PKI-An Operational Perspective

NANOG 38 ARIN XVIII

October 10, 2006

Briefing Contents

- PKI Usage
  - Benefits
  - Constituency Acceptance
  - Specific Discussion of Requirements
- Certificate Policy
- Certificate Policy Framework
  - Policy and Cost Consideration
  - Algorithms and Key Sizes
  - Sample “Overview”

- Roles and Responsibilities
  - Certification Authorities (CAs)
  - Subscribers
  - Relying Parties
  - Registration Authorities (RAs)
  - Critical Roles for Deployment and Sustainment
- PK-Enabling Applications

- Mechanisms
  - X.509 Certificate Fields and Extensions
  - Extension Details
  - RFC 3779
  - Draft Certificate Profile
- Architecture and Transactional View
  - PKI Revocation Architecture
- PKI Trust extension
- Way Ahead for Constituency
- Resources

PKI Usage

- PKI is the foundation for security mechanisms that provides a variety of cryptographically based services through the use of asymmetric key pairs
  - Authentication via enrollment and registration processes which cryptographically bind a key to an identity
  - Integrity of a transaction through digital signature processes
  - Encryption primarily through SSL/TLS

Benefits

- Foundational in securing Internet routing system
  - Analogous to DNSSEC as securing DNS
- Extended usage (such as portal authentication, communication security, billing integrity) may become part of overall capability
  - Requirements may differ, but essential technology and operational impacts remains consistent

Constituency Acceptance

- Published policy has to match goals for integrating public key technology
- Openly identify details on cost to deploy and sustain as well as impact to current business processes
- Anticipate that most ISPs will not want to set up and run their own CAs due to costs and administration burdens
  - RIRs should strongly consider offering "outsourced CA services" for their members
  - ISPs may wish to run their own CAs in their own environments, but it shouldn’t be a requirement
- Ensure expenditures are consistent with phased implementation strategy
- Ensure business case benefits of better security are met

Specific Discussion of Requirements

- The use of a certificate issued to authenticate a representative of an ISP as a representative of that ISP, based on the AS number(s) in the extension, is consistent with stated goal of using PKI to support routing security applications
  - Check to confirm that registrant is same entity as POC for corresponding whois record (for given address)
    - RFC 2725 (Routing Protocol System Security) states that routing object should be validated against both address and AS maintainers
  - Is this global policy across RIRs? Should it be?
- Database(s) to implement this check in authoritative manner

Certificate Policy

- A Certificate Policy (CP) is named set of rules indicating applicability of a certificate to particular community and/or class of applications with common security requirements
- IETF RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Statement) contains framework of topics to be covered when defining certificate usage in a given domain
  - Note that CPS are generally maintained privately within the given domain of the CP

Certificate Policy Framework

- Introduction
  - Participants, usage, policy administration, etc.
- Publication // Repository responsibilities
  - Naming, Identity validation, Identification and Authentication for rekey and revocation requests, etc.
- Life-cycle operational requirements
  - Issuance, key usage, renewal, rekey, revocation and suspension, status services, etc.
- Facility management // operational controls
  - Physical, procedural, audit logging, archival, etc.

- Technical security controls
  - Key pair generation, private key protection, etc.
- Profiles for Certificates, CRLs and Responder services
- Compliance audit and business // legal matters
  - Fees, privacy of personal information, IPR, dispute resolution, etc.

Policy and Cost Consideration

- Subordinate CAs are usually operational for some period of time that is double the time in which they actively issue certificates; the second half of the lifetime, they continue to issue CRLs
  - Lifetime will be dependent upon the business relation between the parties (RIR-ISP, ISP-ISP, ISP-end user) and will vary
- Hardware and software product life cycles are significantly shorter
- Maintenance costs increase when products are no longer supported by vendors

Algorithms and Key Sizes

- Current widespread use of RSA 1024 // 2048 with SHA-1
- Highly recommend following NIST Key Management Guidelines
  - Signature
    - o **EC-DSA = P256; *<u>P384</u>***
  - Encryption Certificates
    - o **EC-DH**
  - Supporting Algorithms
    - o **SHA-256**
    - o **AES**

Sample “Overview”

- Excerpt from draft Certificate Policy for Internet IP Address and AS Number PKI
- “This PKI is designed to support validation of claims by current holders of IP (v4 and v6) address space, and AS numbers, in accordance with the (current) records of the registries and ISPs that act as CAs in this PKI”
- “The ability to verify such claims is essential to ensuring the unique, unambiguous allocation of these resources”

