An Operational ISP & RIR PKI

ARIN / Montreal

2006.04.10

Randy Bush <randy@psg.com>

<http://psg.com/~randy/060410.arin-pki.pdf>

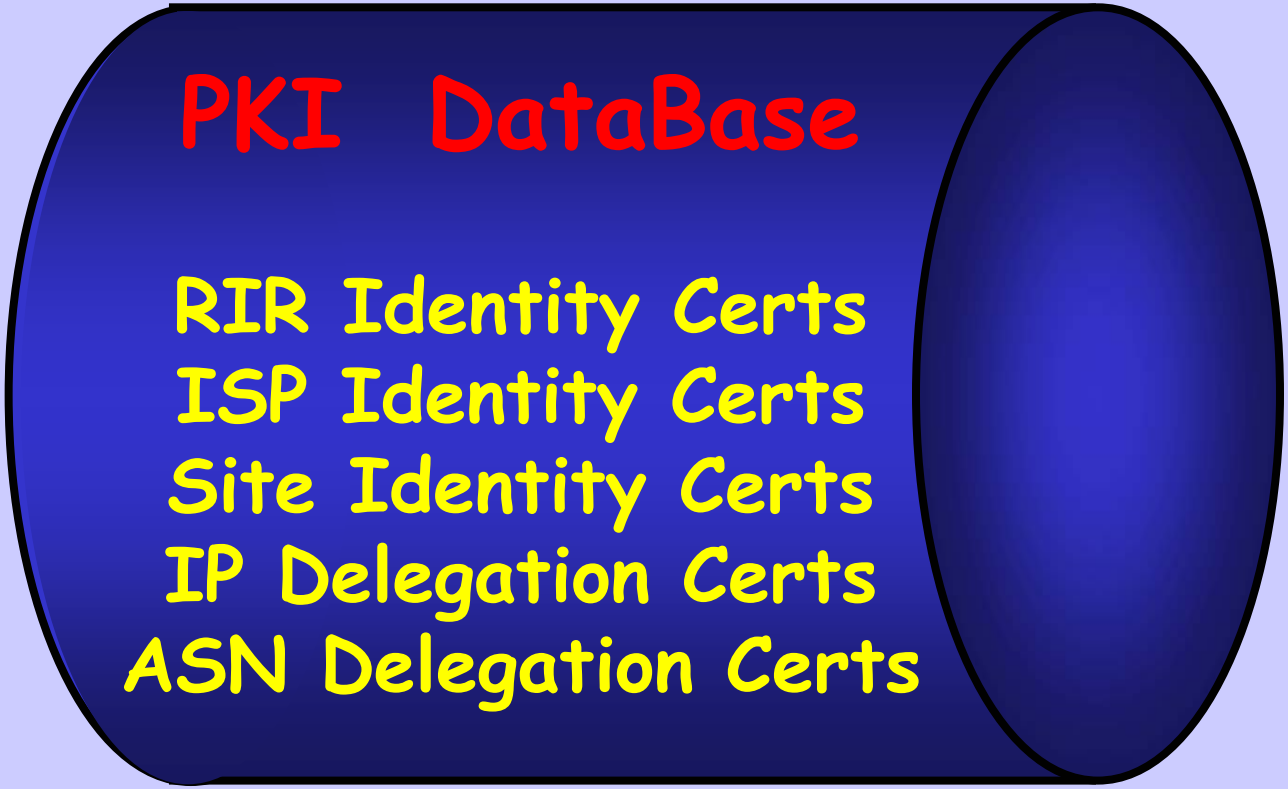
Quicksand

- 'Unknown' quality of whois data
- 'Unknown' quality of IRR data
- No formal means of verifying if a new customer really owns IP space X
- No formal means of verifying routing announcements

