A PKI for IP Address Space and AS Numbers

Dr. Stephen Kent

Chief Scientist - Information Security

BBN
TECHNOLOGIES

Presentation Outline

- Why a PKI?
- Very brief PKI background
- Address & AS number allocation system
- The proposed PKI
- Procedures
  - Initial certificate request, renewal, revocation
  - Requesting route origination
  - Authorizing route origination
  - Multi-homing
  - Address space transfer

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

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
  - …

PKI Terminology

- Certificate: a digitally-signed data structure; typically an X.509 public key certificate (PKC), the certificate standard adopted by the IETF and employed in SSL/TLS, IPsec (IKE), S/MIME, and many other security protocol standards
- Certification Authority (CA): an entity that issues (signs) certificates, aka an Issuer
- Subject: an entity to whom a certificate is issued; for a PKC, the subject is the holder of the private key corresponding to the public key in the certificate
- End entity (EE): a certificate subject that does not issue certificates, i.e., does not act as a CA
- Relying party (RP): an individual or organization that takes actions based on using a public key from a certificate

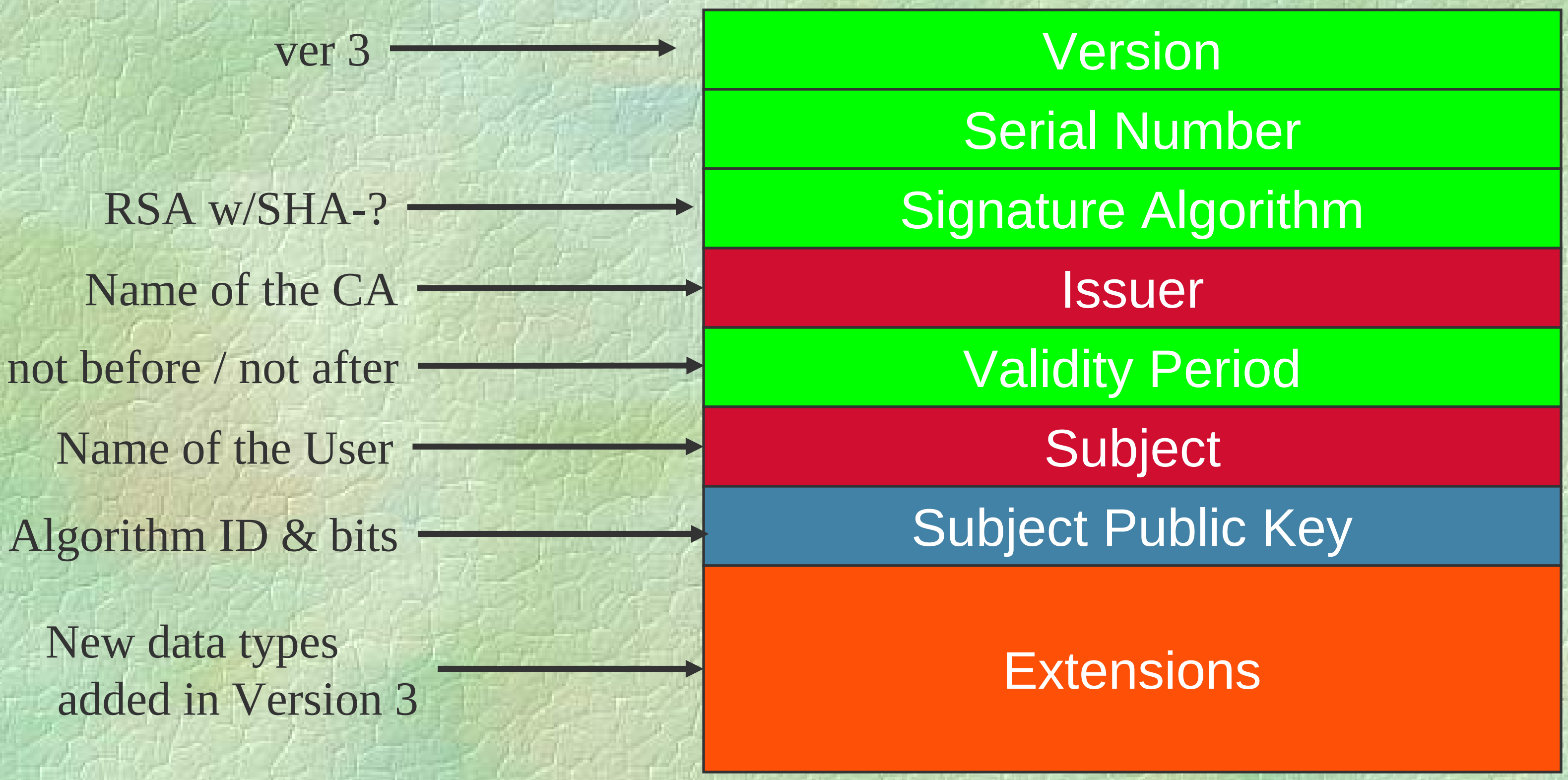
More PKI Terminology

- Trust anchor (aka root): a public key and associated data used as a reference for validating certificates
  - A trust anchor is often represented as a self-signed certificate, but it need not be
- Certification path: a series of certificates between a trust anchor and a certificate being validated, linked by subject/issuer name
- Certificate validation: the process of determining that a certificate is valid
  - creating a certificate path between a certificate and a trust anchor
  - verifying the signature on each certificate in the path
  - checking the revocation status of each certificate in the path
- PKI: a set of procedures, policies, and technical measures employed to manage (issue, renew, revoke, publish) certificates

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 certificates and CRLs (and for ROAs and similar signed objects)
- The PKI makes use of the existing address space and AS number allocation system
- This PKI also embodies the “principle of least privilege” that Russ cited earlier

