IIJ

Internet Initiative Japan

What I Want for Eid ul-Fitr

An Operational ISP & RIR PKI

APNIC / Perth

2006.03.01

Randy Bush <randy@psg.com>

<http://psg.com/~randy/060301.apnic-pki.pdf>

Wikipedia Says

Eid ul-Fitr (Arabic: عيد الفطر), often abbreviated as simply Eid, is an Islamic holiday that marks the end of Ramadan, the month of fasting. *Fitr* means "to break" and therefore symbolizes the **breaking of the fasting period and of all evil habits**.

This year it will be about October 24

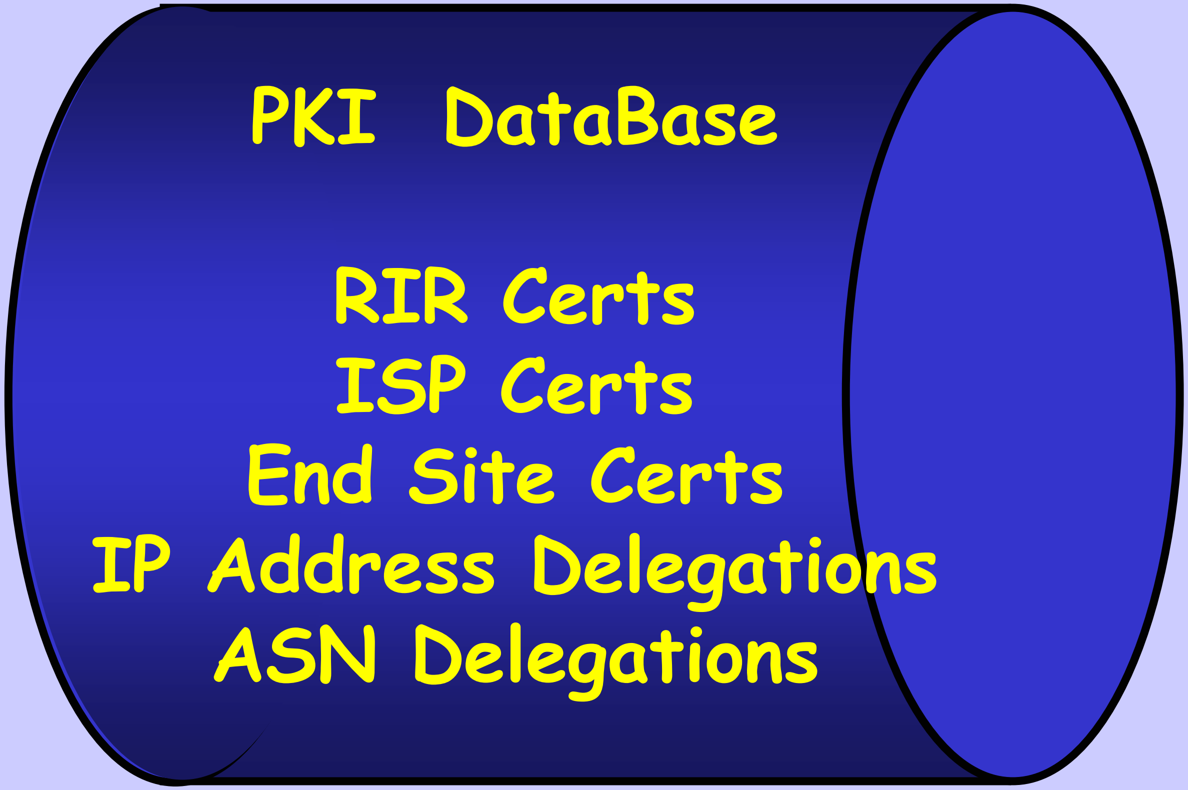
Our Evil Habits

- 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 <http://rip.psg.com/~randy/060119.janog-routesec.pdf>
- The big gap is the PKI, storing and moving the certificates

