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 improve the security of route filter generation
- It also can help ISPs avoid “social engineering” attacks that attempt to trick them into issuing bogus routes

Principles for the PKI

- Use standards
  - X.509 certificates as per IETF PKIX profile
  - RFC 3779 extensions to resource holdings (represent address space and AS numbers)
- No new organizations as CAs
- Support improved security for route filter generation
- Accommodate existing allocation practices
  - Portable allocations from registries
  - Subscriber multi-homing
  - Subscriber moves and takes address space
  - Legacy address allocations
  - Registry transfers
  - …

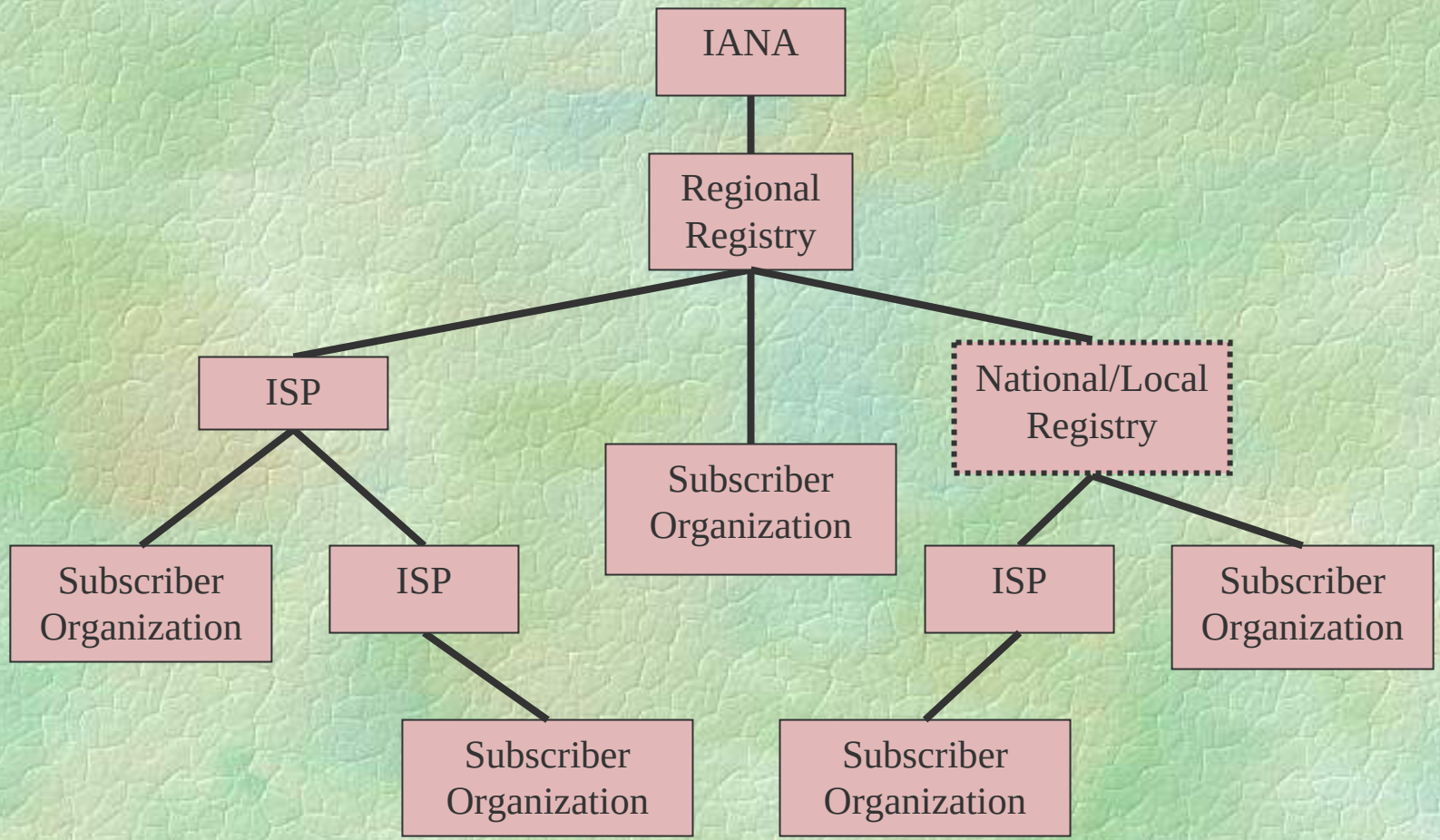
What Does the PKI Look Like?