X.509 Certificate (v3)



ver 3 → Version

Serial Number

RSA w/SHA-? → Signature Algorithm

Name of the CA → Issuer

not before / not after → Validity Period

Name of the User → Subject

Algorithm ID & bits → Subject Public Key

New data types
added in Version 3 → Extensions

Certificate Extensions for the PKI

- **Basic Constraints**
  - Marks the certificate as for a CA (vs. an EE)
- **Certificate Policy**
  - Marks the certificate as being restricted to use with this PKI
- **Key Usage**
  - Says how the public key may be used, e.g., certificate/CRL validation vs. more general signed data validation
- **Key Identifiers**
  - Subject and Issuer identifiers, based on public key hash values, optionally used to assist in selecting the right CA certificate when there are multiple CA certificates with the same name
- **Address space & AS Number (RFC 3779)**
  - one extension represents a list of address ranges
  - the other extension represents a list of AS number ranges

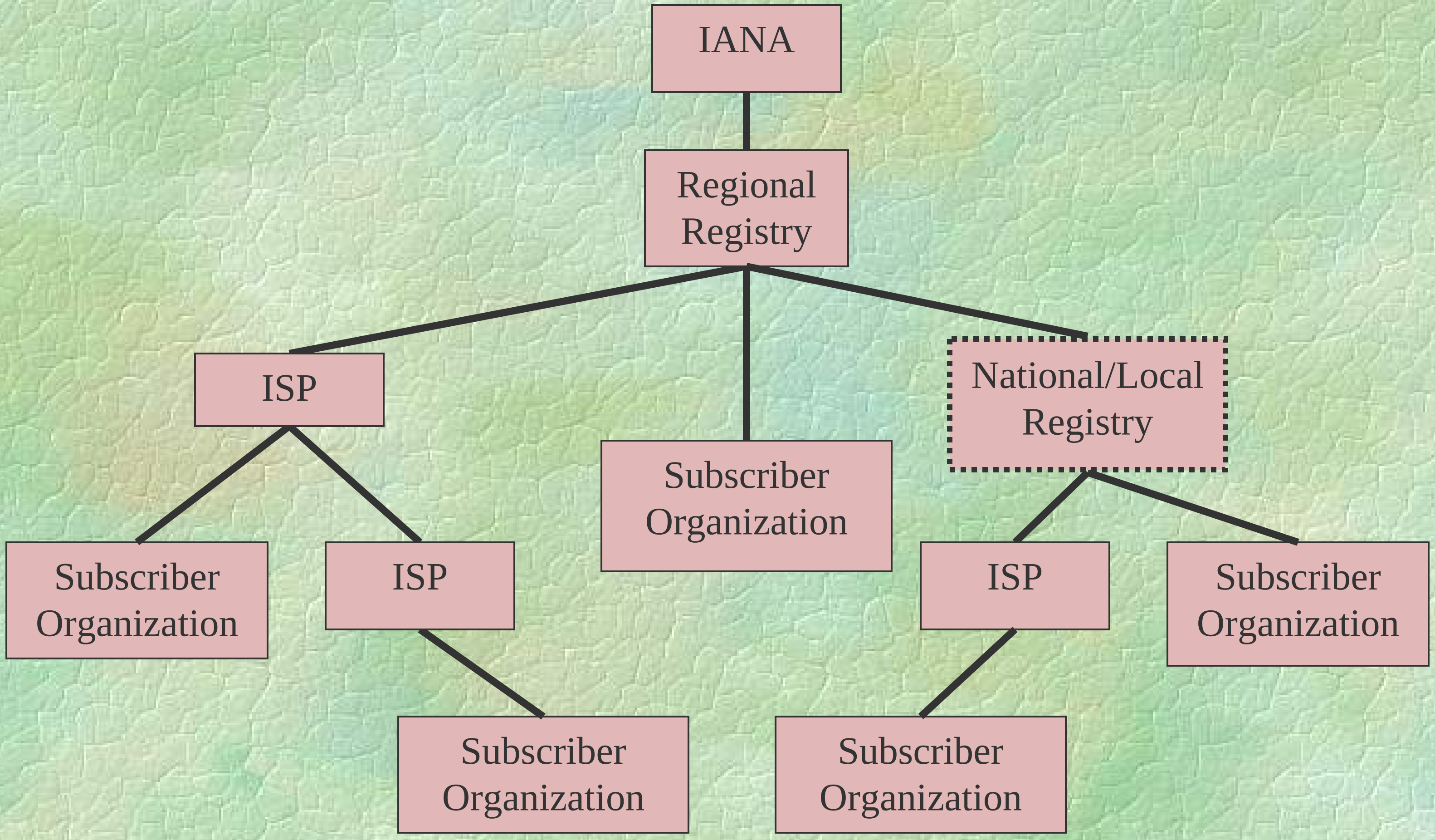
Certificate Extensions for the PKI ?

- **Subject Alternative Name**
  - An extension that allows another name to be associated with the Subject, e.g., DN, a DNS name, or e-mail address
- **Authority Info Access**
  - A pointer to where to find the CA certificate, if the repository system is very distributed
- **CRL Distribution Point**
  - A pointer to the CRL for this certificate, if the repository system is very distributed

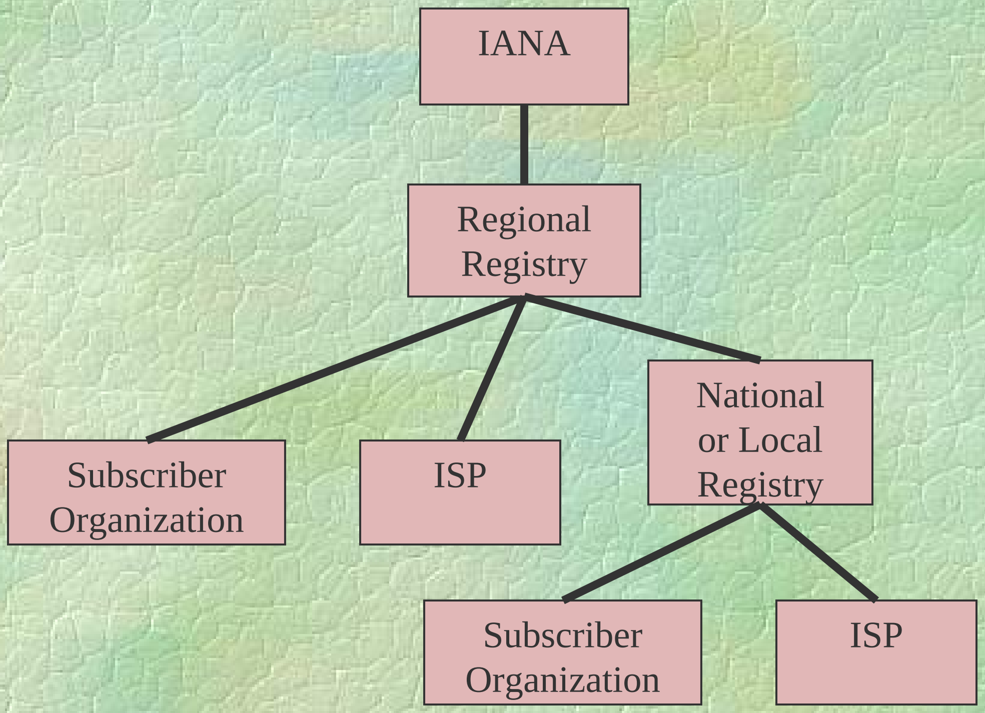
What are we doing with Certificates?

