Progress Report on the ISP & RIR PKI

LACNIX / Isla Margarita

2007.05.23

Randy Bush <randy@psg.com>

Serious Problems!

- '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

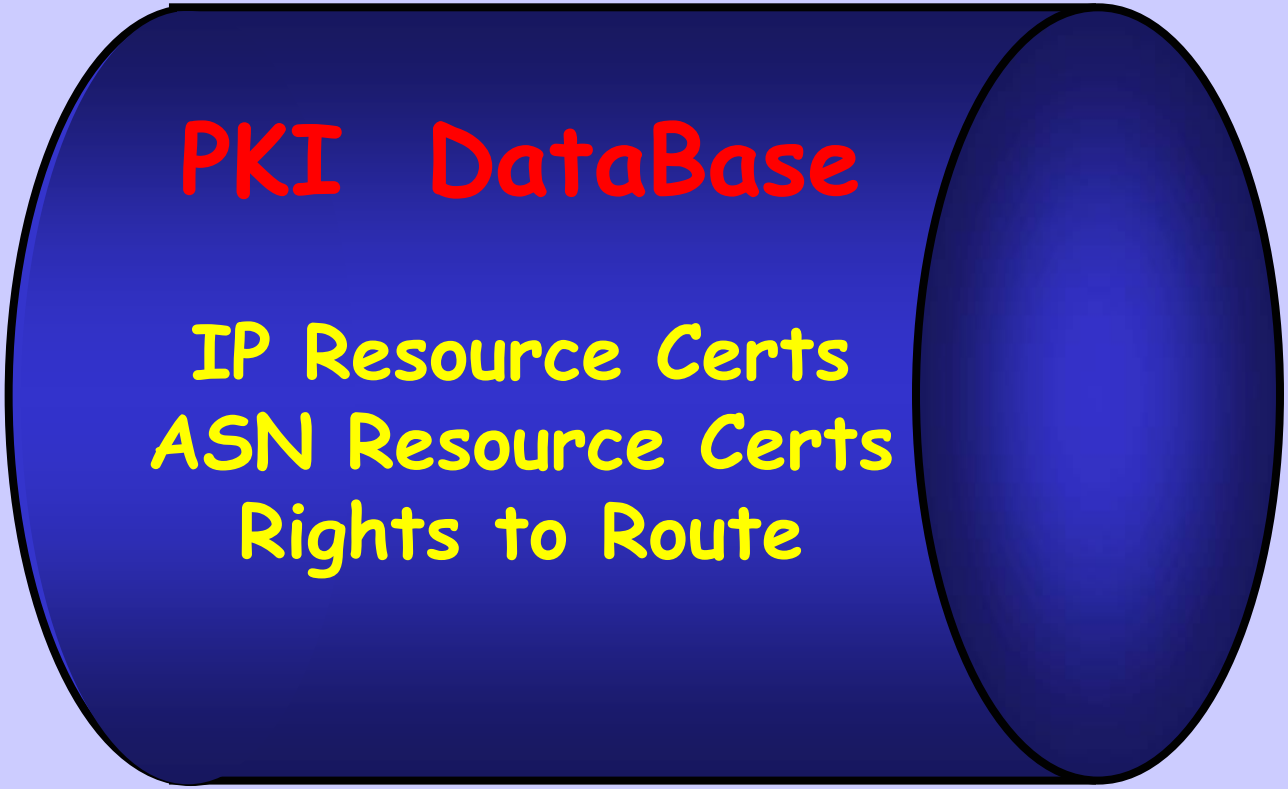
Formal Requirements

- Formally verifiable assertions of rights in IP Address Space and ASNs
- Formally verifiable assertions of rights of ASNs to originate prefixes
- Formally verifiable assertions of the correctness of routing announcements
- Formally verifiable Assignment, Transfer, … of IP prefixes and ASNs

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 verifiable transactions with others:
  - Allocation
  - Sub-Delegation
  - Transfer, Trade, Sale, …!

The Approach

- Components
  - Use X.509 v3 Public Key Certificates with IP Address and ASN Extensions (RFC 3779)
  - Use Existing Technology where possible
  - Leverage existing Open Source software, tools, and deployed systems
  - Contribute to Open Source solutions
- OpenSSL as the foundation platform
  - Add RFC 3779 Extensions for IPs and ASNs
- Certification framework anchored on the IP resource distribution function