- “The PKI encompasses several types of certificates
  - CA certificates for each organization allocating address blocks and AS numbers, and for each address space holder
  - Potential to use end entity certificates for operations personnel to support access control for the repository system”

Roles and Responsibilities

- Certification Authorities (CAs)
- Subscribers
- Relying Parties
- Registration Authorities (RAs)
- Critical Roles for Deployment and Sustainment

Certificate Authority

- CAs are trusted by users to create certificates and are responsible for issuing certificates, publishing certificates, and revoking certificates by placing them on Certificate Revocation Lists (CRLs)
  - Roots or “trust anchors”
  - Subordinate CAs
- Need to clarify which organizations that allocate IP addresses and AS numbers will act as CAs

Subscriber

- Generically, a subscriber is the entity whose name appears as the subject in a certificate and are expected to use the private key associated with the public key contained in the certificate in accordance with the requirements of the CP identified in the certificate
  - Can refer both to ISPs, which can be subscribers of RIRs, NIRs/LIRs and other ISPs, and to organizations that are not ISPs, which are subscribers of ISPs in the networking sense of the term

ARIN Subscriber concept

- A subscriber is the entity who is expected to use the private key associated with the public key contained in the certificate and whose name may appear as the subject in a certificate .
- Subscribers ("certificate holders") can be organizations (CAs), infrastructure components and perhaps individuals
  - May include devices at some point in the evolution of PKI usage
- Attestation relates to currency of resource right-of-use

Relying Parties

- “Entities that need to validate claims of address space and/or AS number current holdings are relying parties. Thus, for example, entities that make use of address and AS number allocation certificates in support of improved routing security are relying parties. This includes ISPs, multi-homed organizations exchanging BGP traffic with ISPs, and subscribers who have received an allocation of address space from ISP A but want to authorize ISP B to originate routes to this space”
- “Repositories make use of certificates for access control – checking for authorization to upload certificate, CRL, and ROA update packages, and thus they too act as relying parties”

Registration Authorities

- RAs are officials recognized by the CA to ensure that the subscribers appropriately present the necessary credentials for registration into the PKI
- A Local Registration Authority (LRA) is an individual authorized by the RA to perform identity verification of human and component applicants, and to authorize issuance of certificates to human applicants

Critical Roles for Deployment and Sustainment

- These will never show up in a CP framework, but are absolutely critical to doing PKI right
- Applications Architect who understands the applications in use and their capabilities or limitations
- Systems Administrator // Operations Specialist who understands the business processes that will benefit from becoming Public-Key enabled as well as the operational environment

- Experienced PKI technology assessor who can verify that PKI vendor capability claims match the needed capabilities of the enterprise PKI
- Subject matter expertise in network routing, firewalls, web architectures, mechanics of SSL, directory services and, if required by the policy, hardware cryptographic tokens
  - These experts would work with the experienced PKI technology assessor to minimize cost and complexity in the design stages

PK-Enabling Applications

- Typically decentralized management of applications
- Resources for PK-enabling are on par with resources needed for maintaining system or upgrading hardware and software
- Enabling the applications and creating the certificates should occur in parallel
- PKE should constitute all aspects of accepting, verifying, utilizing and managing certificates and CRLs

Mechanisms

- Mechanisms
  - Most common certificate format used to represent key and identity binding is X.509v3 certificate structure
  - Originally based on ISO/ITU work for authenticating to and encrypting exchanges with Directory Services
  - Significant implementation and operational enhancements defined through IETF PKIX working group
  - Structure is typically "profiled" in the CP to represent usage, constraints and operational environment
    - Caveat – don't build a profile unless you know what you want to achieve with the PKI and how you plan to support the elements in the profile!

