An Operational ISP & RIR PKI

EOF / Istanbul

2006.04.25

Randy Bush <randy@psg.com>

<http://psg.com/~randy/060425.eof-pki.pdf>

Quicksand

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

We Need To

- Verify that a customer has been allocated a resource they are asking an ISP or upstream to announce (manual)
- Verify the origin of announcements when debugging (manual)
- Verify IRR data when generating route filters (programmatic)
- Allow routers to formally verify BGP announcements as to origin and path

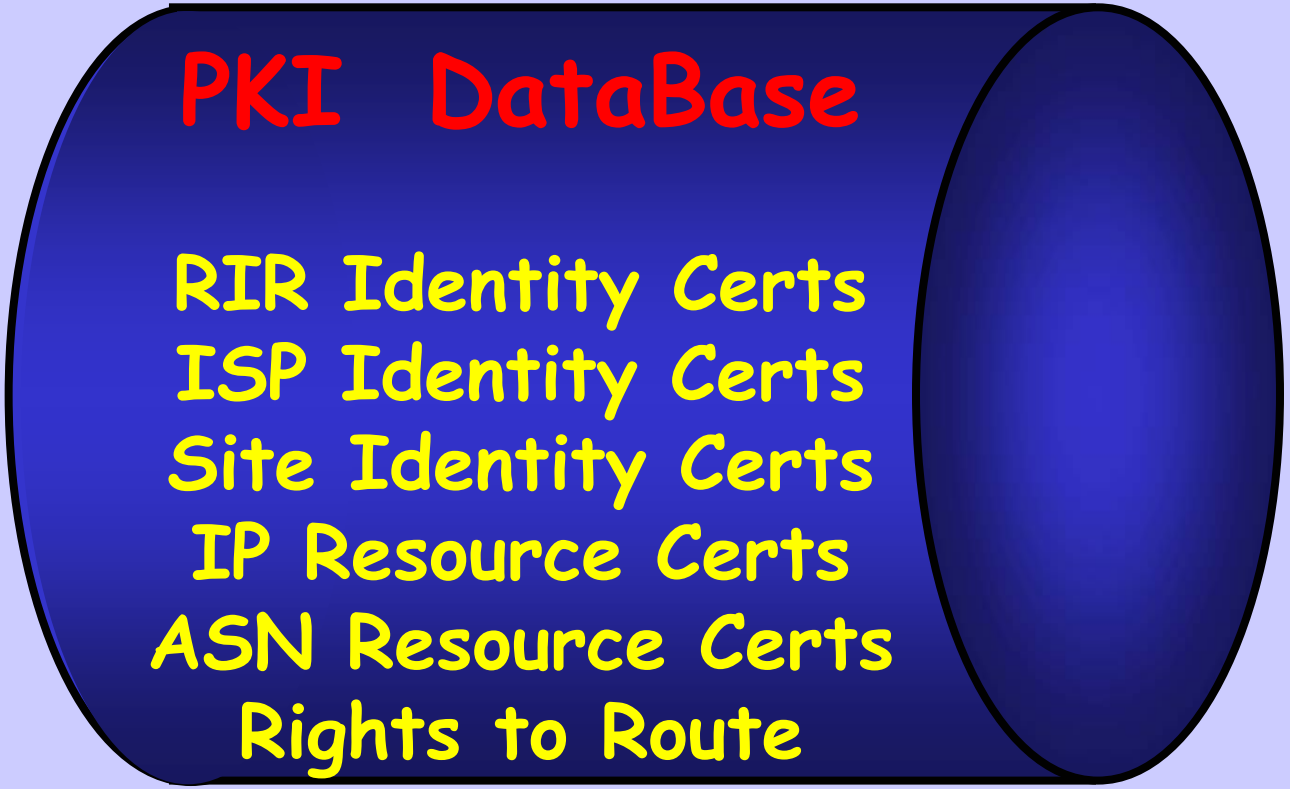
Provide

- Formally verifiable assertions of rights in IP Address Space and AS Numbers
- Formally verifiable assertions of rights of ASNs to originate prefixes
- Formally verifiable assertions of the correctness of routing announcements