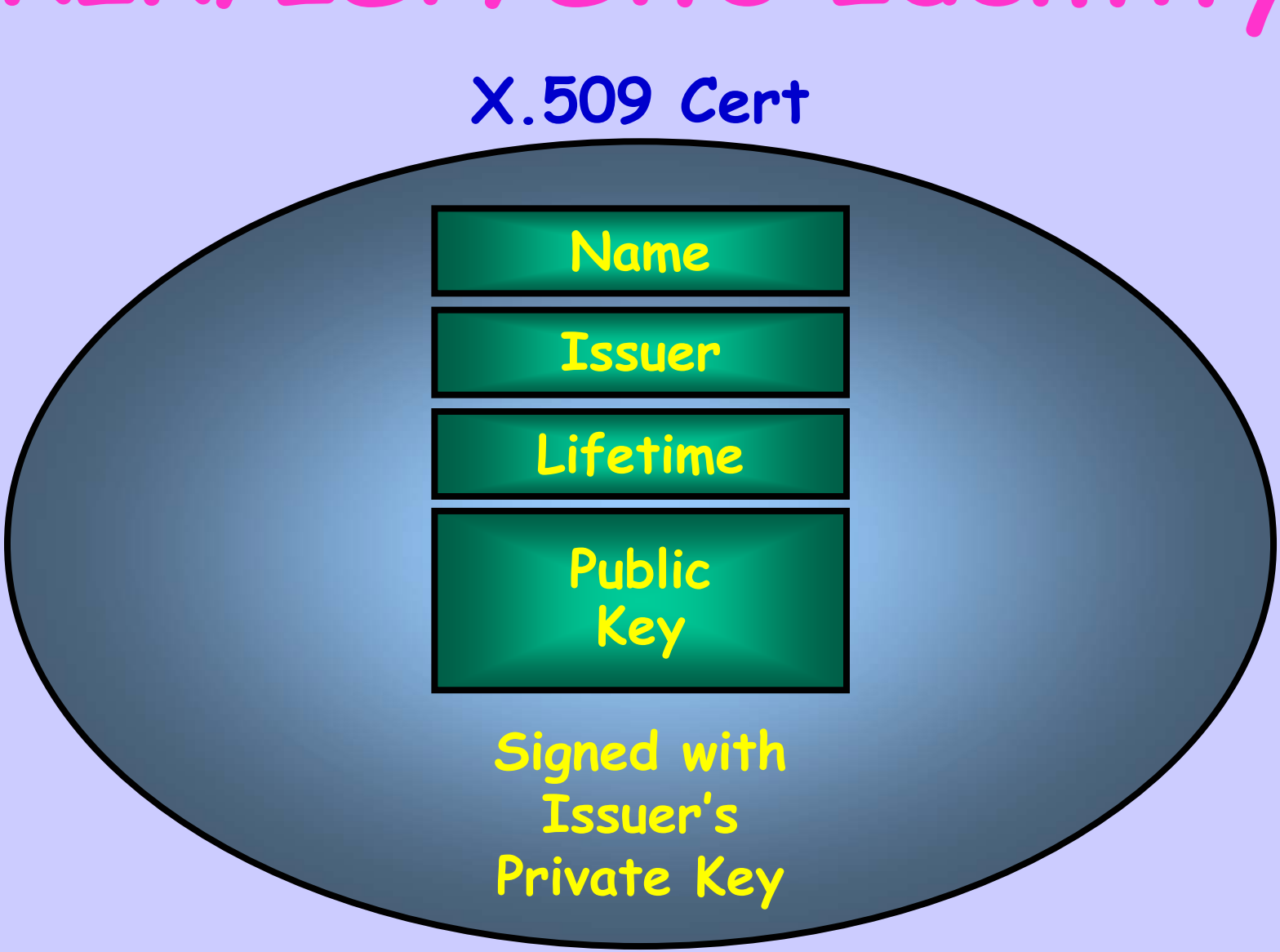
Routing Security Gap

- Routing (not router) Security is a major problem
- See Steve's presentation and <http://rip.psg.com/~randy/060119.janog-routesec.pdf>
- The big gap is the PKI, certificate structure, creation, storing, and moving