- 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



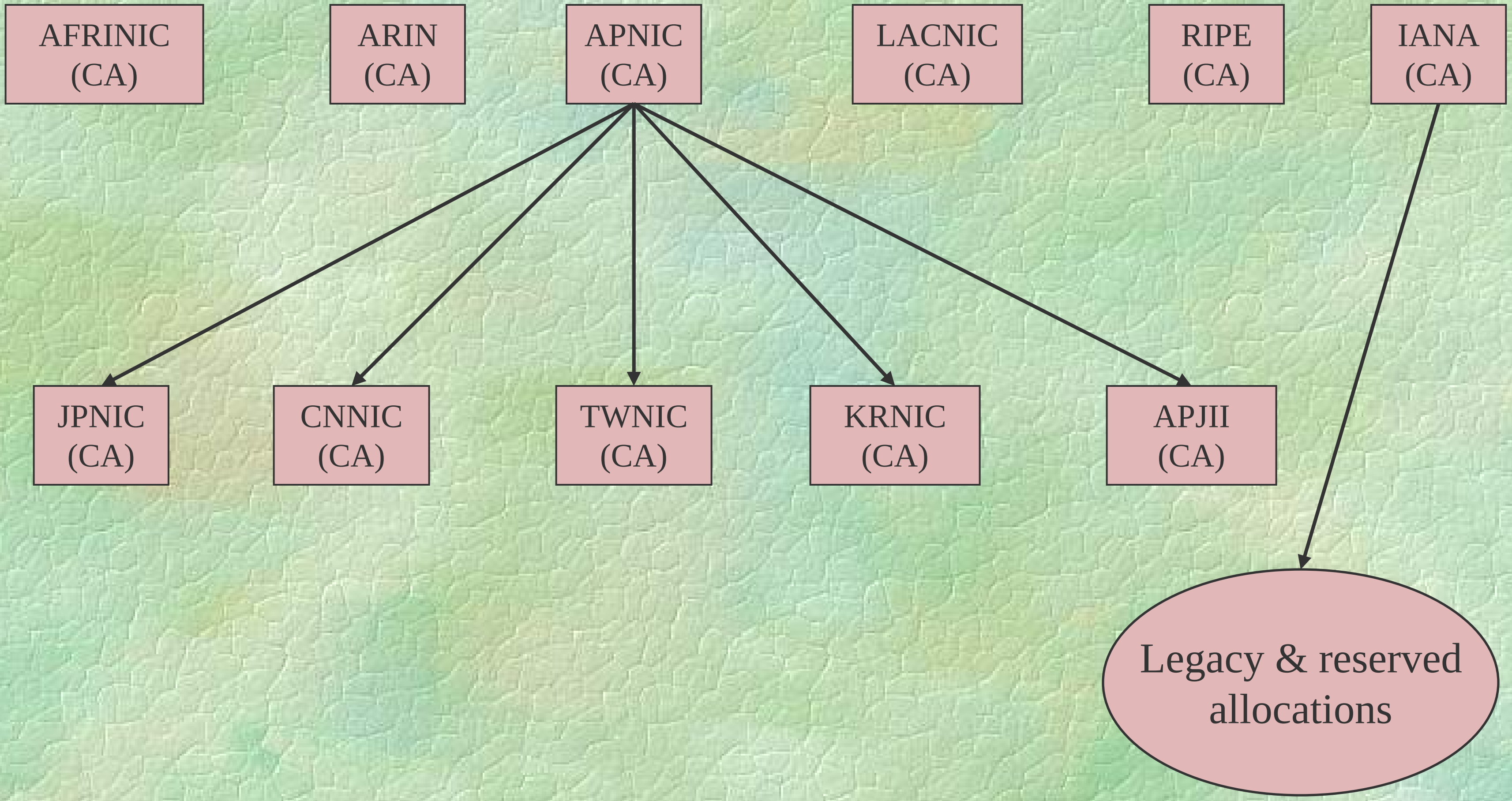
AS Number Assignment Hierarchy



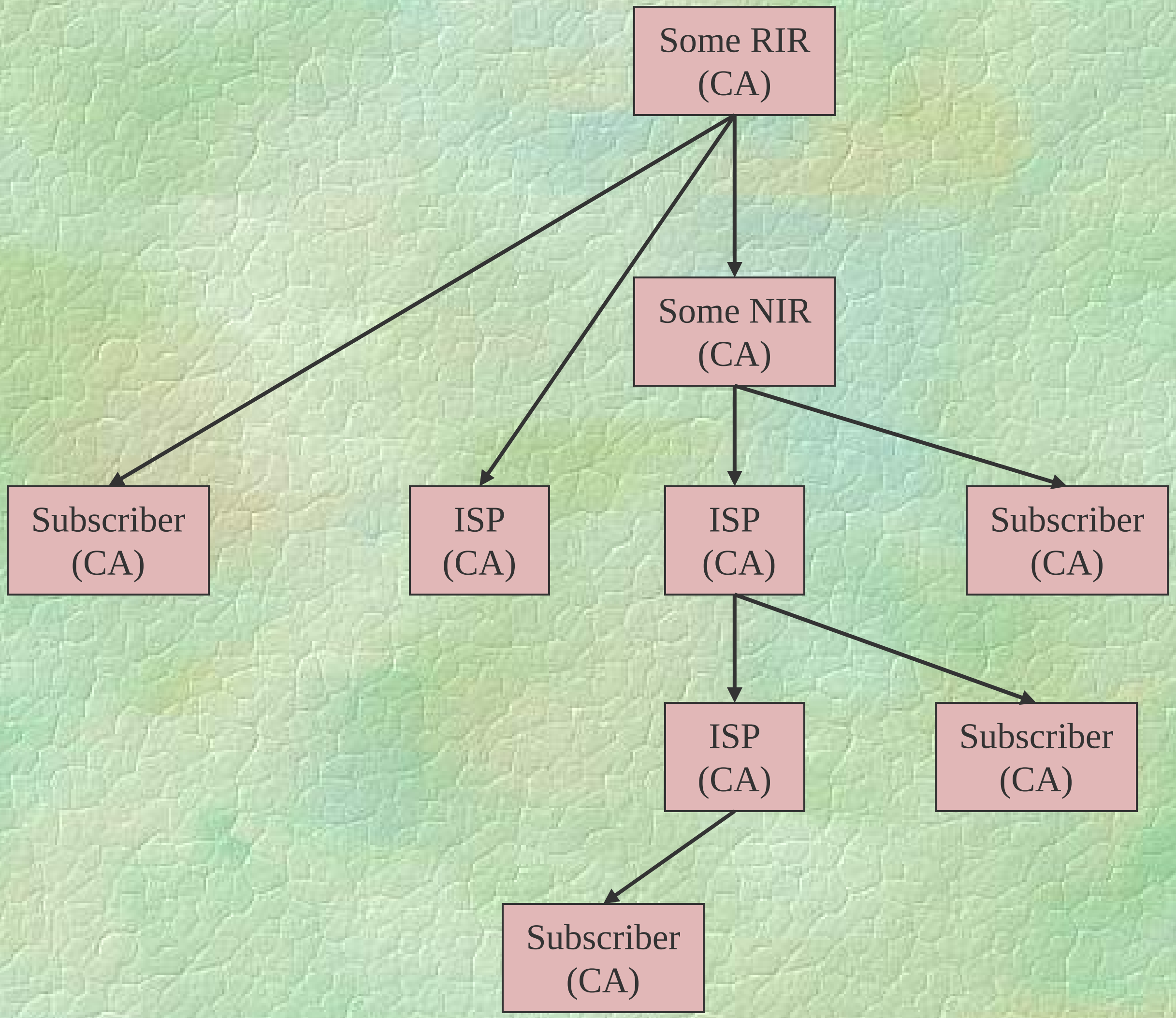
How Will the PKI Work?

- The 5 RIRs and IANA act as roots for the system
- 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 in its database records