- The PKI consists of three parts:
  - X.509 certificates that attest to address space and AS number holdings, plus associated CRLs
  - Signed objects that allow a PKI participant to make assertions about its resource holdings
    - Authorizing an ISP to originate routes for prefixes, to advertise a route, etc.
  - A repository system for these certificates, CRLs, and signed objects (not discussed today)
- The PKI makes use of the existing address space and AS number allocation system and the organizations who operate this system

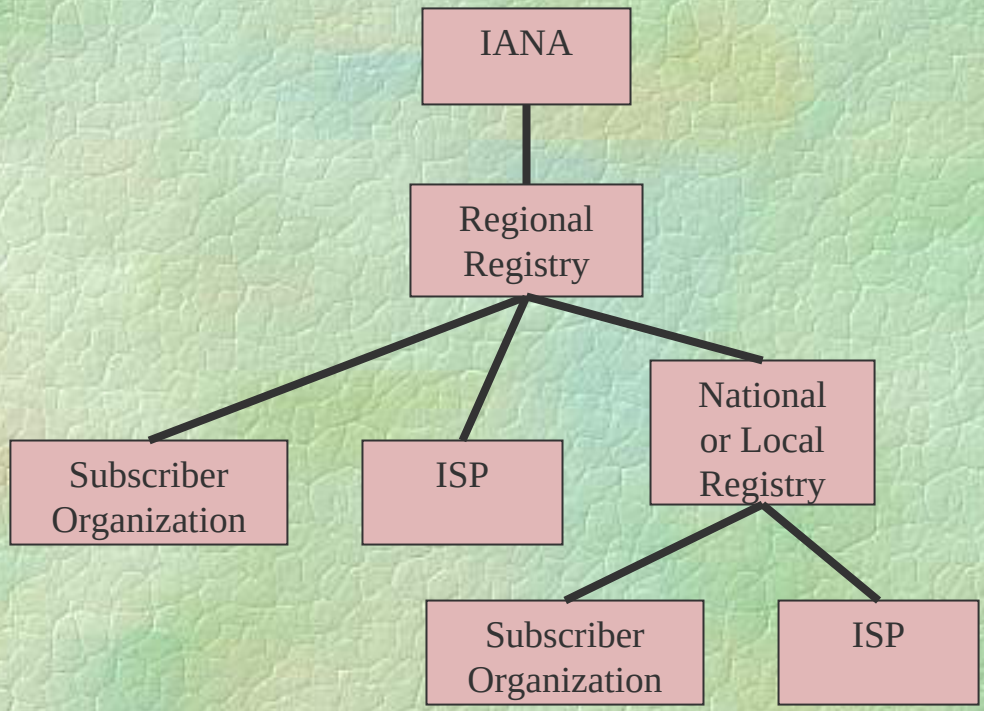
What are we doing with Certificates?

- The intent in this PKI is to issue certificates that attest to resource holdings by registries, ISPs, and subscribers (where appropriate)
- Because the allocation of these resources is done via a simple, hierarchic scheme, the PKI should parallel this scheme
- Each entity that participates in the allocation process should act as a CA, issuing certificates to match the resource allocation records of that entity