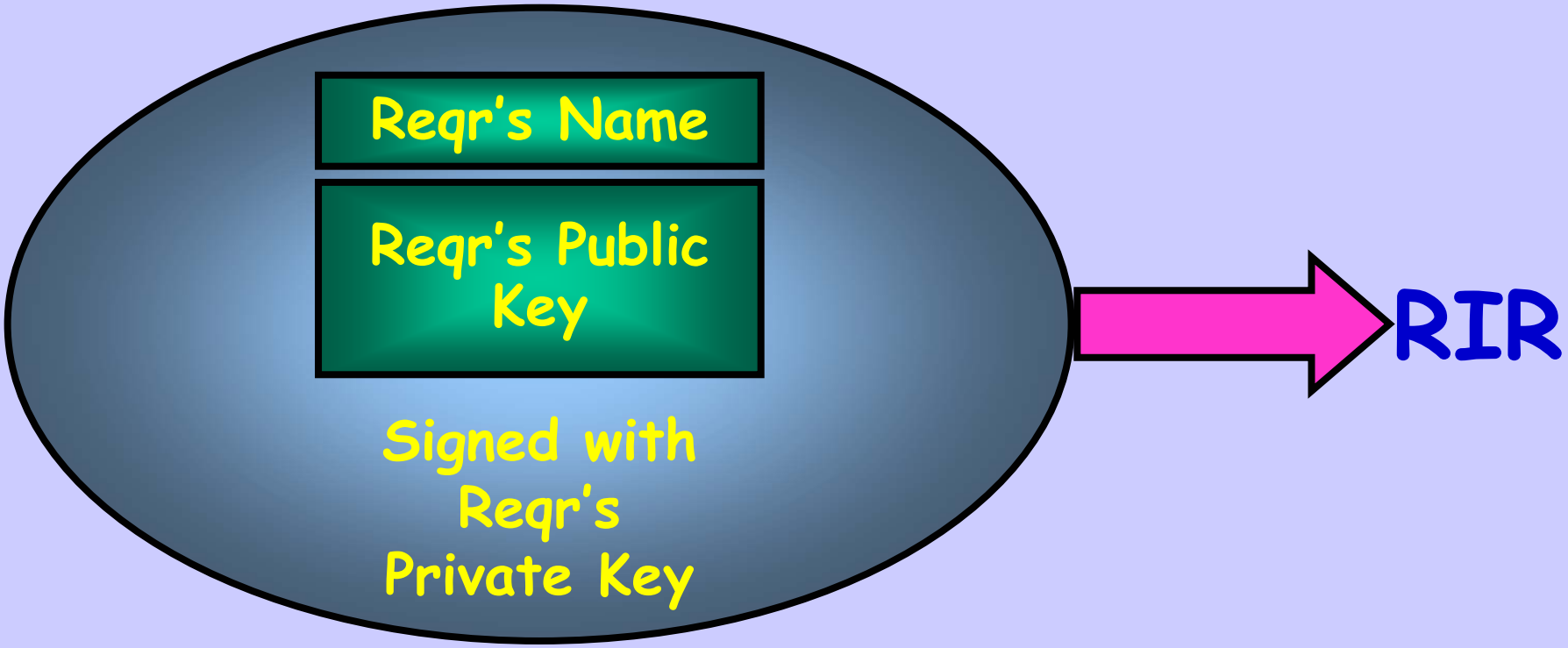
Public Key Infrastructure



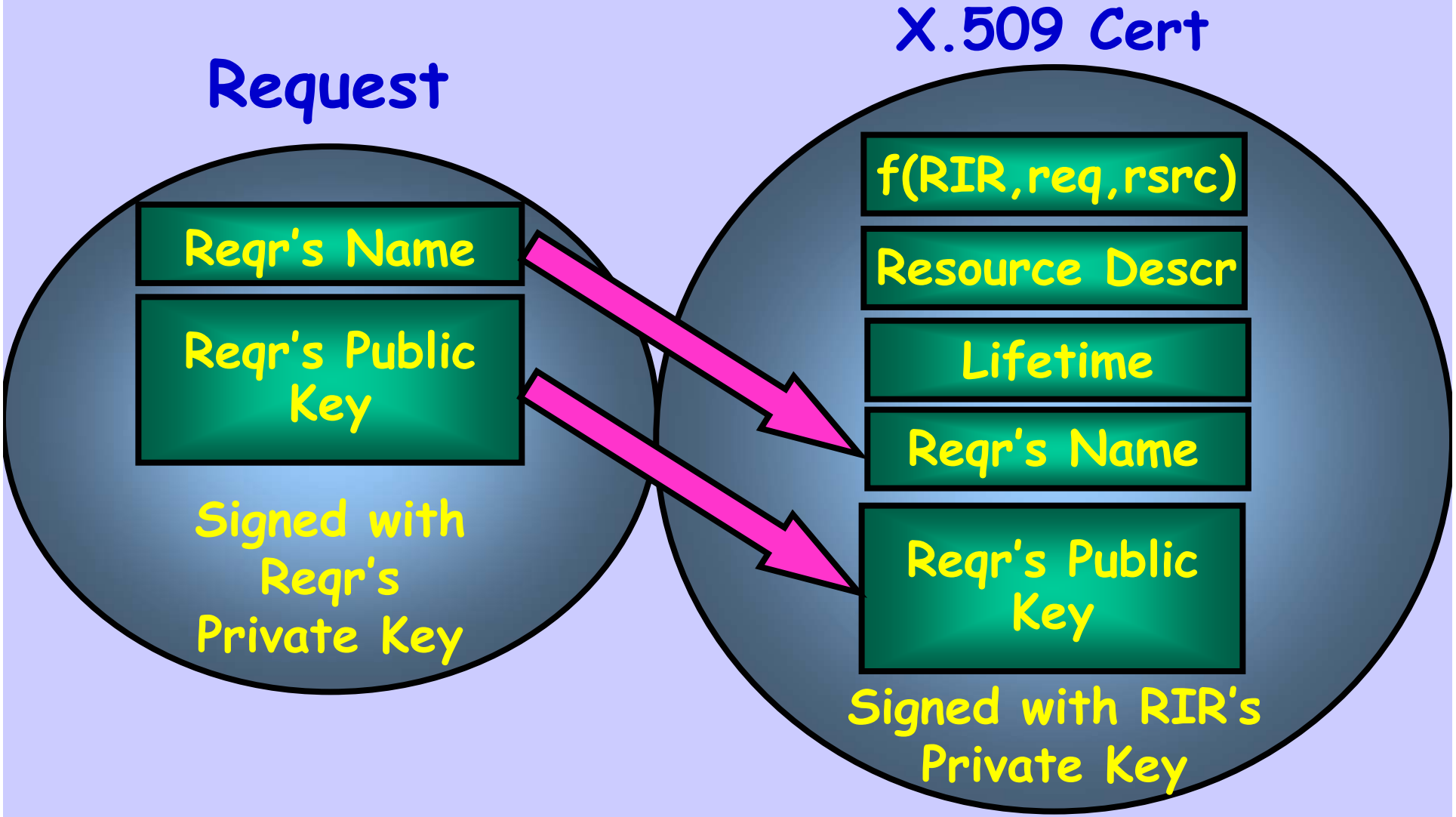
RIR/ISP/Site Identity



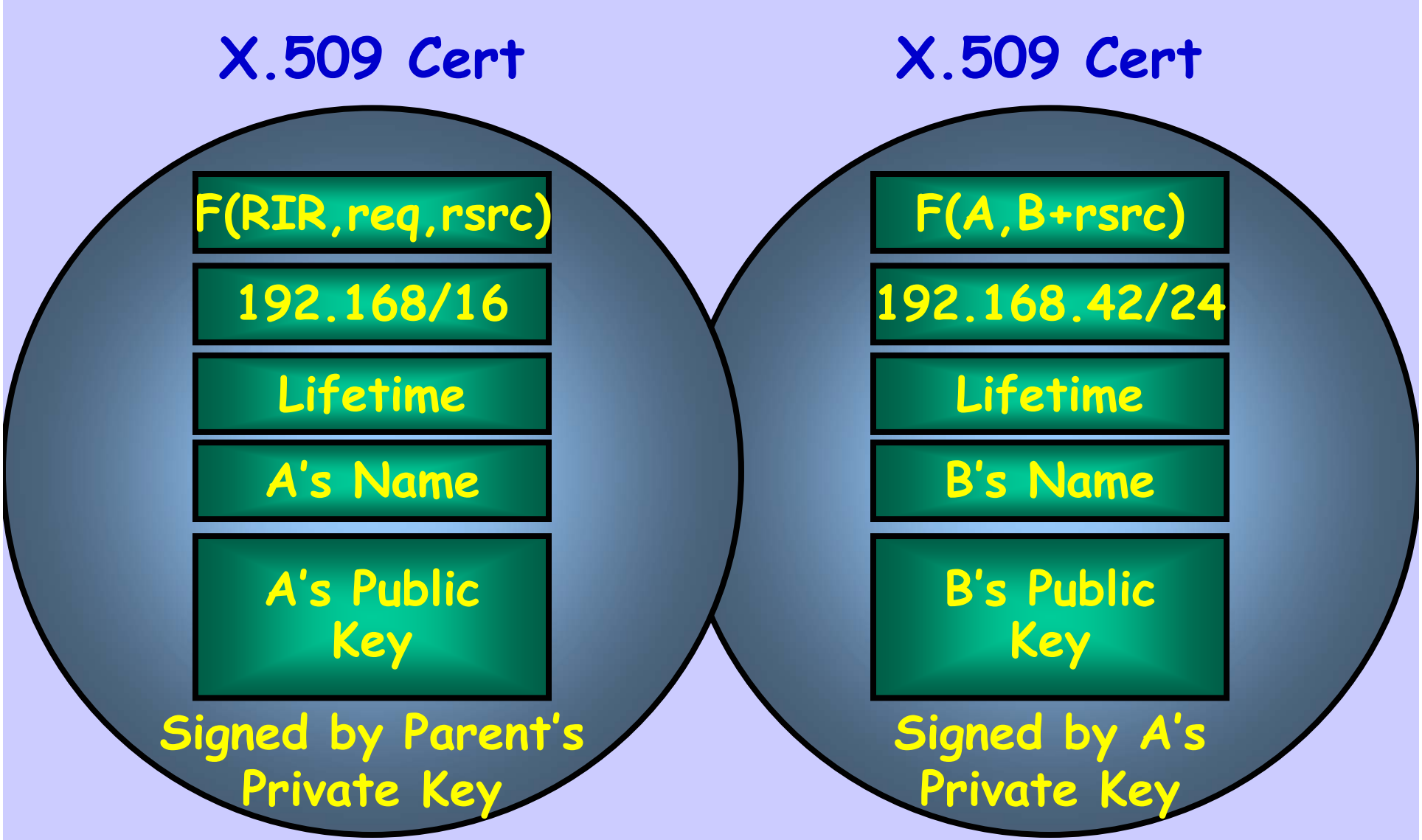
Resource Request



A Resource Allocation



Allocation Chain



IP and AS Attestations

- Specifies identity == {name,public key} of recipient
- Specifies block to be delegated
- Signed by allocator's private key
- Follows allocation hierarchy
  - IANA (or whomever) to RIR
  - RIR to ISP
  - ISP to downstream ISP or end user enterprise

IP Delegation Chain

- IANA allocates to RIR
  S.*iana* (192/8, *rir*)
- RIR allocates to ISP
  S.*rir* (192.168/16, *isp*)
- ISP allocates to User
  S.*isp* (192.168.42/24, *user*)
- Anyone can verify it all, because the public keys *iana*, *rir*, *isp*, and *user* are in the public PKI