Public Key Infrastructure



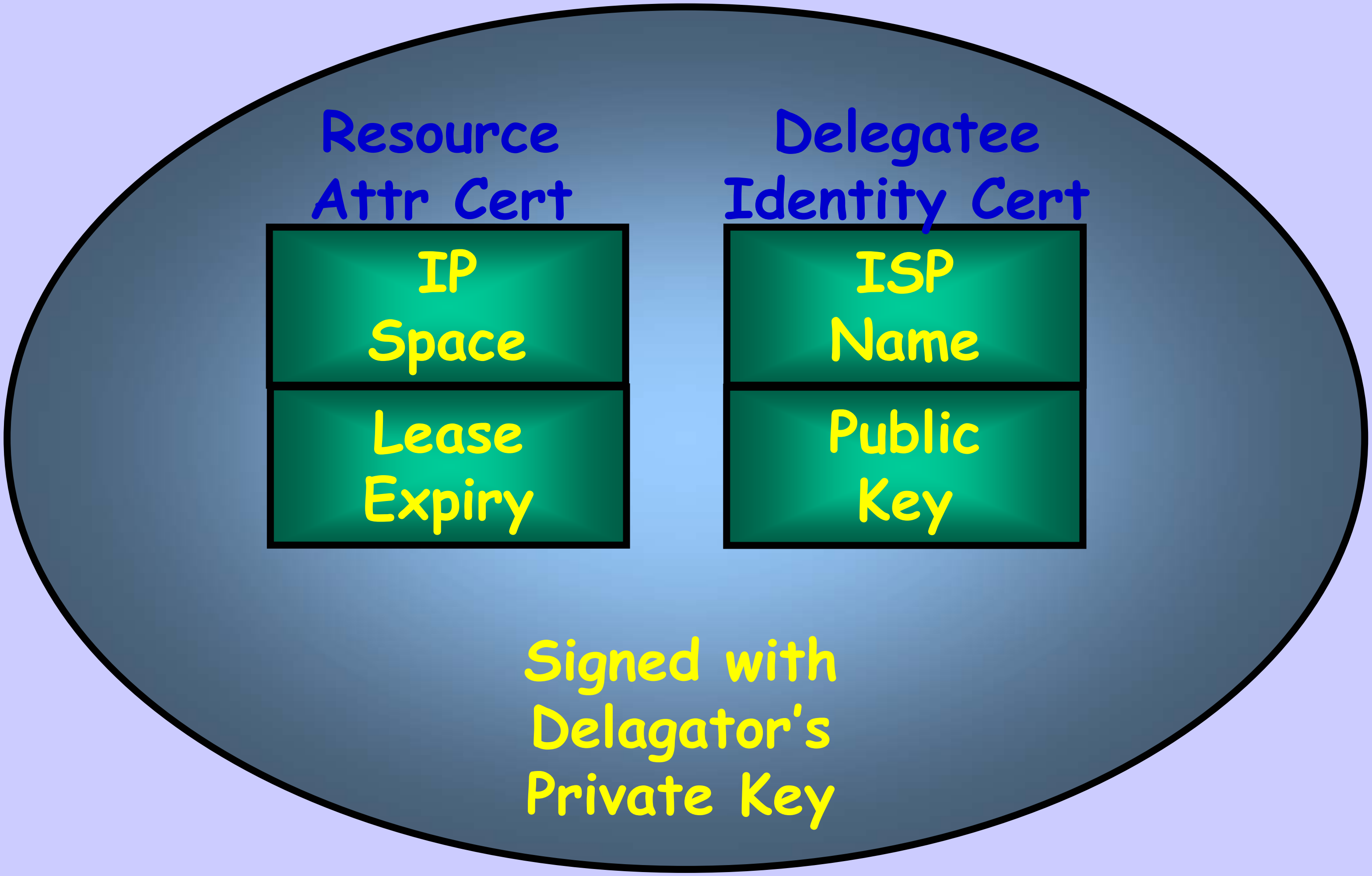
PKI DataBase

RIR Certs
ISP Certs
End Site Certs
IP Address Delegations
ASN Delegations

IP and AS Attestations

- Specifies identity == 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

An IP Delegation



Resource Attr Cert

IP Space

Lease Expiry

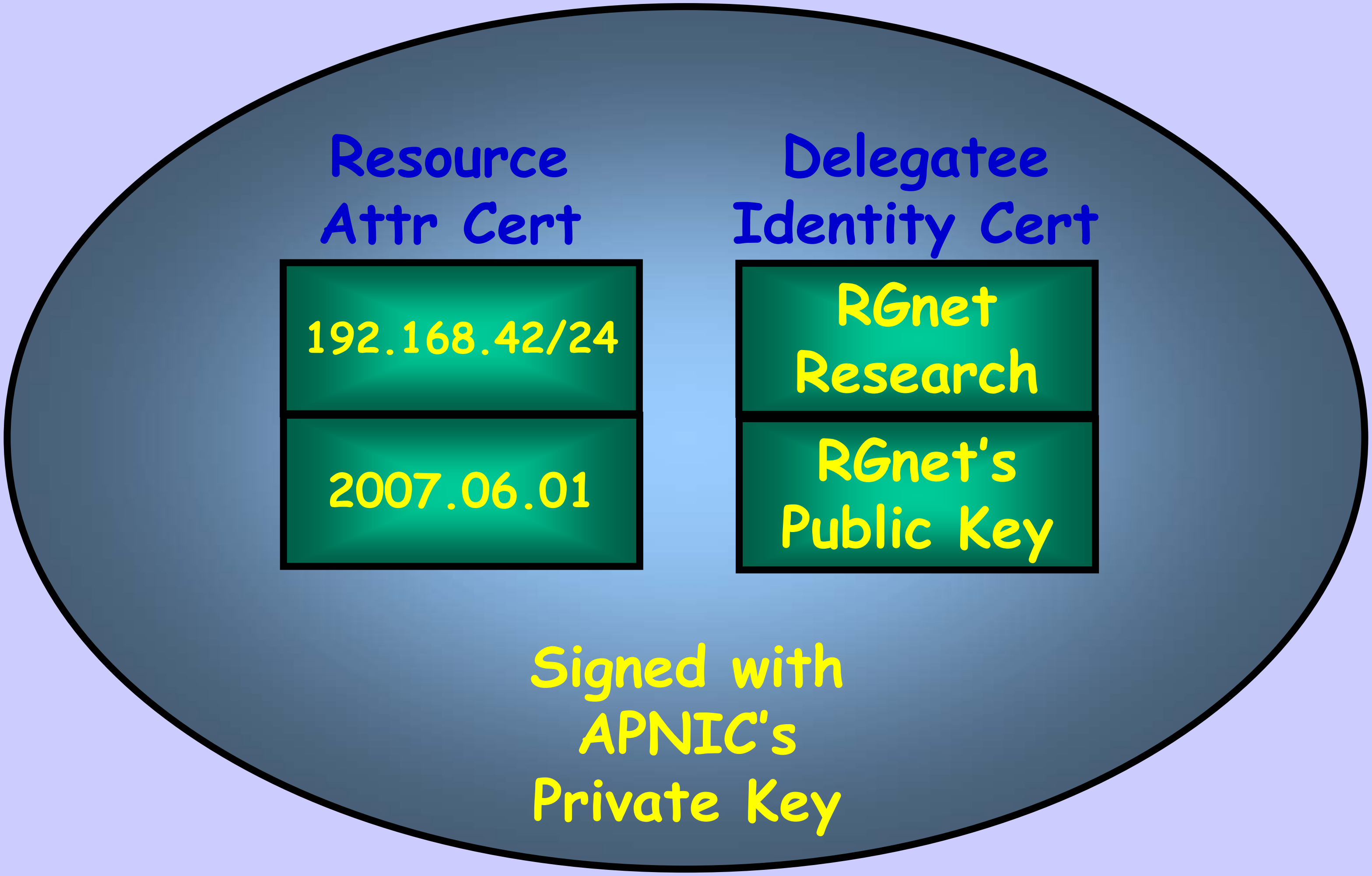
Delegatee Identity Cert

ISP Name

Public Key

Signed with Delagator's Private Key

IP Delegation Example



Resource Attr Cert

192.168.42/24

2007.06.01

Delegatee Identity Cert