- All resource holders are certification authorities (CAs)
- Address and AS number data represented via RFC 3779
- Each certificate path represents sub-allocation by the organizations noted above, a subset constraint that can be verified by ISPs downloading these certificates

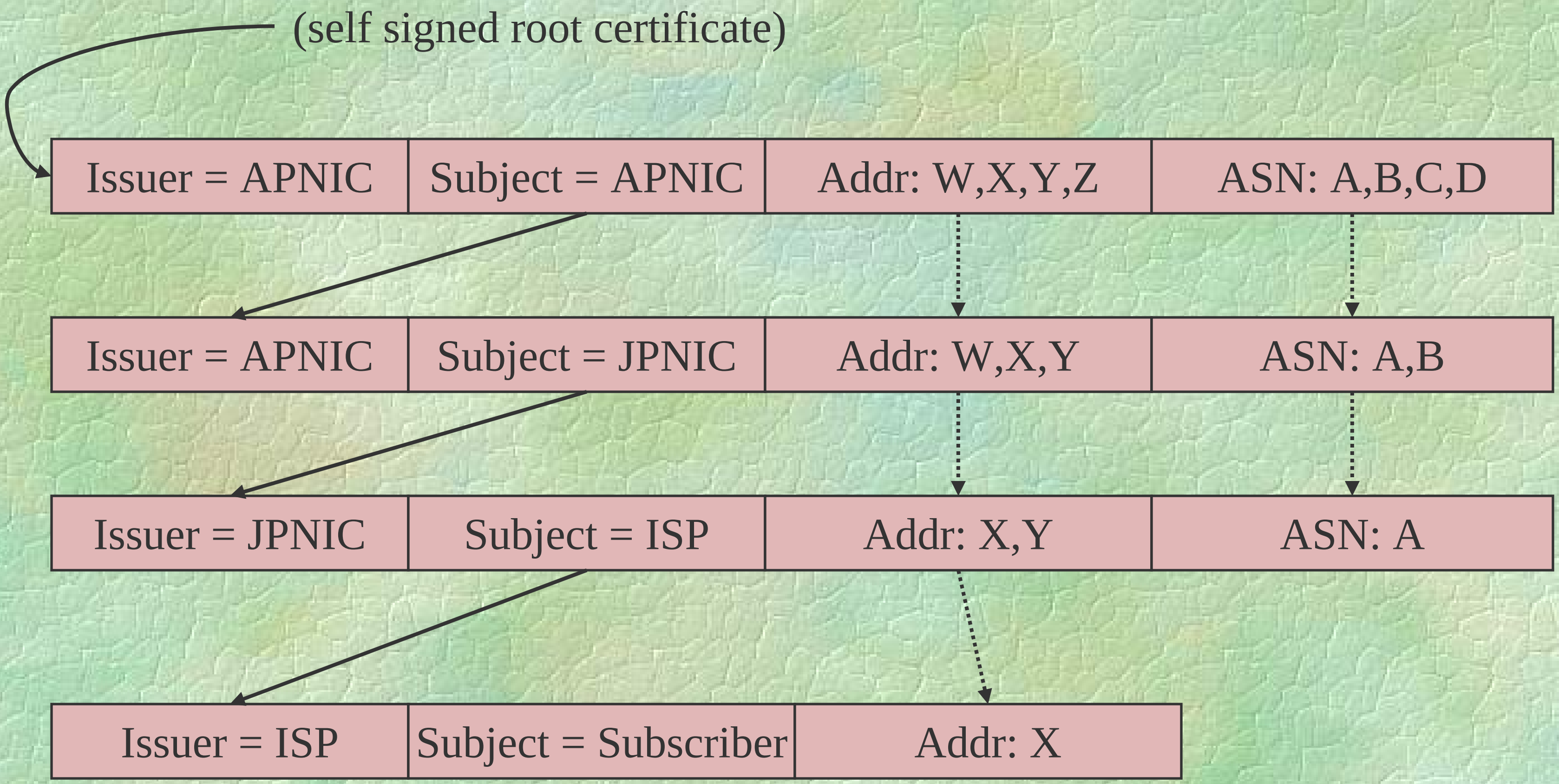
PKI Top Tier Example (APNIC)