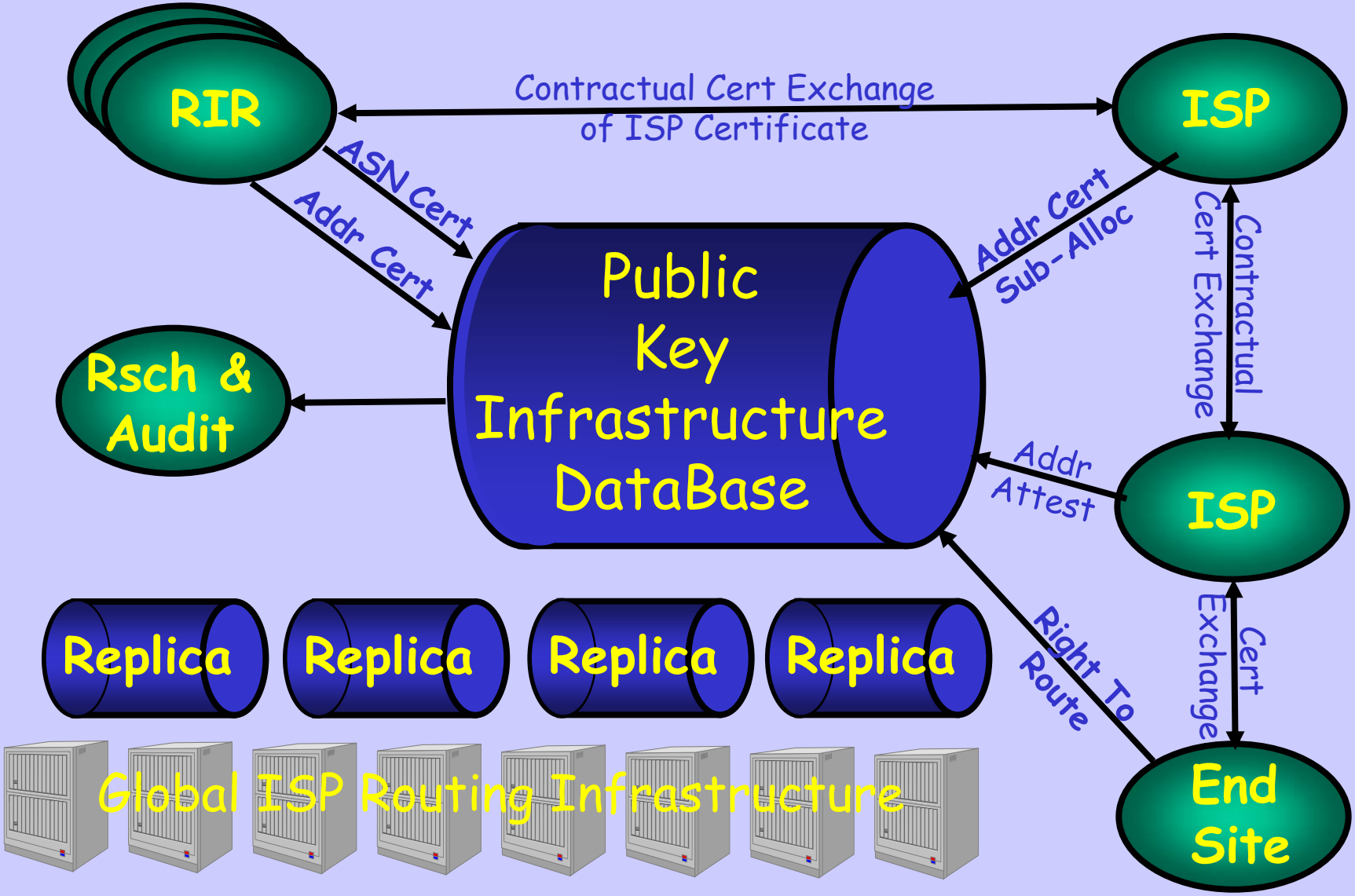
Operate Across RIRs

- 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

PKI Interfaces/Users



IANA/RIR Identity

- IANA/RIR generate 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, …

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

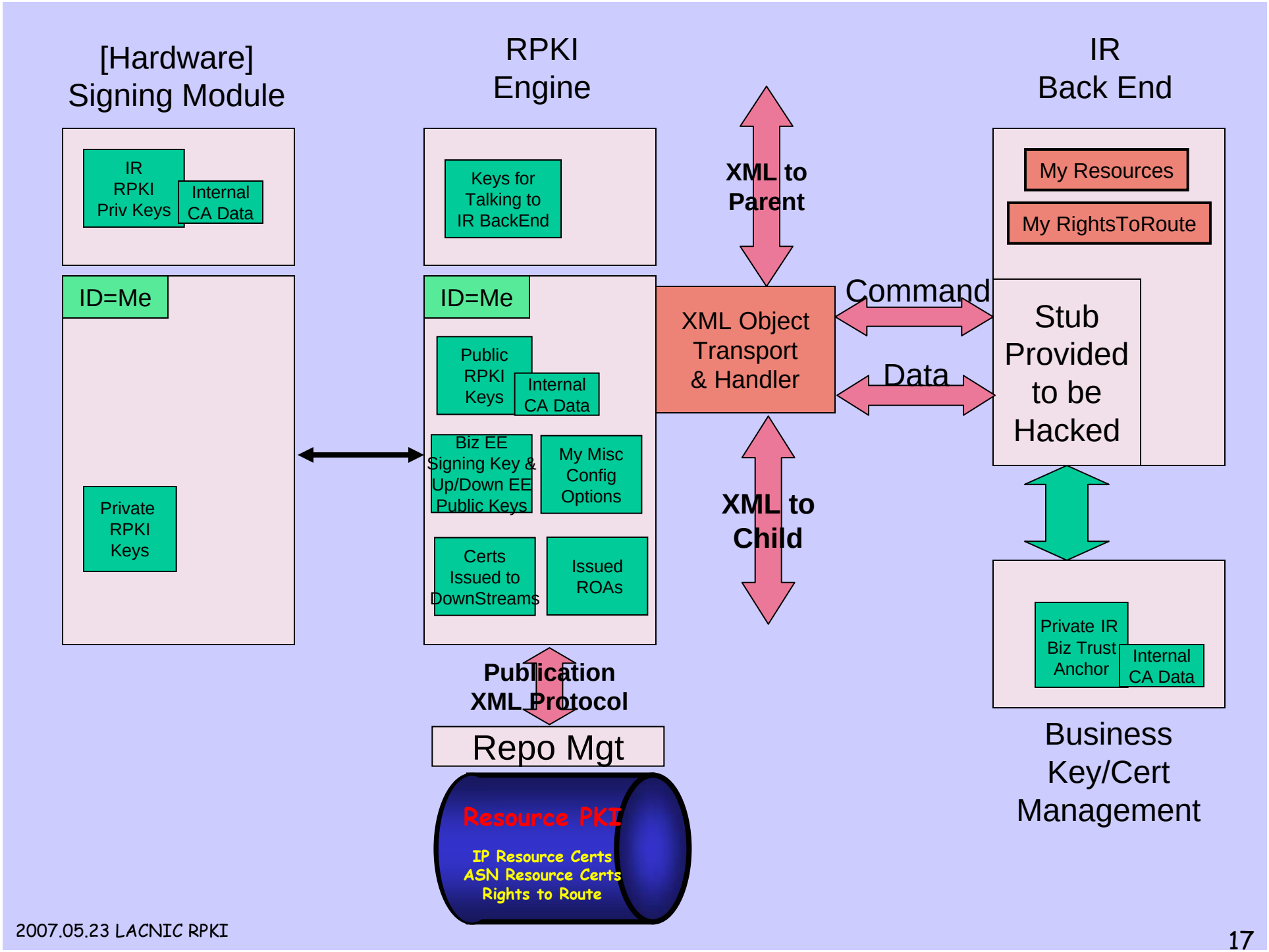
- RIR allocates to ISP
  S.*rir* (192.168/16, *isp*)
- ISP allocates to Downstream
  S.*isp* (192.168.128/17, *dstr*)
- Downstream allocates to User
  S.*dstr* (192.168.142/24, *user*)
- Anyone can verify it all, because the public keys *rir*, *isp*, *dstr*, and *user* are in the public PKI

Business Certificates

- RIRs generate business 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 sign transport of 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

Underlying Certificate PKI Architecture

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


[Hardware]
Signing Module
IR
RPKI
Priv Keys
Internal
CA Data
ID=Me
Private
RPKI
Keys
RPKI
Engine
Keys for
Talking to
IR BackEnd
ID=Me
Public
RPKI
Keys
Internal
CA Data
Biz EE
Signing Key &
Up/Down EE
Public Keys
My Misc
Config
Options
Certs
Issued to
DownStreams
Issued
ROAs
XML to
Parent
XML Object
Transport
& Handler
XML to
Child
Command
Data
IR
Back End
My Resources
My RightsToRoute
Stub
Provided
to be
Hacked
Private IR
Biz Trust
Anchor
Internal
CA Data
Business
Key/Cert
Management
Publication
XML Protocol
Repo Mgt
Resource PKI
IP Resource Certs
ASN Resource Certs
Rights to Route

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
- Run and Manage a Repository

Tools for ISPs

- Acquire business certs from RIRs
- Generate IP and ASN requests to RIRs and Upstreams
- Generate biz certs for customer ISPs and End-User sites
- Validate resource certificates
- Run and Manage a Repository

State of Play

- APNIC did a simple prototype
- OpenSSL 3779 done by ARIN
- Distributed repository done by ARIN
- R&D teams almost finished with multi-RIR and ISP/user protocols
- APNIC & ARIN driving the protocol, designs, model, essentially XML/CMS
- The result are all open source

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

ARIN, for continuing support of Research and Development

APNIC, RIPE, LACNIC, AfriNIC

Internet Initiative Japan

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