X.509 Certificate Fields and Extensions

- Version
- Serial Number
- Issuer Signature Algorithm
- Issuer
- Validity Period
- Subject
- Subject Public Key Info
- Issuer Unique Identifier
- Subject Unique Identifier
- *Authority Key Identifier*

- *Subject Key Identifier*
- *Key Usage*
- Extended Key Usage
- Private Key Usage Validity Period
- Subject Alternative Name
- Name Issuer Alternative
- Subject Directory Attributes
- *Basic Constraints*
- Name Constraints
- *CRL Distribution Points*

- Freshest CRL
- *Authority Info Access*
- *Subject Info Access*
- *Certificate Policies*
- Policy Mappings
- Policy Constraints
- Inhibit anyPolicy
- *IPAddrBlock*
- *AS Identifier*
- Signature

Extension Details

- **Extensions are either mandatory or optional and critical or non-critical**
- **Profile**
  - **Authority and subject key id are hashes of the respective public keys**
  - **Key Usage (critical) defines how key is to be used**
  - **Basic Constraints (critical) identifies CA**
  - **CRL DP provides location of CRLs**
  - **Authority and subject Information Access identifies point of publication for all certificates issued by the issuers' superior CA and location of information related to subject if it's a CA**
    - **SIA not present if subject is NOT a CA**
  - **Certificate Policies (critical) contains OID for Resource Certificate Policy**