Address Allocation Hierarchy



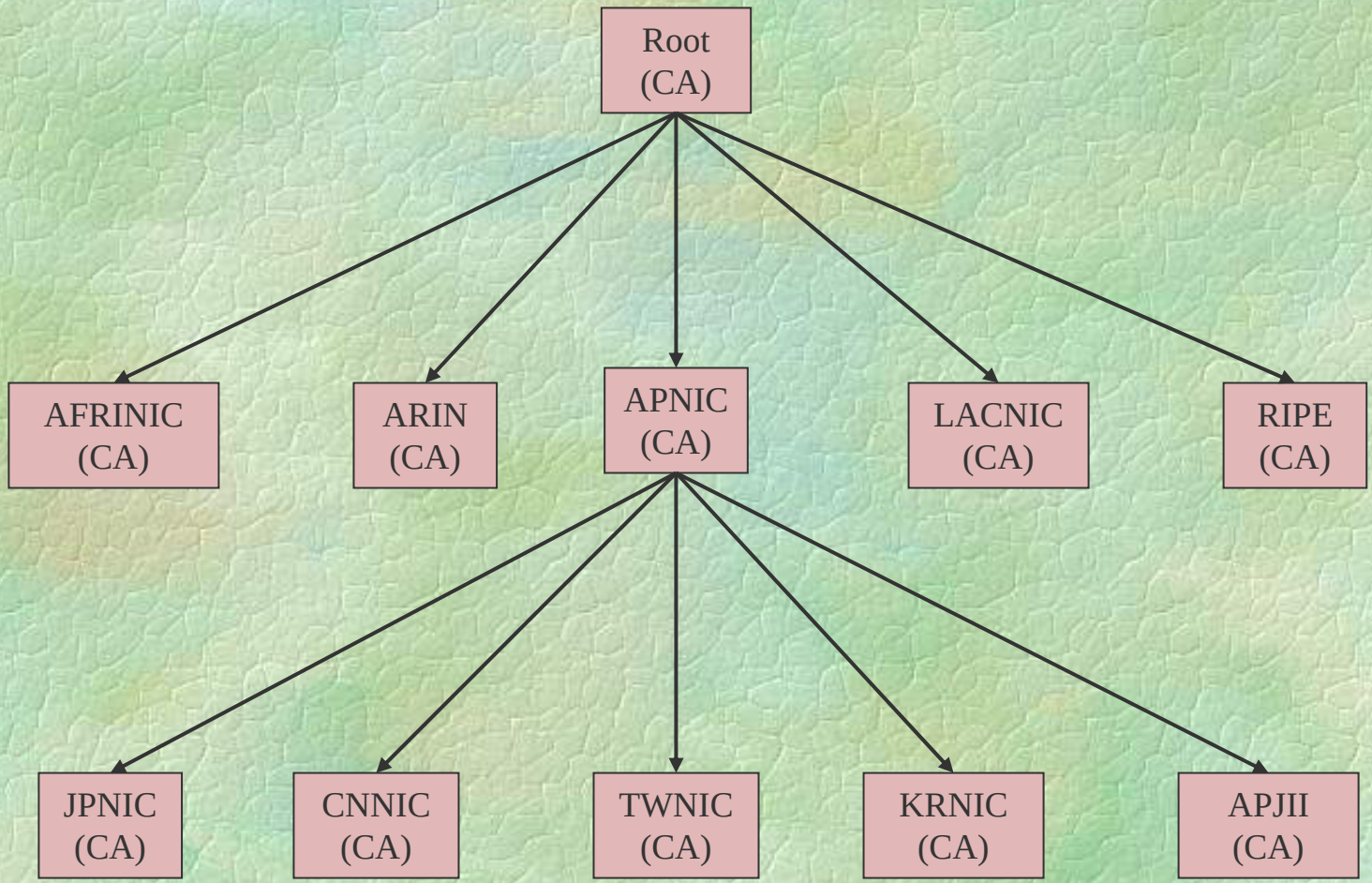
AS Number Assignment Hierarchy



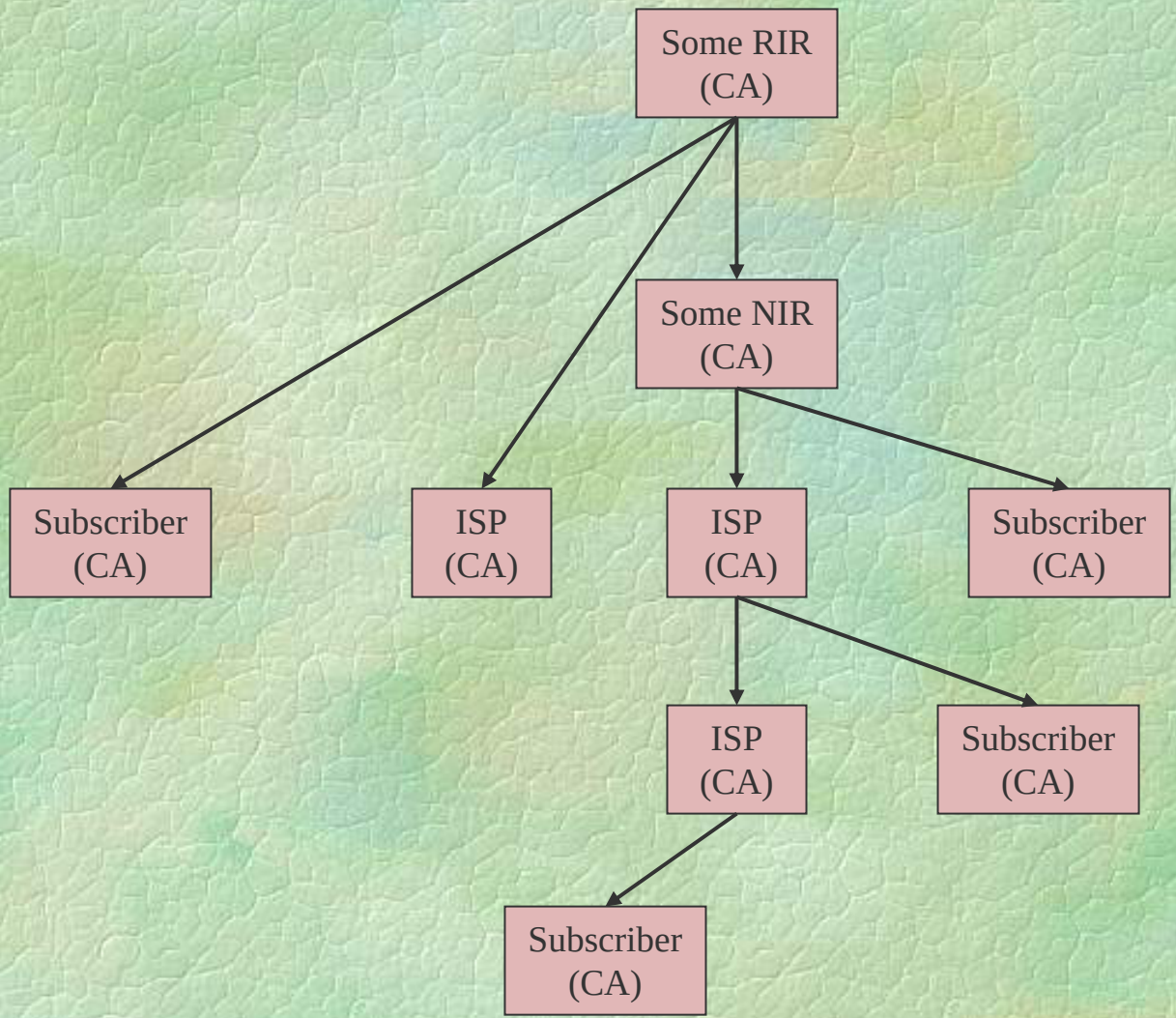
How Will the PKI Work?

- The root issues certificates to the 5 RIRs, and each RIR issues certificates to national/local registries (if applicable) and to ISPs and subscribers
- ISPs issue certificates to downstream providers and to subscribers
- Each organization issues certificates that match the address space (and AS number) allocations it database records
- 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

