An Operational ISP & RIR PKI

ARIN / Montreal

2006.04.10

Randy Bush <randy@psg.com>

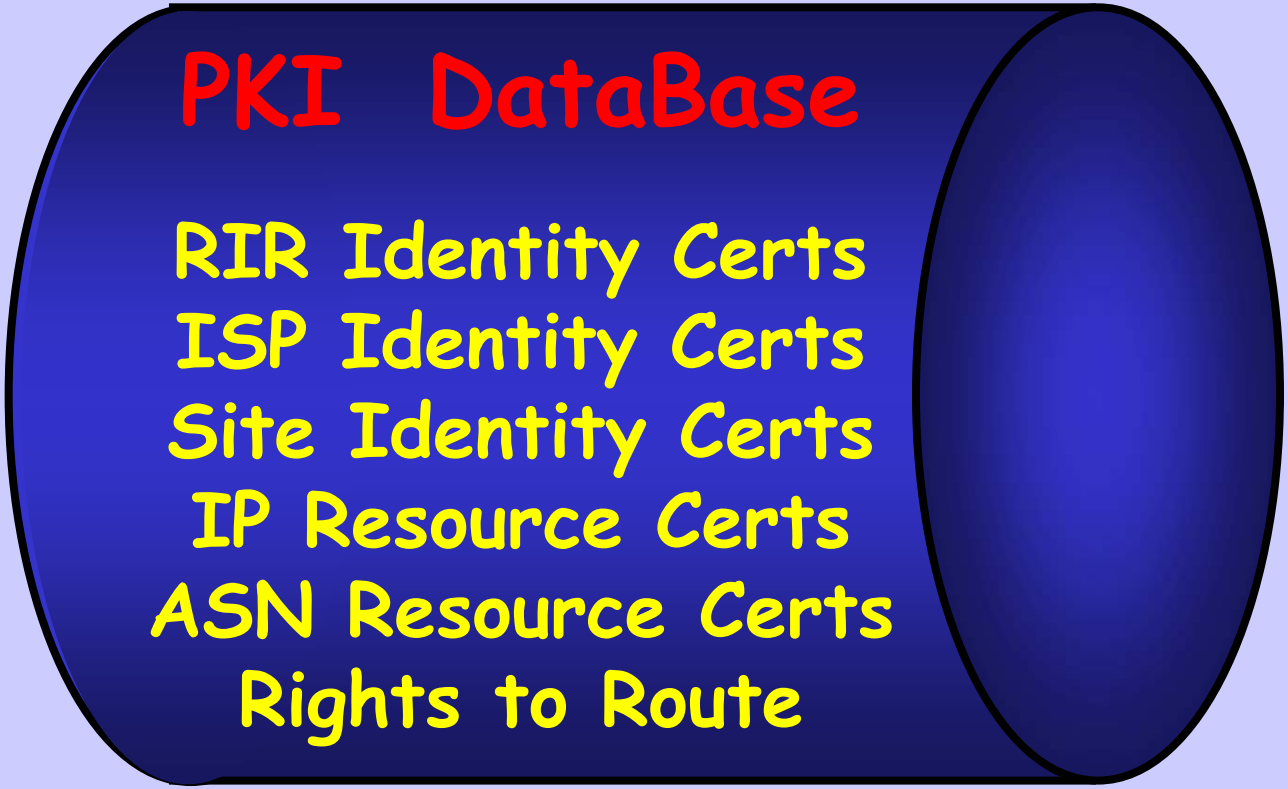
Quicksand

- '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

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



Formal Verifiable System which Allows RIRs and ISPs 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

Underlying Cert and PKI Architecture which

- 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

Application Range

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

Operate Across RIRs

- With different kinds of 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 cert 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