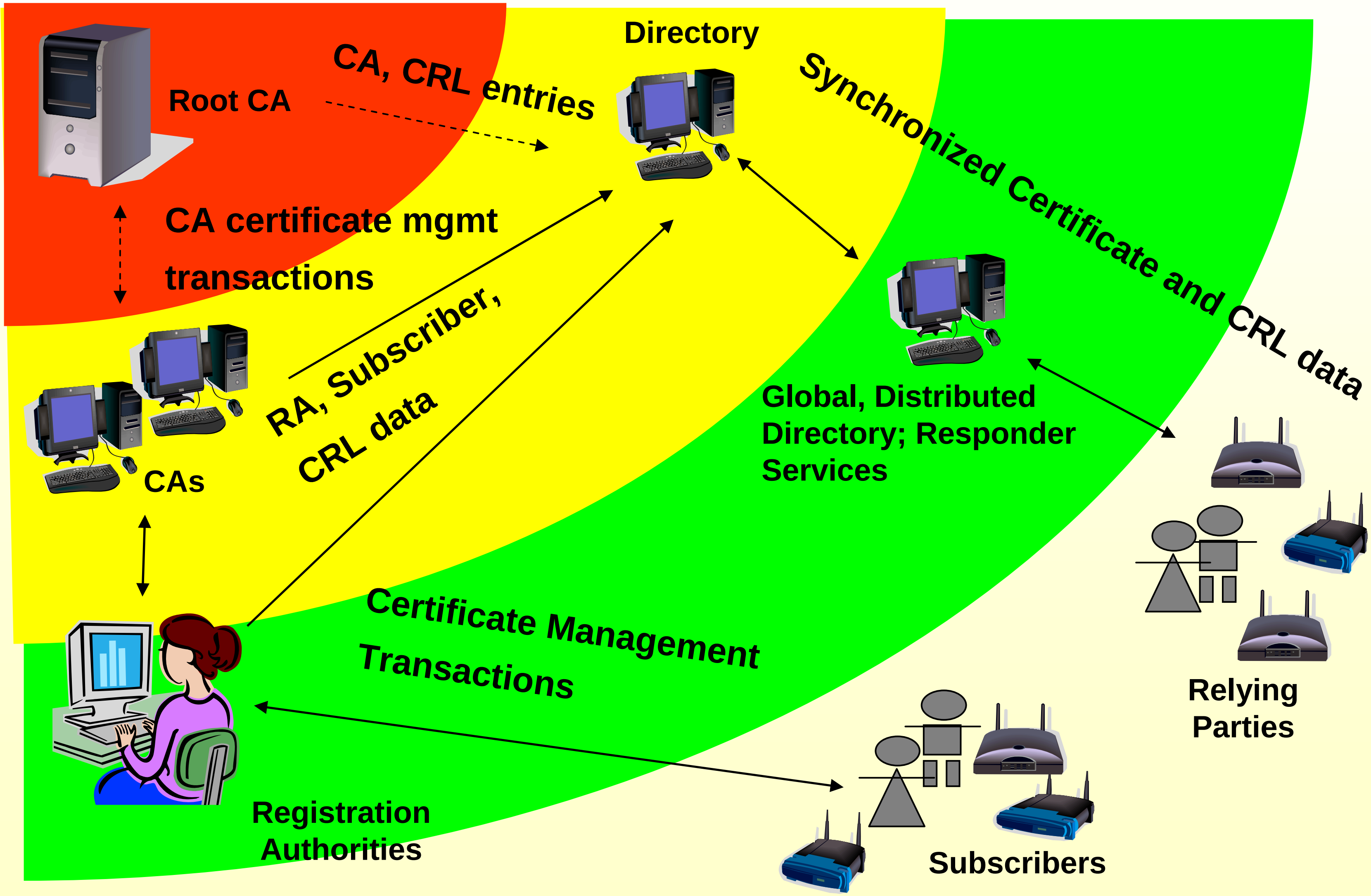
RFC 3779

- Defines two X.509 v3 certificate extensions: first binds list of IP address blocks, or prefixes, to subject of certificate; second binds list of autonomous system identifiers to subject of certificate
- Extensions may be used to convey authorization of subject to use IP addresses and autonomous system identifiers contained in extensions
- Right-to-use
  - for IP address prefix, being authorized to specify the AS that may originate advertisements of the prefix throughout the Internet
  - For autonomous system identifier, being authorized to operate a network(s) that identifies itself to other network operators using that autonomous system identifier

Draft Certificate Profile

- A Profile for X.509 PKIX Resource Certificates
  - APNIC
  - July 2006
- Defines which extensions must be used
- Test criteria for RFC 3779 extensions need to be developed
  - NIST PKI Test Suite covers almost every other known extension

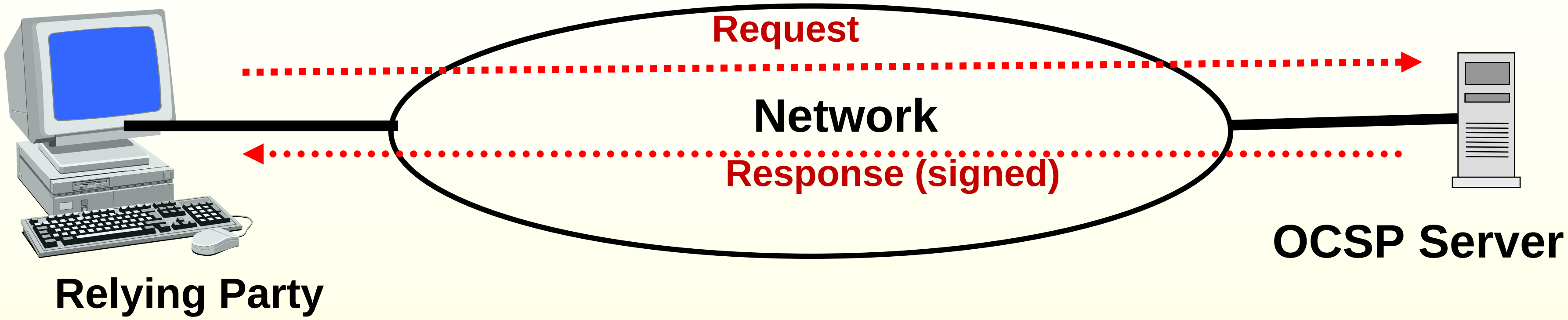
Architecture and Transactional View



PKI Revocation Architecture

- Certificate Revocation Lists (CRLs) are used to identify certificates that are (for any number of reasons) no longer valid
- Checking the CRL is essential element of certificate path validation to ensure certificates are still ‘good’
- Choice of mechanisms to convey revocation data and how the relying parties apply them are very dependent on applications, network, size of CRL and assurance required in PKI

- Full CRL checking at client
  - Most complex option; many client applications cannot perform necessary operations
- RFC 2560 On-line Certificate Status Protocol (OCSP) Responders
  - Off-loads processing (yes/no) to OCSP service; client simply conveys certificate under assessment to the OCSP responder and waits for answer
  - Enhancements under development in IETF draft for Server-based Certificate Validation Protocol (SCVP)