PKI Vertical Slice Example



Certificate Chain Example



(self signed root certificate)

Issuer = APNIC	Subject = APNIC	Addr: W,X,Y,Z	ASN: A,B,C,D
Issuer = APNIC	Subject = JPNIC	Addr: W,X,Y	ASN: A,B
Issuer = JPNIC	Subject = ISP	Addr: X,Y	ASN: A
Issuer = ISP	Subject = Subscriber	Addr: X	

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
- Meaningful names only for the top tiers (registries & IANA)
- 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

Certificate Request Procedure (1/2)

- An ISP (or subscriber) contacts an RIR to request a certificate for its resource allocation from that RIR
  - The RIR could issue one certificate for ALL the ISP resources OR split the resources across multiple certificates if requested
- The RIR verifies that it is communicating with the ISP in question, based on the RIR’s database and whatever technical security means it employs
- The ISP generates a key pair, and sends the public key to the RIR via an integrity-secure channel
- The RIR issues a certificate to the ISP, containing:
  - The ISP’s public key
  - A name generated by the RIR, unique to the RIR’s space
  - An RFC 3779 extension listing the ISP’s address allocations

Certificate Request Procedure (2/2)

- The same procedure applies to
  - an ISP or subscriber requesting an address space certificate from an NIR/LIR
  - an ISP or subscriber requesting an address space certificate from an ISP
  - an ISP or subscriber requesting a certificate for his AS number holdings
- The certificate duration would typically be tied to the contract with the registry or ISP, plus a grace period

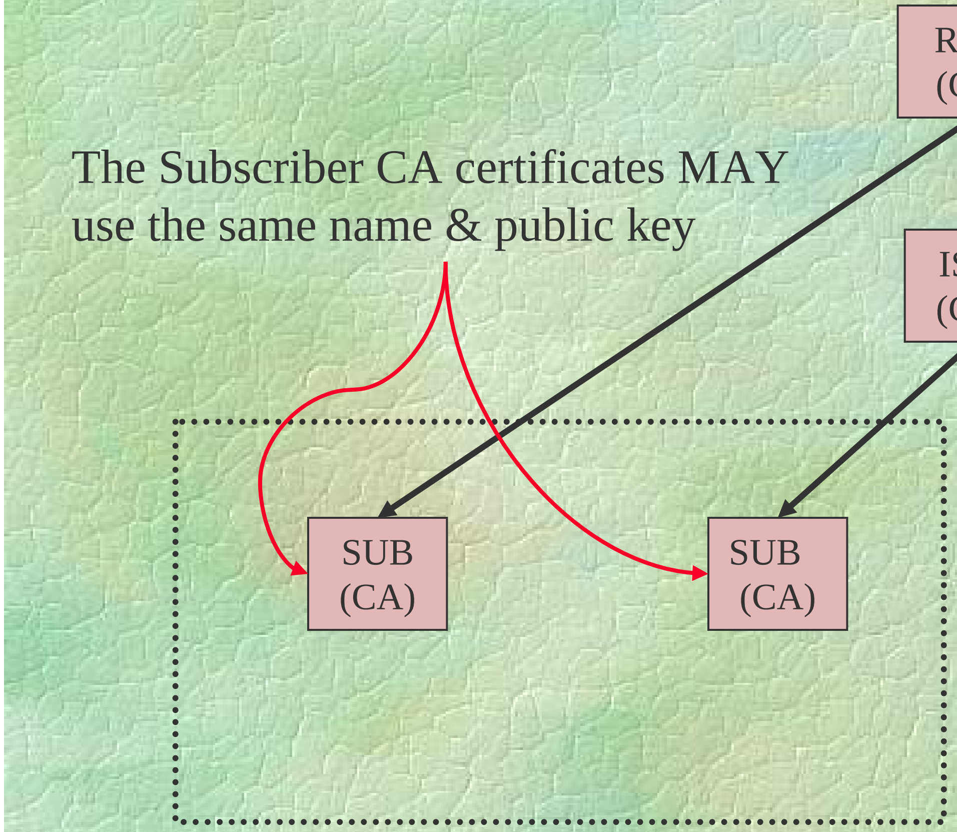
Adding Resources

- If a resource holder acquires additional resources from the same source (e.g., a registry) then that source can issue a new certificate reflecting these additional resources
  - The resource holder requests the additional resources, and indicates that it wants them added to its current certificate
  - The registry will start with the current resource holder certificate, modify the RFC 3779 extension(s) to reflect the additional resources, assign a new serial number, update the validity interval, and sign the new certificate
  - 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
- Or, if the subject desires, he can get a new certificate with just the new allocation in it

Multiple Allocation Sources

- If a subscriber (or ISP) acquires resources from multiple sources, he needs multiple certificates, to reflect the different sources
- Each certificate may use 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 public key
- If the subscriber wants certificates with the same name, he 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


RIR$_A$
(CA)
The Subscriber CA certificates MAY use the same name & public key
ISP$_X$
(CA)
SUB
(CA)
SUB
(CA)