No Real-World ID

- The RIR system can **not** provide verifiable identity

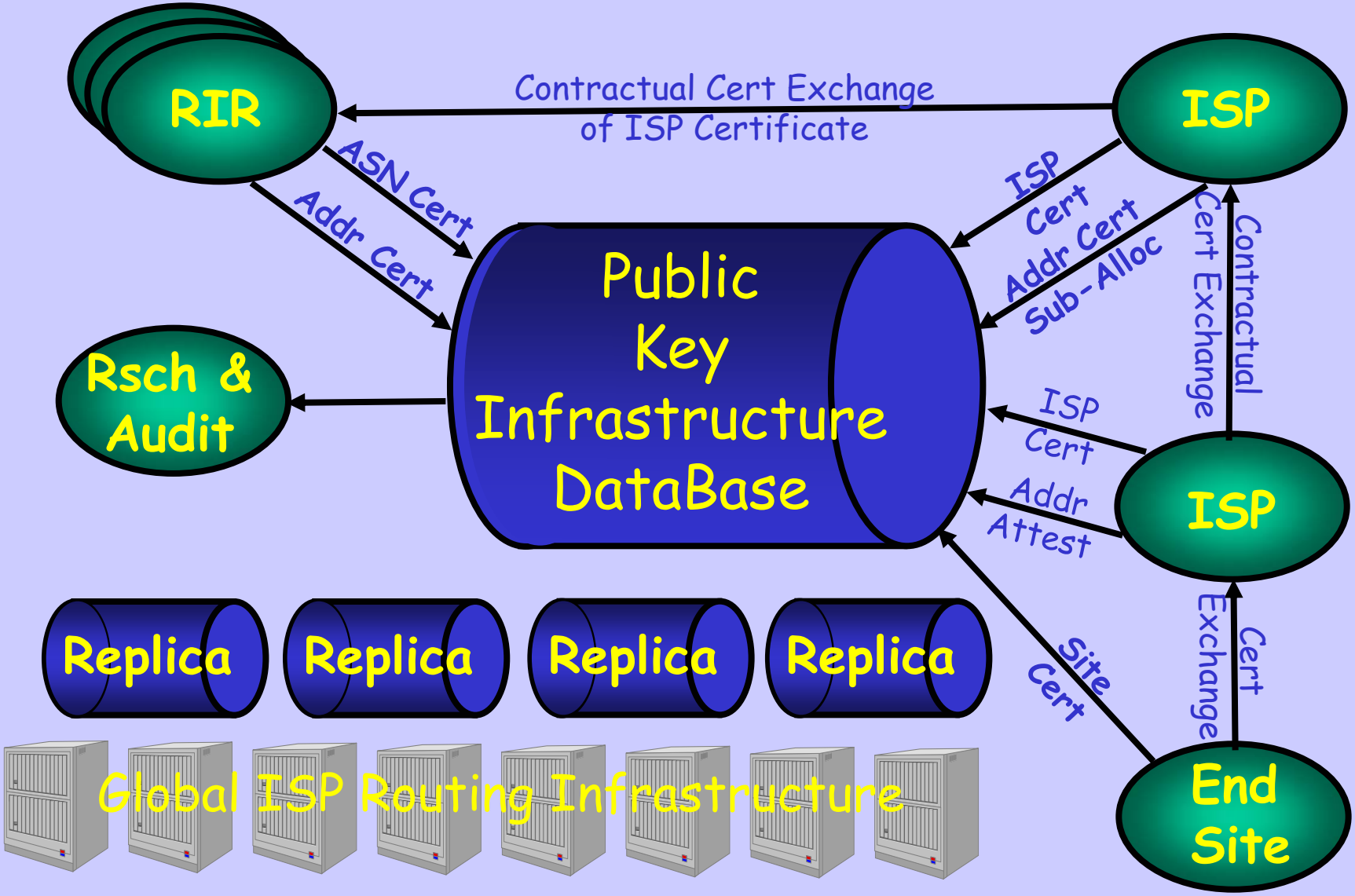
"A commercial CA will protect you from anyone from whom they won't take money."