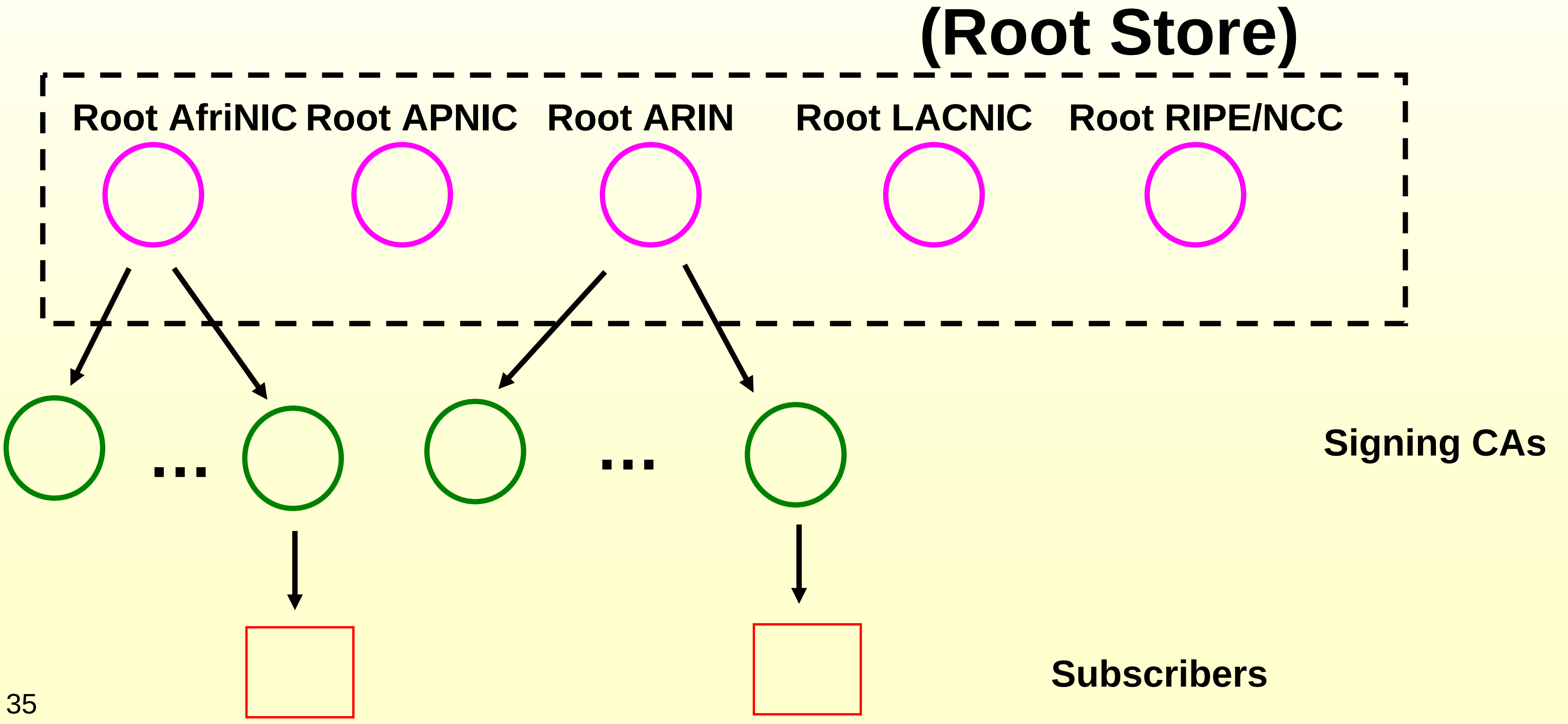


- Some consideration must be given to how the client handles the signed response, to avoid “looping”
- Infrastructure needs to “feed” CRLs to OCSP service – not standardized