This subscriber has allocations of addresses from ISP$_X$ and from RIR$_A$. He needs two CA certificates to preserve the subset Property, but both certificates can carry the same CA name. It is not uncommon for a CA to have multiple certificates issued to it by other CAs

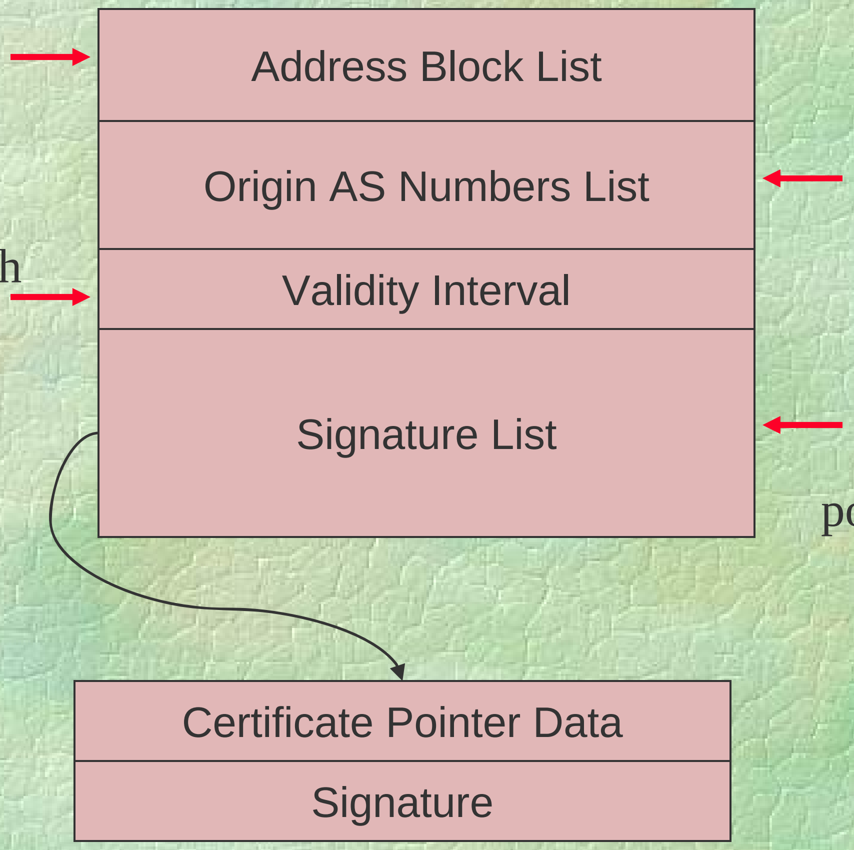
Route Origination Security

- One PKI goal is to enable ISPs to verify of route origination
- 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 he wants all of his 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 Composition

- **Address prefixes**: one of more prefixes, corresponding to the NLRI that the ROA signer authorizes for origination by one or more ISPs, enumerated below
- **AS numbers**: the ISP(s) authorized to originate routes to the above list of prefixes
- **Validity Interval**: start and end time & date defining the interval for which the ROA is valid
- **Signature List**: a set of pairs of data used to verify the ROA
  - Certificate pointer: data to help a verifier locate a shadow certificate needed to verify this signature on the ROA
  - Signature: digitally signed hash of the above data, plus an indication of the hash algorithm and digital signature algorithm employed