-- Matt Blaze

What it Can Do

- The RIR system can let you verify that a resource is 'owned' by someone who can demonstrate that they have the private key matching the public key of the entity to which it was allocated
  - By the RIR, or
  - Someone down the allocation hierarchy from the RIR

PKI Interfaces/Users



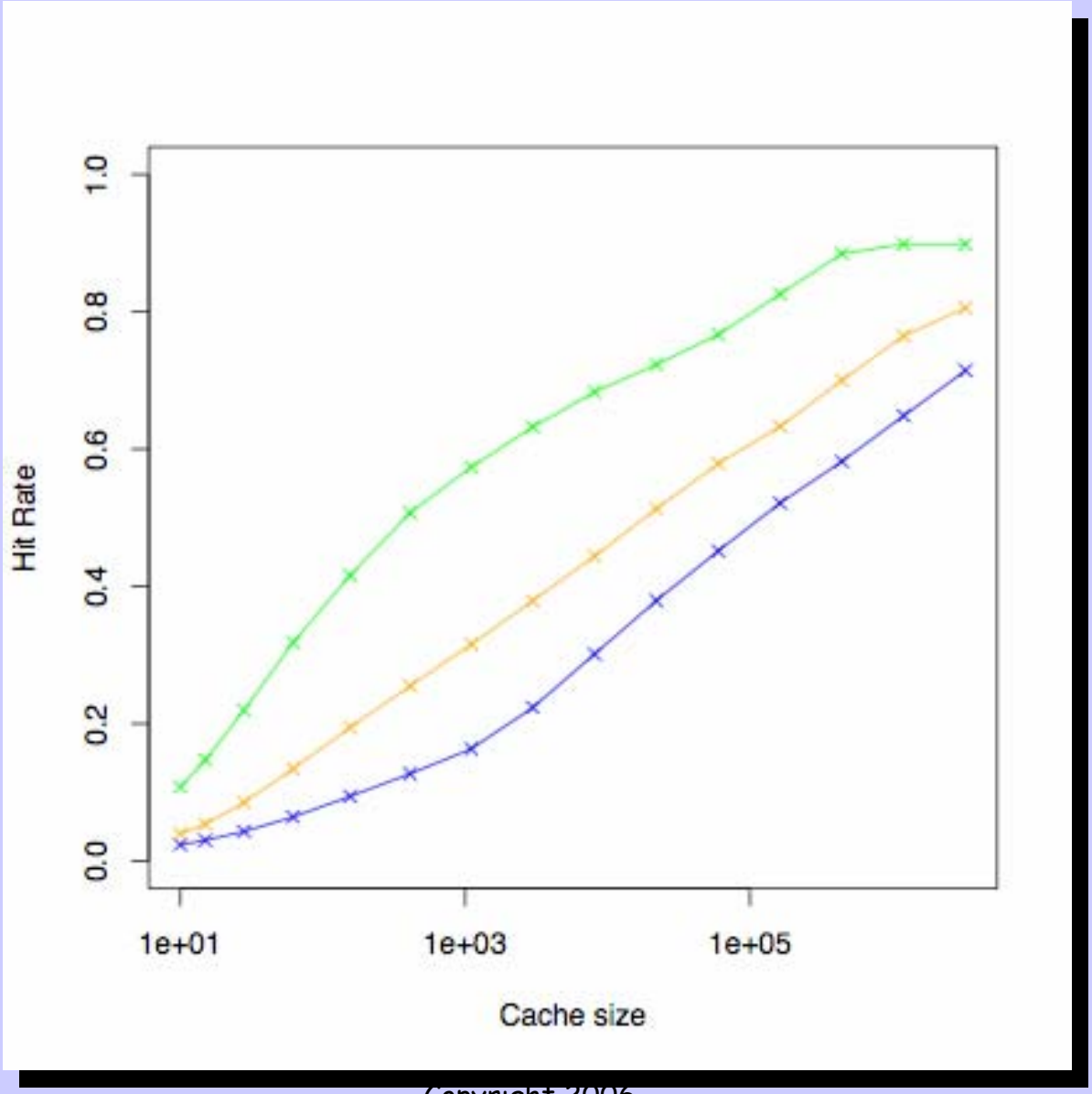
PKI Management API

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

BGP Routing Security

- PKI system will provide 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

Cache Size vs. Hit Rate



Thanks to Our Kind Sponsors & Clue-Givers

Geoff, George, & APNIC

Internet Initiative Japan

NSF via award ANI-0221435

Steve Bellovin & JI