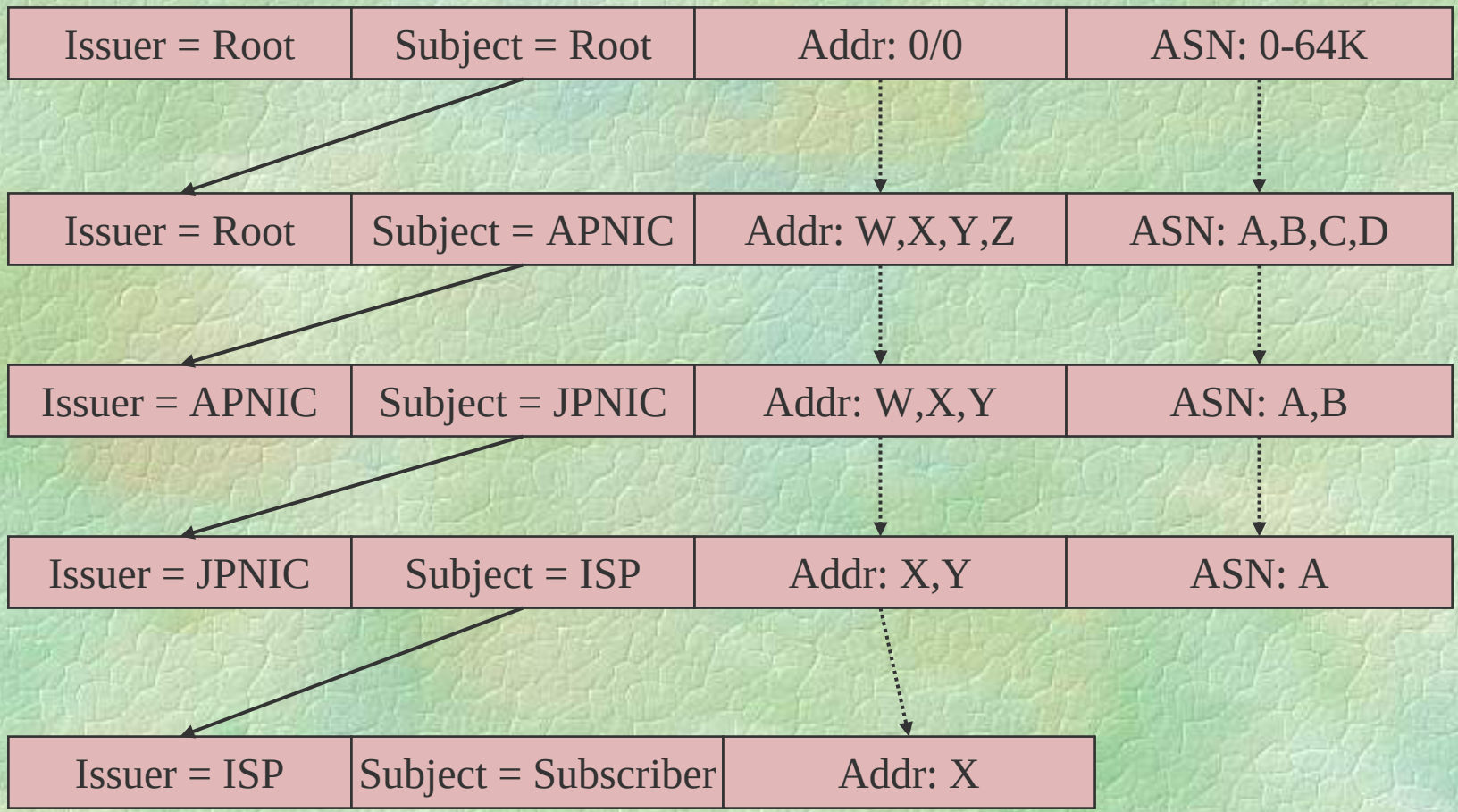
PKI Top Tier Example (APNIC)



PKI Additional Details Example



Certificate Chain Example



Names in Certificates

- Because the intent of the PKI is to enable digital signing of objects that express authorization, is it not necessary for these certificates to contain meaningful names!
- This is a big departure from most PKI designs, but it is appropriate for this context, and it helps avoid liability issues for CAs
- Use meaningful names only for the top tiers (registries)
- Allow CAs to assign non-meaningful names (locally), but also allow a subscriber to request the same name from two CAs (once it has been assigned a name by one of them), to facilitate consolidation of allocations from multiple sources

Some Name Examples

- RIR CA name
  - C = AU, O = APNIC, OU = Resource Registry CA
- NIR CA name
  - C= JP, O = JPNIC, OU = Resource Registry CA
- ISP or subscriber CA name
  - CN = FC3209809268