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

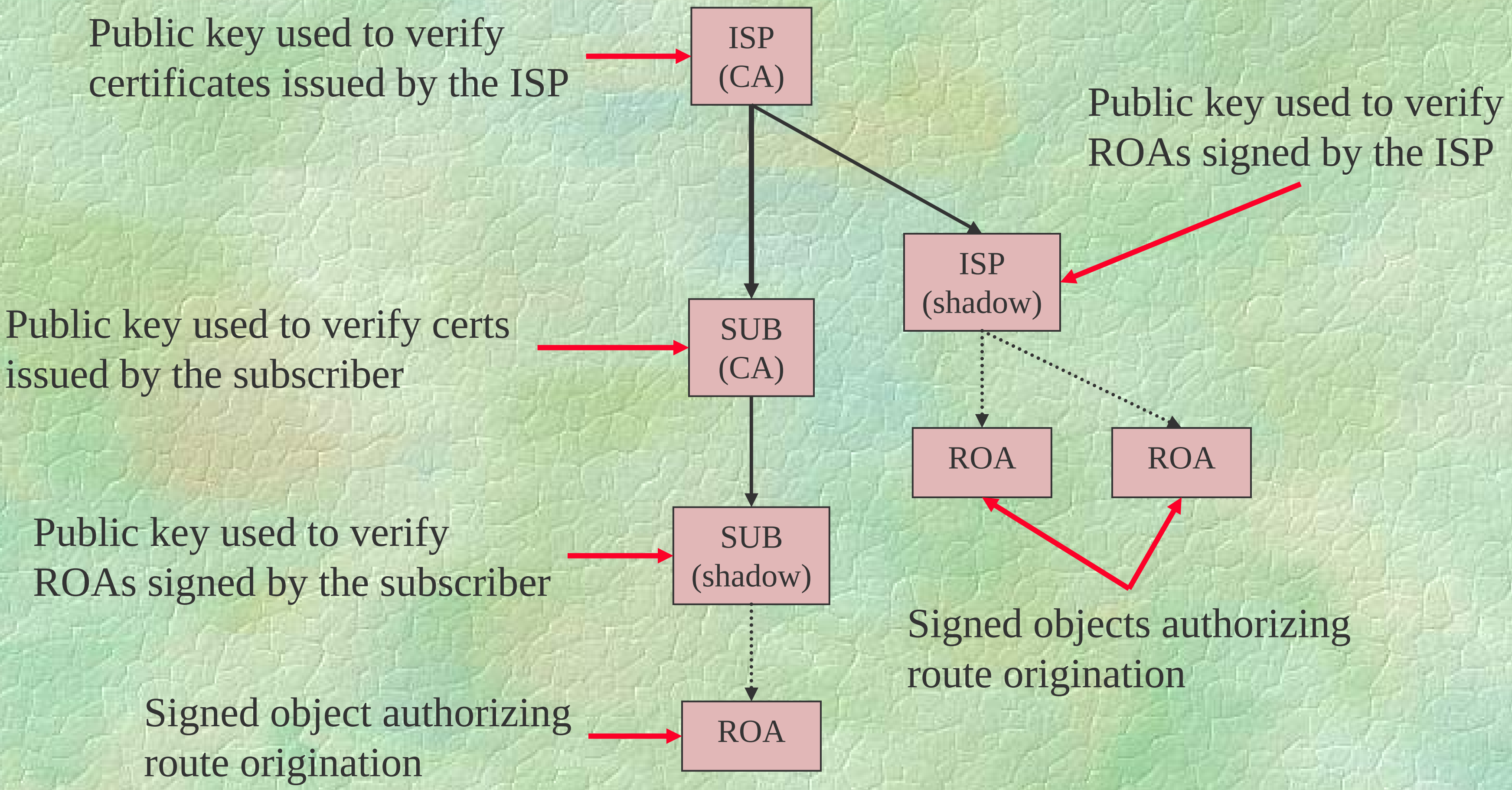
Certificate Pointer Data

Signature

PKI Details re ROAs

- Each entity in the PKI is represented as a CA, so that it can issue certificates to reflect sub-allocation
- Good PKI practice says that a CA should NOT sign objects other than certificates and CRLs
- So, we introduce an end-entity (EE) certificate under each ISP & each subscriber CA, and use the corresponding private key to sign ROAs (ISPs and some subscribers sign ROAs, but registries don’t)
- We call this a “shadow” certificate
- This indirection helps manage ROA revocation, i.e., to revoke a ROA before it expires, a resource holder revokes the shadow certificate (issue a CRL with that certificate)

PKI with Shadow Certificates



Public key used to verify certificates issued by the ISP

ISP (CA)

Public key used to verify ROAs signed by the ISP

ISP (shadow)

Public key used to verify certs issued by the subscriber

SUB (CA)

ROA

ROA

Public key used to verify ROAs signed by the subscriber

SUB (shadow)

Signed objects authorizing route origination

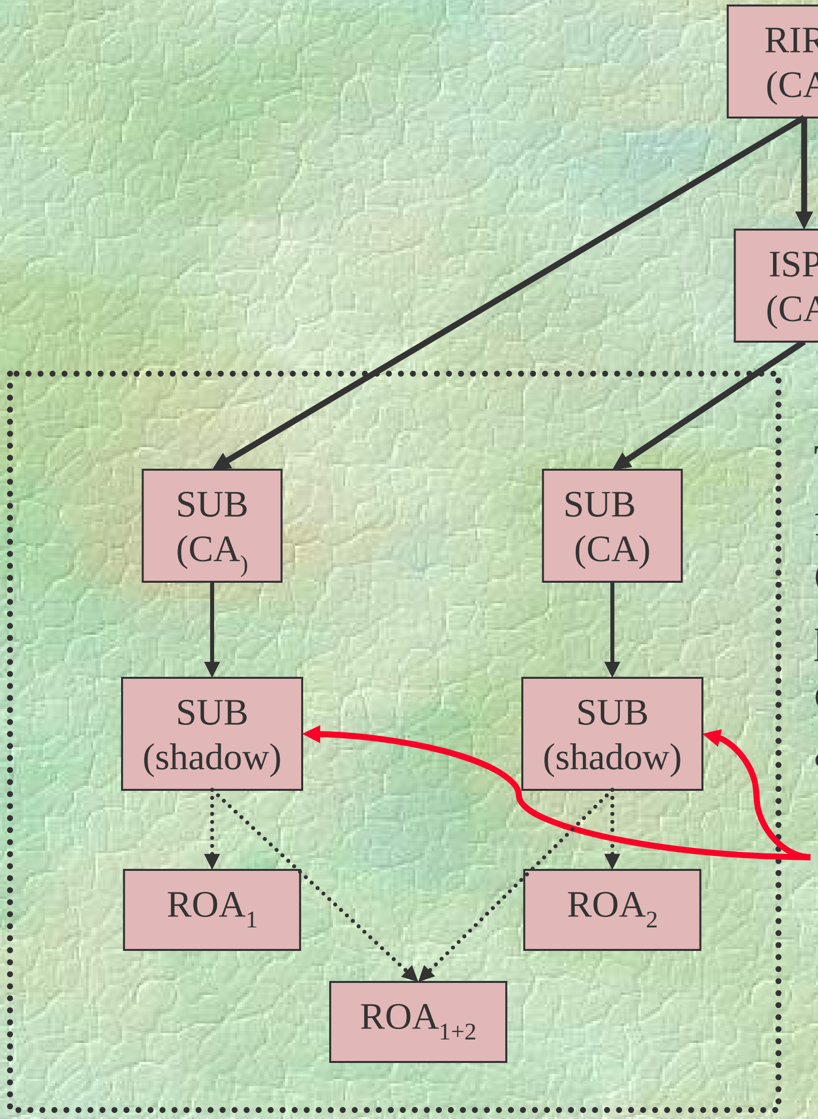
Signed object authorizing route origination

ROA

Generating a ROA

- An ISP (or subscriber) generates one ROA for each set of addresses for which it wants to authorize route origination
  - If all prefixes of the resource holder are to be advertised by the same ISPs, and came from one source, then the entity signs one ROA with all the prefixes and all the AS numbers of the holder
  - If the resource holder wants to authorize some ISPs to originate some prefixes, and other ISPs to originate other prefixes, the holder signs one ROA for each set of addresses to be independently originated
  - If a resource holder has addresses from different sources, it must generate a separate ROA to accommodate each source, even if the same ISPs will appear in each ROA

Multi-source Allocations & ROAs



This subscriber has allocations of addresses from ISP$_X$ and from RIR$_A$. He 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

Single-homed to Multi-homed

- If a subscriber has an address from his ISP, and is connected ONLY to that ISP, the subscriber does NOT need a certificate and does NOT sign a ROA
- If the subscriber wants to be dual-homed, THEN he needs a certificate, so that he can sign a ROA naming both the current and the new ISPs as authorized originators of his address space
- After he gets a certificate from his current ISP
  - Generate an EE (shadow) certificate
  - Sign a ROA naming both ISPs
  - Provide ROA to both ISPs, as part of convincing them to advertise the allocation
  - Public the certificate, CRL, and ROA in the repository

Subscriber Move

- If a subscriber has an address allocation from an ISP, AND he wants to move to a new ISP, AND he wants to keep his current address space, THEN he needs to
  - Get a certificate from his current ISP
  - Generate an EE (shadow) certificate
  - Generate and sign a ROA for his new ISP
  - Provide ROA to his new ISP, as part of convincing it to advertise the allocation
  - Publish the certificate, CRL, and ROA in the repository
- Is it OK to have the certificate from the old ISP be in the path for the subscriber, forever, or should there be a transfer of the resource through the issuing registry?