Routing Security Gap

- The big gap is the PKI - certificate structure
  - Creating
  - Storing
  - Moving, and
  - Validating

Public Key Infrastructure



Application Range

- Handle both resource ownership
  - ASNs and IP space
- And certified transactions with RIR:
  - Allocation
  - Billing
  - DNS delegation

Operate Across RIRs

- With different kinds of IP/ASN allocations
  - Normal
  - Experimental
  - Legacy, …
- And resources received from multiple RIRs

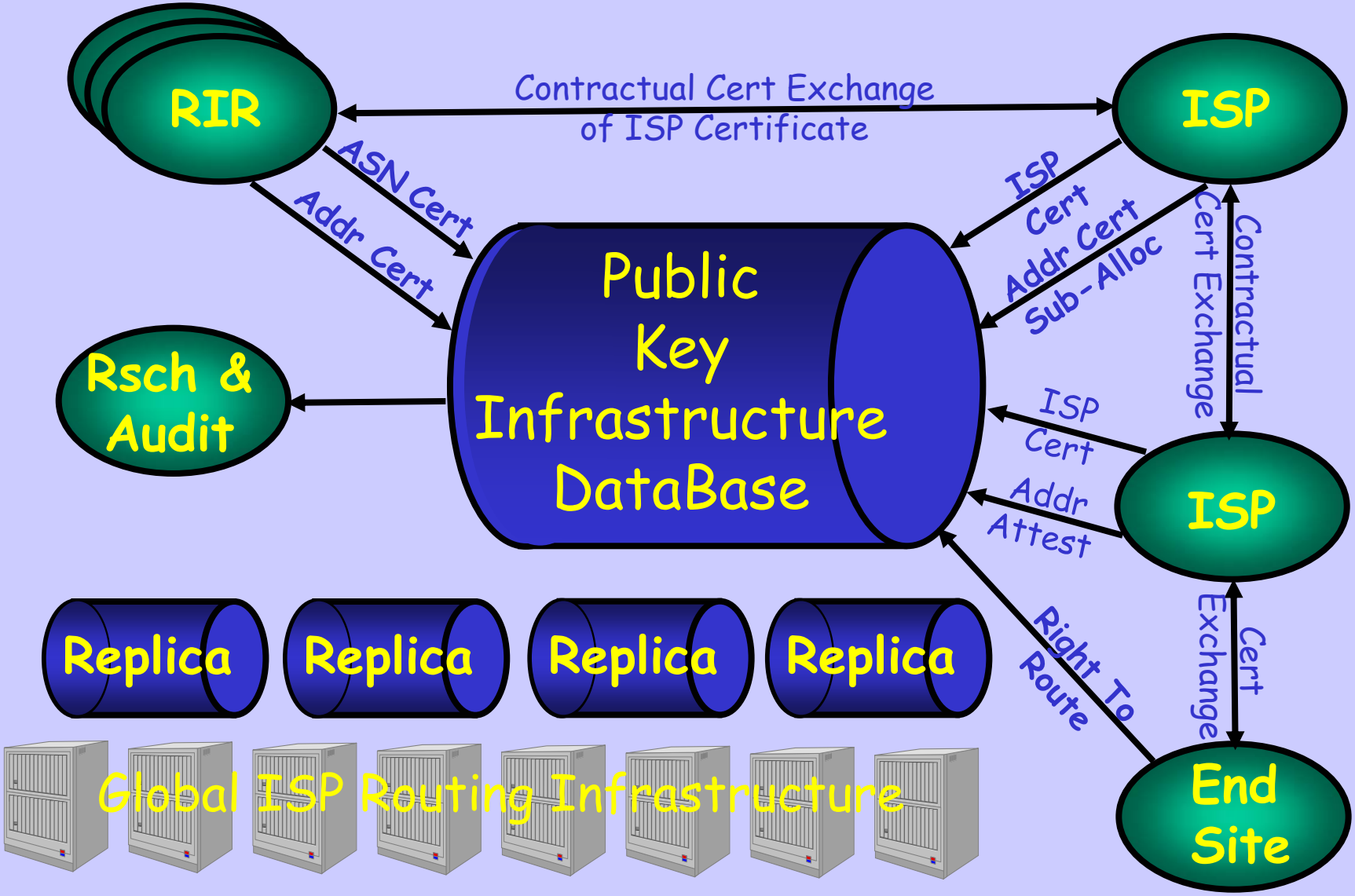
Security Policy Control

- Big ISPs need to control their own security policies
- I.e. manage their own certificate hierarchy with their own security policies
- Most members will not want to do this, but will ask the RIRs to handle the work

Aggregation Needs

- De-aggregate a resource and route the pieces separately
- De-aggregate a resource and transfer a portion to a third party
- Acquire a resource allocated to an ARIN member while my RIR is APNIC