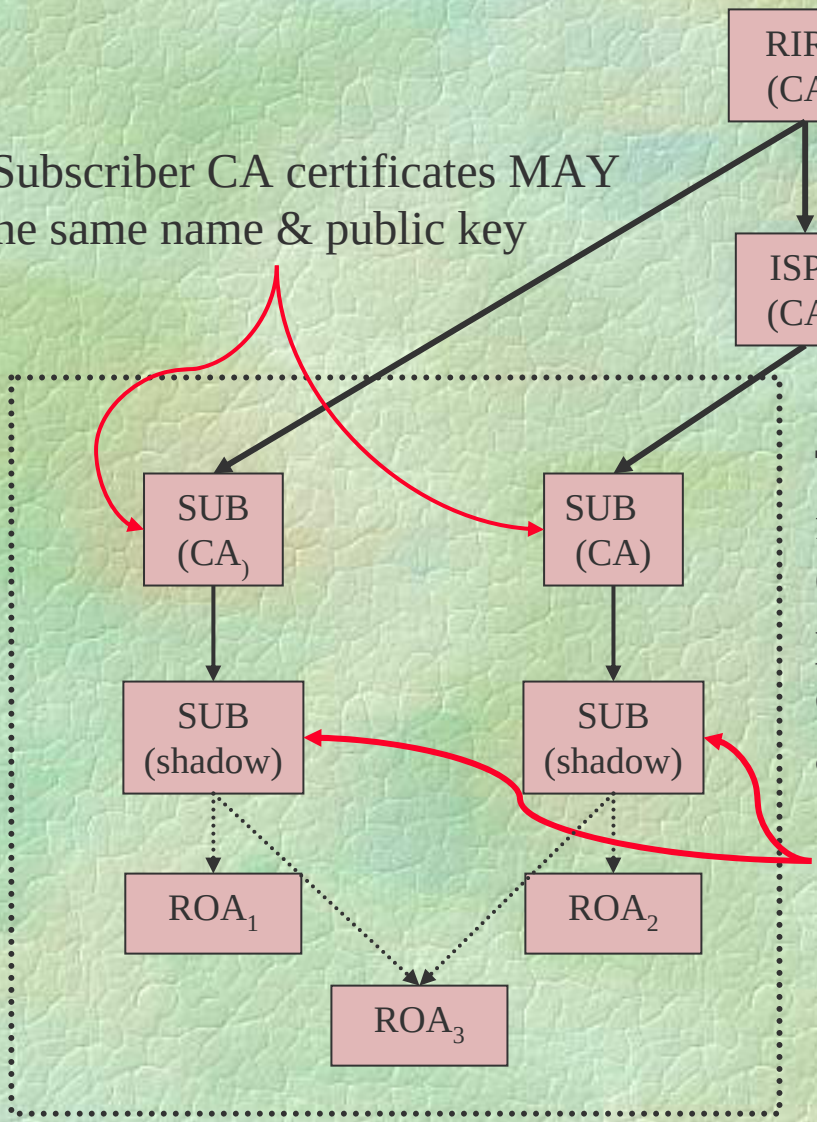
Adding Resources

- If a resource holder acquires additional resources from the same source (e.g., registry) then that source can issue a new certificate reflecting these additional resources
  - The new certificate can replace the old one and add in the new allocations, or
  - The new certificate can be distinct from the old certificate, and contain just the new allocation
  - Note: there is no need to change the public key in the certificate, and no need to revoke the old certificate if resources are ADDED
- Also, AS numbers can be put in separate certificates from addresses if the subject desires

Multiple Allocation Sources

- If a subject acquires resources from multiple sources, it needs multiple certificates, to reflect the different sources
- Each certificate should MAY the same subject name and MAY use the same public key, if the subscriber wants to bundle these allocations, OR each certificate may use a different name and a different public key
- If the subscriber wants certificates with the same name, it MUST demonstrate that the name has been assigned by another registry or ISP when requesting a new certificate from a different source