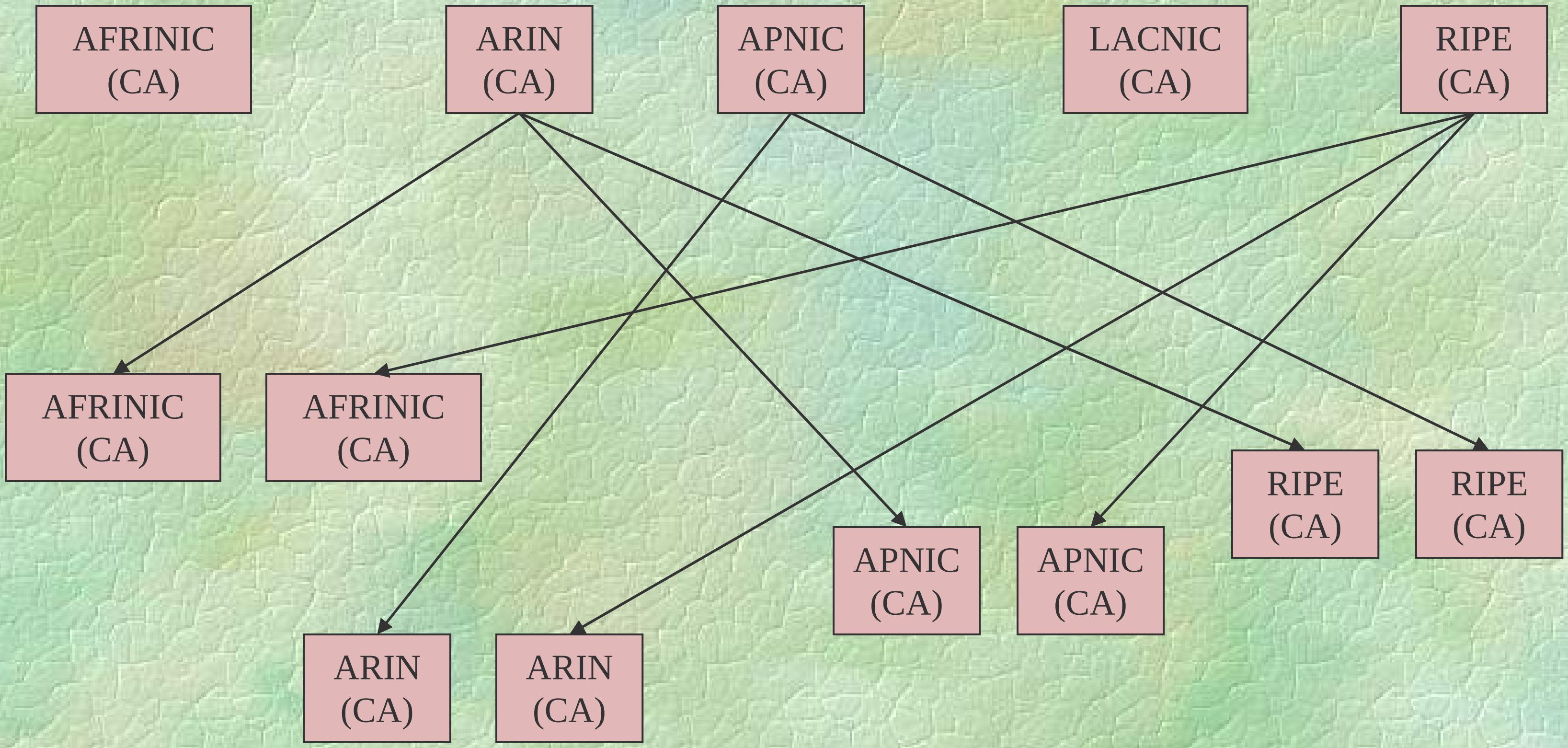
Subscriber with Portable Allocation

- A subscriber may acquire an address allocation from a registry
- The registry will issue a certificate to the subscriber as discussed earlier
- The subscriber must
  - Generate an EE (shadow) certificate under its CA
  - Sign a ROA naming one of more ISPs as authorized to originate routes to the prefix
  - Publish his certificate, CRL, and ROA
  - Communicate the ROA to the ISP(s) in question, to convince them to advertise the prefix for this subscriber

Registry Transfers

- One RIR transfers addresses to another by issuing a cross-certificate to the other RIR
- But, to preserve the subset property demanded by RFC 3779, the target RIR certificate MUST NOT contain the IANA-allocation
- So, each RIR may need as many as 4 additional certificates to accommodate transfers from the other RIRs
- These other certificates are NOT trust anchors; each is reached via a cross-certificate from another RIR

PKI with (some) Cross Certificates



Repositories

- We prefer a model with one repository per RIR (and IANA)
- ISPs & subscribers upload their own new data, download repository 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

Uploading Certificates, CRL, & ROAs

- A resource holder needs to upload changed certificates, CRLs, and ROAs to the repository
  - Certificates will usually change infrequently, only when new allocations are received
  - The ISP decides how frequently to issue its CRLs
  - ROAs change only when allocation change, or when origination authorization changes
- Uploading requires SSL-authenticated login, using a certificate issued under the resource holder's CA
- Repository verifies the authority of the uploader, e.g., using an EE certificate held by NOC staff

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

Questions?