- Aggregate resources obtained separately
- Possibly from/via multiple RIRs

PKI Interfaces/Users



IP and AS Certificates

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

IP Delegation Chain

- RIR allocates to ISP
  S.*rir* (192.168/16, *isp*)
- ISP allocates to Downstream
  S.*isp* (192.168.128/17, *dstr*)
- Downstream allocates to User
  S.*isp* (192.168.142/24, *user*)
- Anyone can verify it all, because the public keys *rir*, *isp*, *dstr*, and *user* are in the public PKI

ISP / End-Site Certs

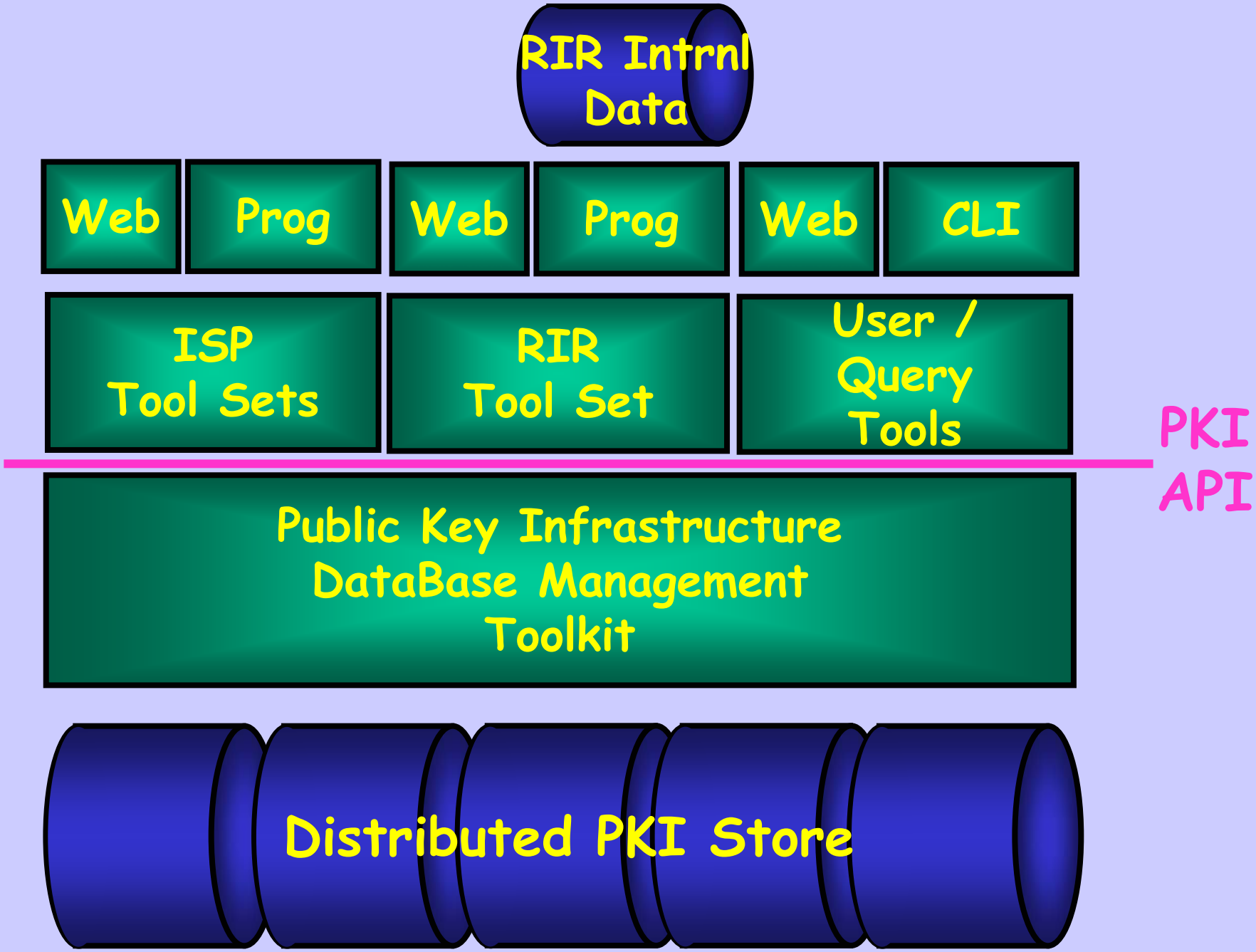
- RIRs generate identity certs for members
- Need only be reproducible, they are not formal identities, because are only used
  - In business transactions where they are exchanged and managed by contract, or
  - To create IP or ASN certs
- May be based on 'external', e.g. Thawte certs, used to generate an identity cert within the RIR PKI
- ISPs may use an ARIN identity for an APNIC allocation or business transaction