Multi-source Allocations



The Subscriber CA certificates MAY use the same name & public key

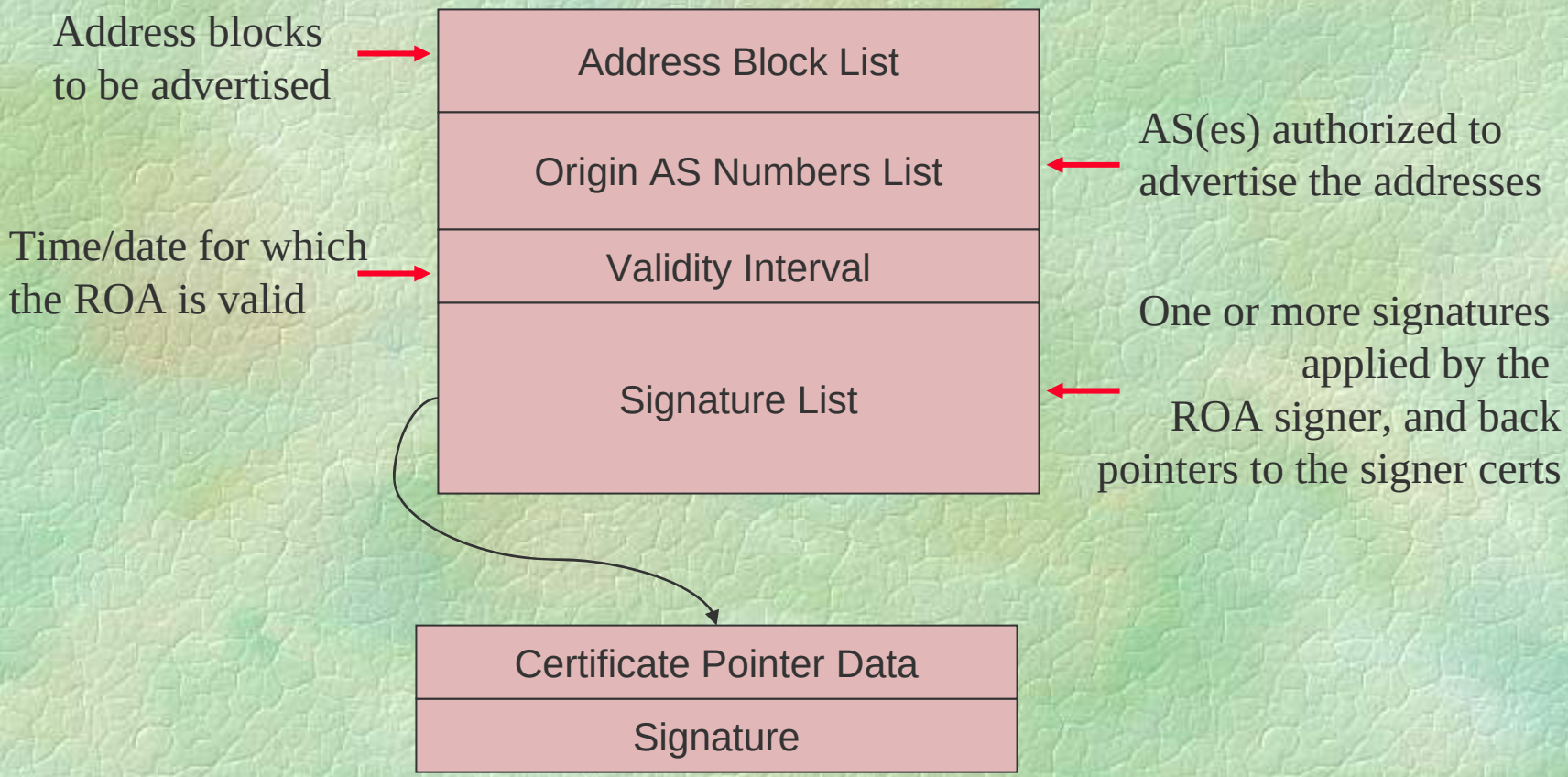
This subscriber has allocations of addresses from ISP$_X$ and from RIR$_A$. It needs two CA certificates to preserve the subset property, and must issue separate shadow certificates to sign ROAs for each allocation.

The Subscriber shadow certificates MAY use the same name and public key

Route Origination Security

- One PKI goal is to enable verification of route origination by ISPs
- To support this goal, each address space holder needs to digitally sign an object enumerating the AS(es) authorized to advertise routes on behalf of the address space holder
- We call the object a route origination authorization (ROA)
- An address space holder issues one ROA if it wants all of its ISPs to advertise the same set of prefixes
- If an address space holder wants different ISPs to advertise different sets of prefixes, then the holder issues multiple ROAs, one for each set of prefixes to be originated separately
- Since each ISP is an address space holder, it would sign a ROA authorizing itself to advertise the addresses it holds

ROA Format


Address blocks to be advertised
Address Block List
Origin AS Numbers List
AS(es) authorized to advertise the addresses
Time/date for which the ROA is valid
Validity Interval
Signature List
One or more signatures applied by the ROA signer, and back pointers to the signer certs
Certificate Pointer Data
Signature

Using the PKI (I)

- Simple route filter generation
  - Download 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 validated 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
  - ISP can now accept request from user with confidence

Using the PKI (II)

- More ambitious route filtering
  - An ISP can generate a signed object that authorizes a neighbor to advertise a route
  - The object would include the AS number(s) of the neighbor, the AS number(s) of the signer, and the prefixes to be advertised
  - The object also would contain previous instances of objects of this sort, to form a chain of signed authorizations, paralleling the route being advertised
  - These objects could be distributed via an IRR, or just passed around privately among ISPs, …

Summary

- The proposed PKI provides
  - A more secure basis for route filter generation than current IRR data, because of the intrinsic strong authentication, integrity, and authorization controls the PKI provides
  - A foundation for more comprehensive BGP security mechanisms
  - A basis for ISPs to counter social engineering attacks intended to can them to originate 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

Contemplation?