RGnet Research

RGnet's Public Key

Signed with APNIC's Private Key

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

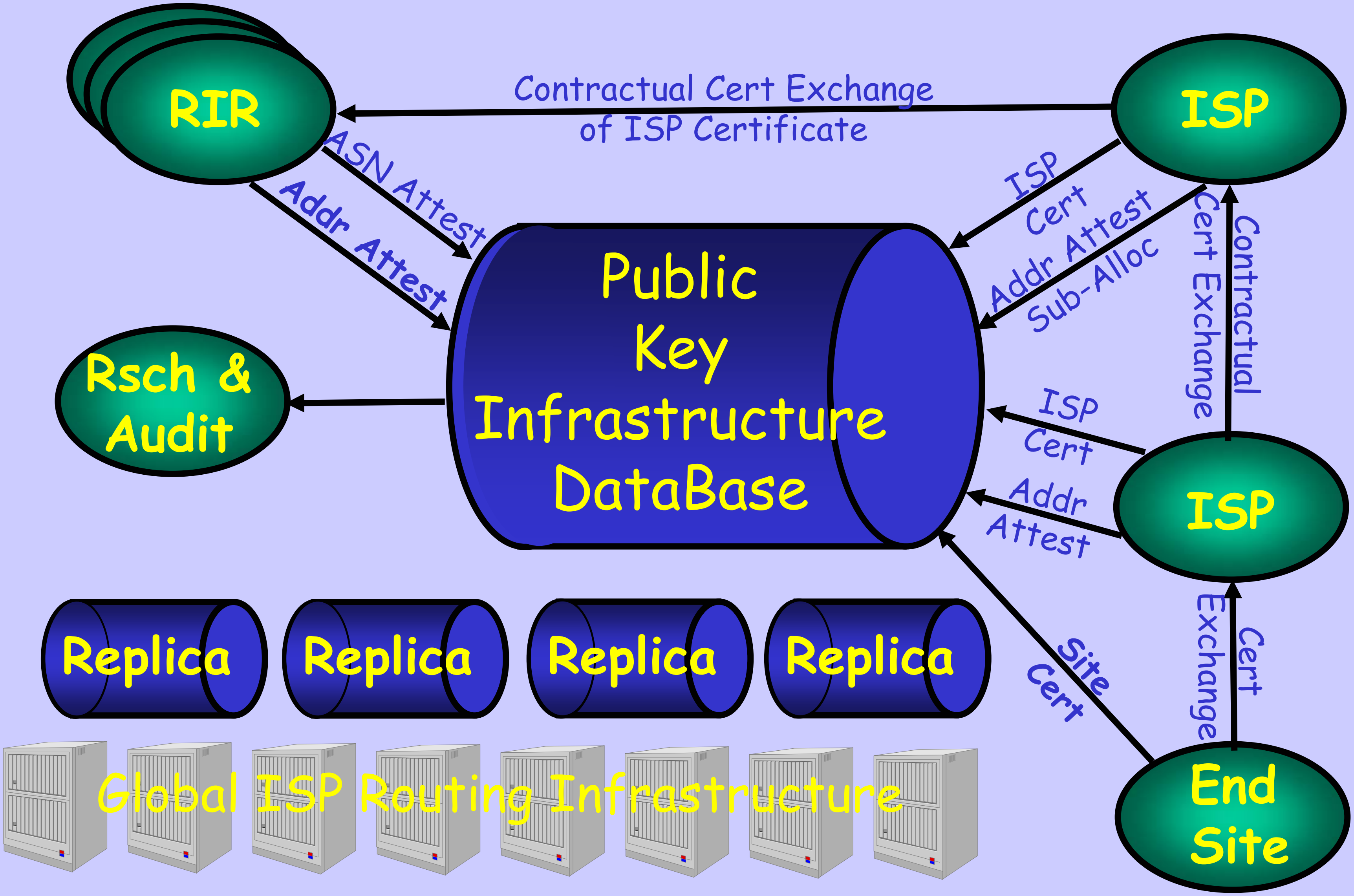
ISP / End-Site Certs

- May be acquired anywhere, Thawte, self-signed, …
- RIRs surely will issue as a service for members who don't get them elsewhere
- They need no attestation 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
- Big ISPs may use an ARIN identity for an APNIC allocation or business transaction

RIR Identity

- Similarly, RIR **identities** are their public keys, part of a cert
- They can get their cert from the 'above', RIR, NRO, IANA, or
- They can buy outside, or generate a self-signed cert, or …
- The harder 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 attestations from *upstairs*
- Attest to allocation of Address Space and ASNs to ISPs
- 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 and register role certs with RIRs and Upstreams
- Generate certs for downstream ISPs and End-User sites
- Attest to IP allocations to downstream ISPs and End-Users

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