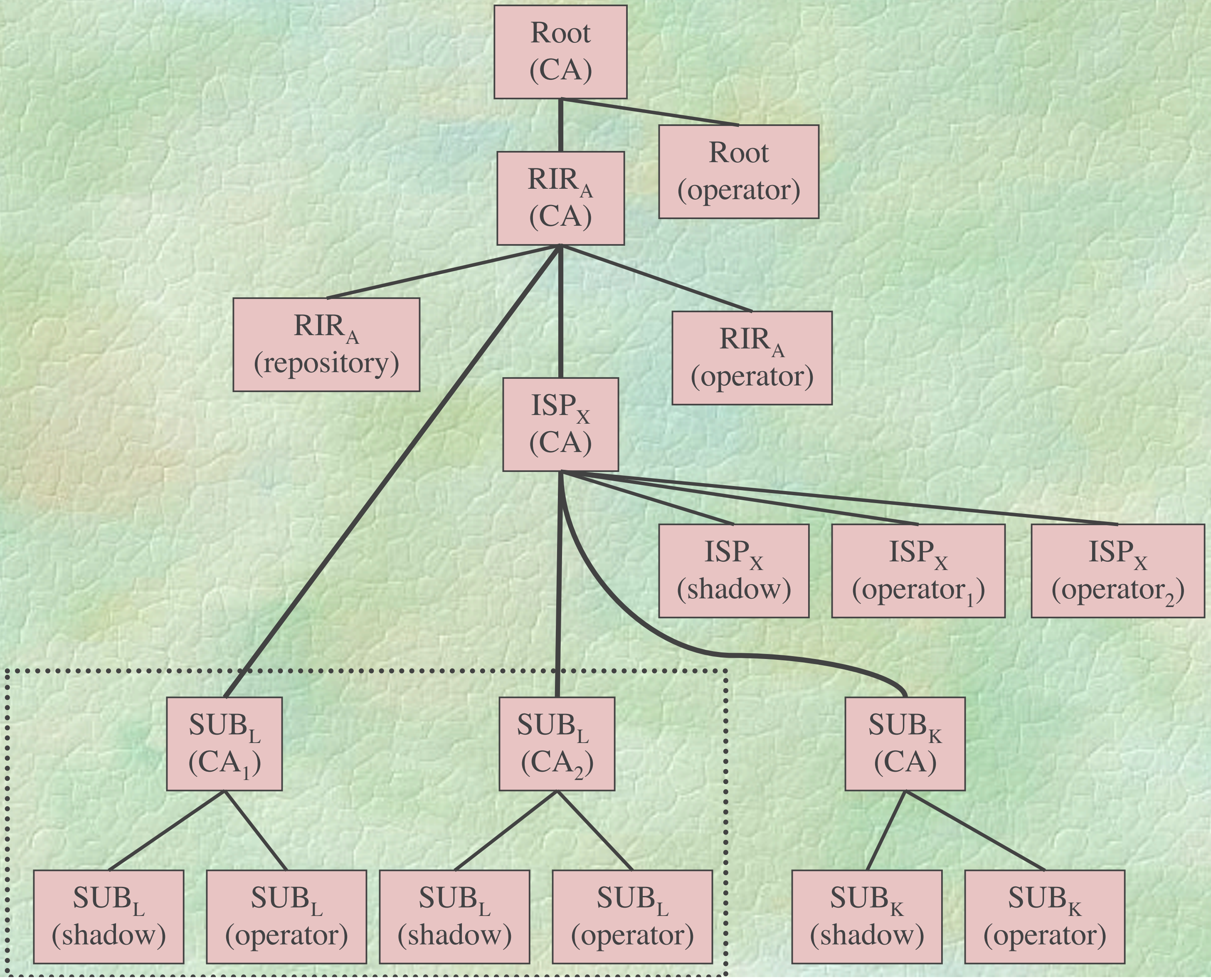
Next hop AS list for ISPs

Back pointer to ROA signer's certificate

Time/date for which the ROA is valid

Digital signature applied by the ROA signer

PKI Example


Root (CA)
Root (operator)
RIR_A (CA)
RIR_A (repository)
RIR_A (operator)
ISP_X (CA)
ISP_X (shadow)
ISP_X ($operator_1$)
ISP_X ($operator_2$)
SUB_L (CA_1)
SUB_L (CA_2)
SUB_K (CA)
SUB_L (shadow)
SUB_L (operator)
SUB_L (shadow)
SUB_L (operator)
SUB_K (shadow)
SUB_K (operator)

Repositories

- Assume a repository model that parallels the whois database system, one repository per RIR
- ISPs & subscribers upload their own new data, download reposiroty changes, on a daily basis
- Each ISP will need to contact each RIR repository to gather all the data need to verify ROAs
- Repositories can use the PKI to enforce access controls to counter DoS attacks
  - Access granted only to PKI users
  - An ISP or subscriber is automatically prevented from overwriting data of another ISP or subscriber

Using the PKI

- Route filter generation procedure
  - Download all the (changed) repository data: certificates, CRLs, and ROAs
  - Verify the certificate paths
  - Use shadow certificates to verify ROAs
  - Construct a table of authorized origin ASes and address prefixes from the ROAs
- Securing route origination requests
  - Subscriber (or downstream ISP) sends a ROA to the ISP that it wants to advertise its prefix, e.g,, via S/MIME
  - ISP verifies the ROA and that the sender is the subscriber in question

Summary

- The proposed PKI provides
  - A more secure basis for route filter generation than IRR data, because of the intrinsic strong authentication, integrity, and authorization controls it provides
  - A foundation for more comprehensive BGP security mechanisms
  - A basis for ISPs to counter social engineering attacks intended to generate bogus routes
- Work is underway to make this PKI a reality
  - Test certificates are being generated
  - A draft CP for the PKI has been written
  - A draft CPS for registries and one for ISPs has been written
  - APNIC is developing software to support the PKI

Questions