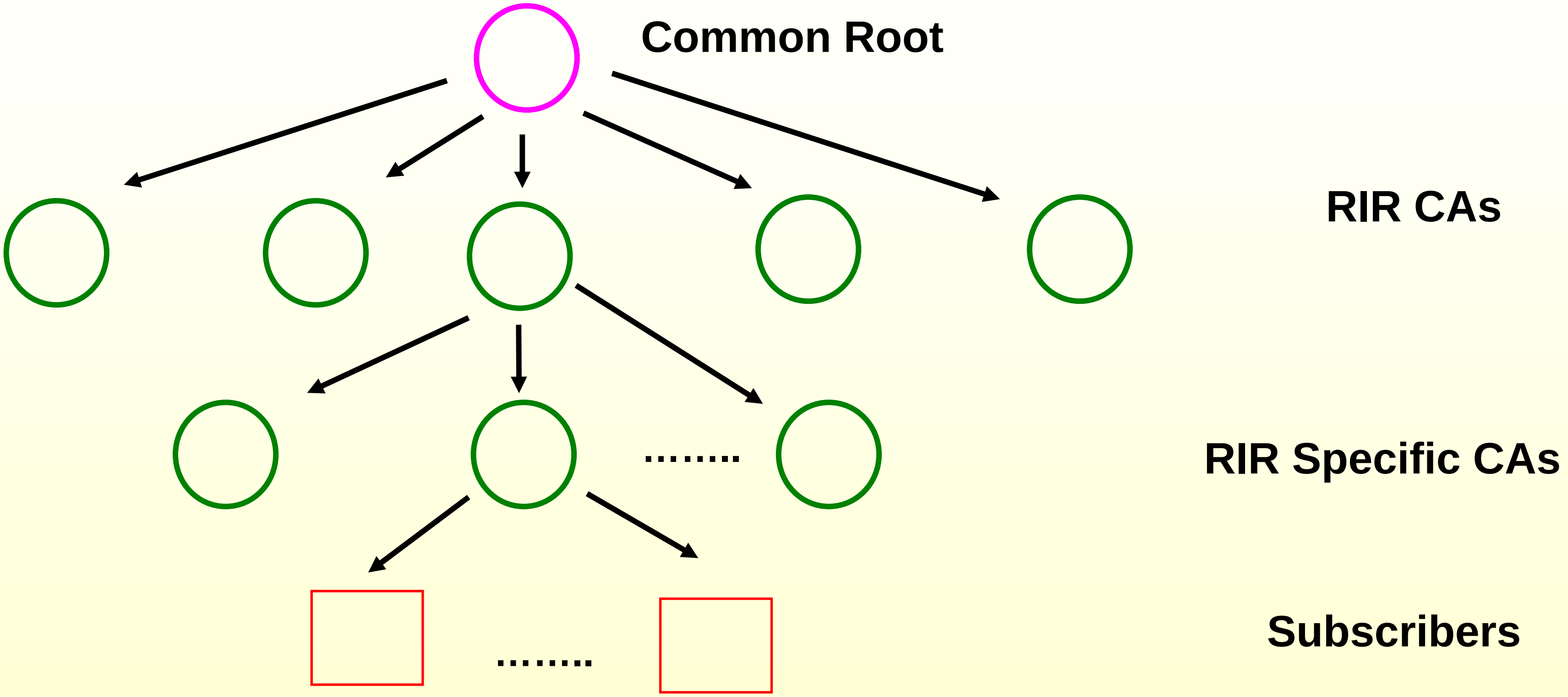
PKI Trust Extension

- Other RIRs are marching ahead with PKI deployments
- Variety of mechanisms available, but trust extension must meet business case and policy considerations
  - Must be considered at beginning of policy and architecture planning stage in order to ensure interoperability with minimum perturbation as architecture deployment occurs
  - Minimize cost and complexity both at relying party applications level and at operations level
    - **Are applications capable of building complex validation paths?**
    - **What does it take to ‘map’ certificate policies for equivalencies?**