RIR Identity

- RIR identities are the root trust anchors for the system
- They can get their certificates from the NRO, IANA
- They can buy outside, or generate a self-signed cert, or …, but
- The hard issues are key rollover, revocation, …

Underlying Certificate PKI Architecture

- Allows one open implementation to be used by all
- Yet allows each RIR to have its own business processes and user front end
- And allows ISPs and end sites to build their own processes on top of the base tool-set



PKI Management API

- Trans-RIR API for dealing with distributed repository
- Describes interfaces and transactions for creating, publishing, validating, … certificates etc.
- The PKI is self-authenticating because it is just a bundle of certs
- So no need for transport security!

Tools for RIRs

- Create root ASN and IP space certificates
- Issue IP and ASN allocations to ISPs and End Sites
- Generate and lodge ISP certs
- Manage their own cert sets

Tools for ISPs

- Acquire identity certs from RIRs
- Generate IP and ASN requests to RIRs and Upstreams
- Generate certs for downstream ISPs and End-User sites
- Generate and manage role certs
- Validate resource certificates

Some Open Issues

- One central physical store is not operationally feasible
- API needs to include 'rcynic' to assemble and validate pieces
- Cert/key rollover and revocation
  - Trust points, e.g. RIRs, IANA
  - ISP identity certs
- Trust point changes may require secured communication channels

State of Play

- APNIC has a trial implementation
- APNIC & ARIN are converging on multi-RIR and ISP viewpoint requirements
- George & Geoff finalizing the first API model, essentially a C/perl interface
- The sub-API work has started
- The result will be open source
- Soon, RIRs and LIRs can code above

BGP Routing Security

- Over 3-10 years, PKI system provides the basis for verifiable BGP routing
- S-BGP, or SOBGP, or …
- But I am biased toward S-BGP
  - Is congruent with BGP, no weird baggage
  - Does not require publication of my policy
  - Does not rely on more external data

Thanks to Our Kind Sponsors & Clue-Givers

Geoff, George, & APNIC

Internet Initiative Japan

NSF via award ANI-0221435

Steve Bellovin & JI