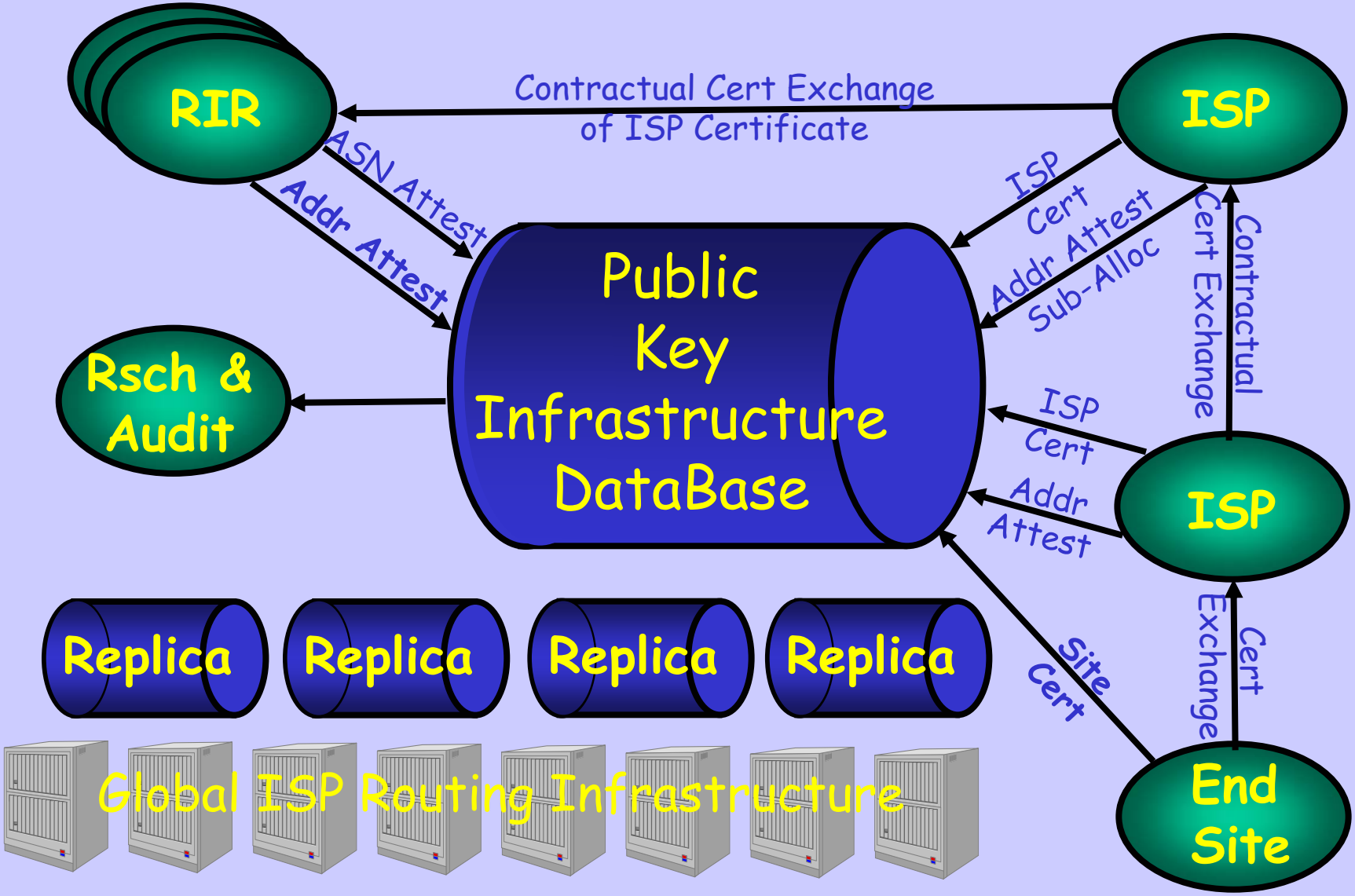
ISP / End-Site Certs

- May be acquired anywhere, Thawte, self-signed, …
- RIRs surely will issue as a service for members who don't get them elsewhere
- Need only be reproducible, not formally verifiable, because they are only used
  - In business transactions where they are exchanged and managed by contract, or
  - Bound to IP or ASN attestations by the RIRs or upstream ISPs
- ISPs may use an ARIN identity for an APNIC allocation or business transaction

RIR Identity

- RIR identities are their X.509 identity certificates
- They can get their certificate from the NRO, IANA
- They can buy outside, or generate a self-signed cert, or …
- The hard issues are key rollover, revocation, …

PKI Interfaces/Users



Transacting with PKI

- RFC 2585 describes FTP and HTTP transport for PKIs
- Also describes interfaces and the transactions for publishing certs etc.
- The PKI is self-authenticating because it is just a bundle of certs
- So no need for transport security!

Tools for RIRs

- Generate and receive ISP certs
- Receive ASN and IP space delegations from *upstairs*
- Issue IP and ASN allocations to ISPs and End Sites
- Manage their own keys

How ISPs Can Use

- Manual verification of customer's claim to own space
- Debugging hijacking issues
- Validation of IRR data when building route filters
- And, of course, in the long run, secured BGP

Tools for ISPs

- Generate and/or acquire their own identity certs
- Generate IP and ASN requests to RIRs and Upstreams
- Generate certs for downstream ISPs and End-User sites
- Validate resource certificates

Some Open Issues

- Coordination of updates, one central repository is not operationally feasible
- LDAPv3 (RFC 3377) and RFC 2829 Authentication Methods for LDAP may address this issue
- Cert/key rollover and revocation
  - 'root' certs, e.g. iana or whatever
  - ISP certs

  May require a separate and secured communication channel

Thanks to Our Kind Sponsors & Clue-Givers

Internet Initiative Japan

NSF via award ANI-0221435

Steve Bellovin & JI

Questions for Board

- Should ARIN be issuing real identity certificates?
- Do IP and ASN allocations derive from the IANA, NRO, …?
- What should be the lifetime of identity certificates and allocations?
- Should A transferring part of an IP allocation to B preclude A from announcing the covering prefix?