Multiple Trust Anchors

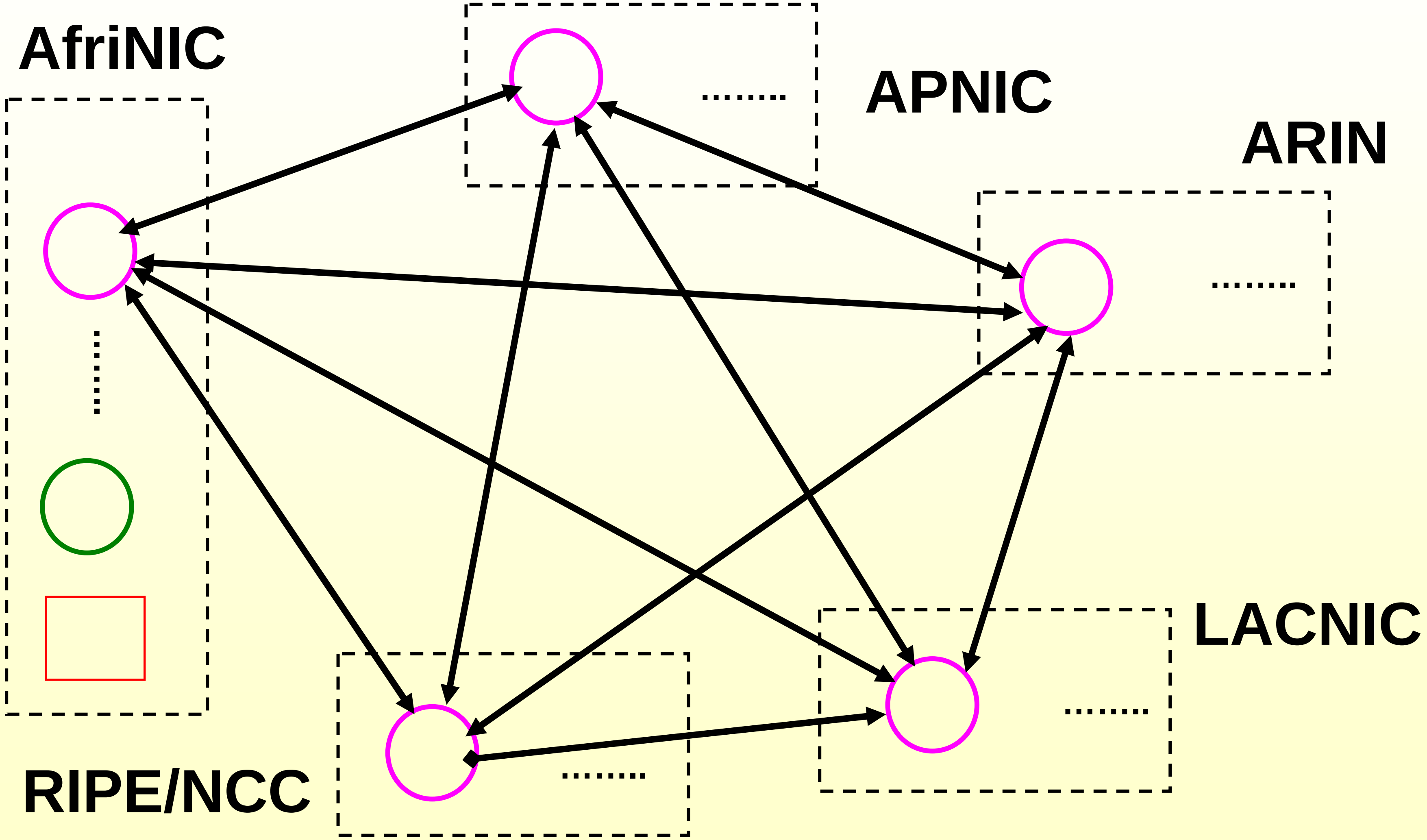


Common Rooted Hierarchy



- Who will run the Root?
- Transition the root to Common Root from RIR-Specific Root
- Lack of flexibility of trust from RIR to RIR

Bilateral Cross Certification among Roots of Hierarchies



- Cross certification is not currently in APNIC plans
- Anticipate that RIRs may issue certificates for each other for the resources that were traded or moved into the receiving RIR region
  - Common Certificate Policy required for equivalency in issuance assurance

Way Ahead for Constituency

- Think in Stages
- Start with Strategic view
  - Evaluate the business needs and create a model based on CP structure
  - Understand the architecture, technology, operational and support requirements and the impact to the existing business and applications context
  - Don’t forget to include interoperability with other PKI domains

- Develop pre-deployment criteria
  - Creating CP, training for operations and support elements, specifying the business processes that will be affected; acquiring hardware, software and services
- Limited initial deployment with selected participants
  - Leverage prototype systems being developed in various RIRs (APNIC, RIPE NCC) to raise awareness, experiment with usability and acceptance of proposed architecture
- Full rollout throughout enterprise, plan for interoperability with other domains

Resources

- RFCs
  - RFC 2560 – Online Certificate Status Protocol
    - http://www.ietf.org/rfc/rfc2560.txt
  - RFC 2725 – Routing Policy System Security
    - http://www.ietf.org/rfc/rfc2725.txt?number=2725
  - RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Statement
    - http://www.ietf.org/rfc/rfc3647.txt?number=3647
  - RFC 3779 - X.509 Extensions for IP Addresses and AS Identifiers
    - http://www.ietf.org/rfc/rfc3779.txt?number=3779

- Drafts
  - A Profile for X.509 PKIX Resource Certificates
    - o www.ietf.org/internet-drafts/draft-ietf-sidr-res-certs-02.txt
  - Server-Based Certificate Validation Protocol
    - o www.ietf.org/internet-drafts/draft-ietf-pkix-scvp-27.txt
- NIST Key Management Guidelines
  - Part 1: General
    - o Csrc.nist.gov/publications/nistpubs/800-57/Sp800-57-Part1.pdf
  - Part 2: Best Practices for Key Management Organizations
    - o Csrc.nist.gov/publications/nistpubs/800-57/Sp800-57-Part2.pdf
- PKI Test Suites
  - Csrc.nist.gov/pki/testing/xpaths.html

Questions?

- **Additional requests for information?**