DNSSEC Impact on Registries

Edward Lewis, Neustar

Jakob Schlyter, .SE

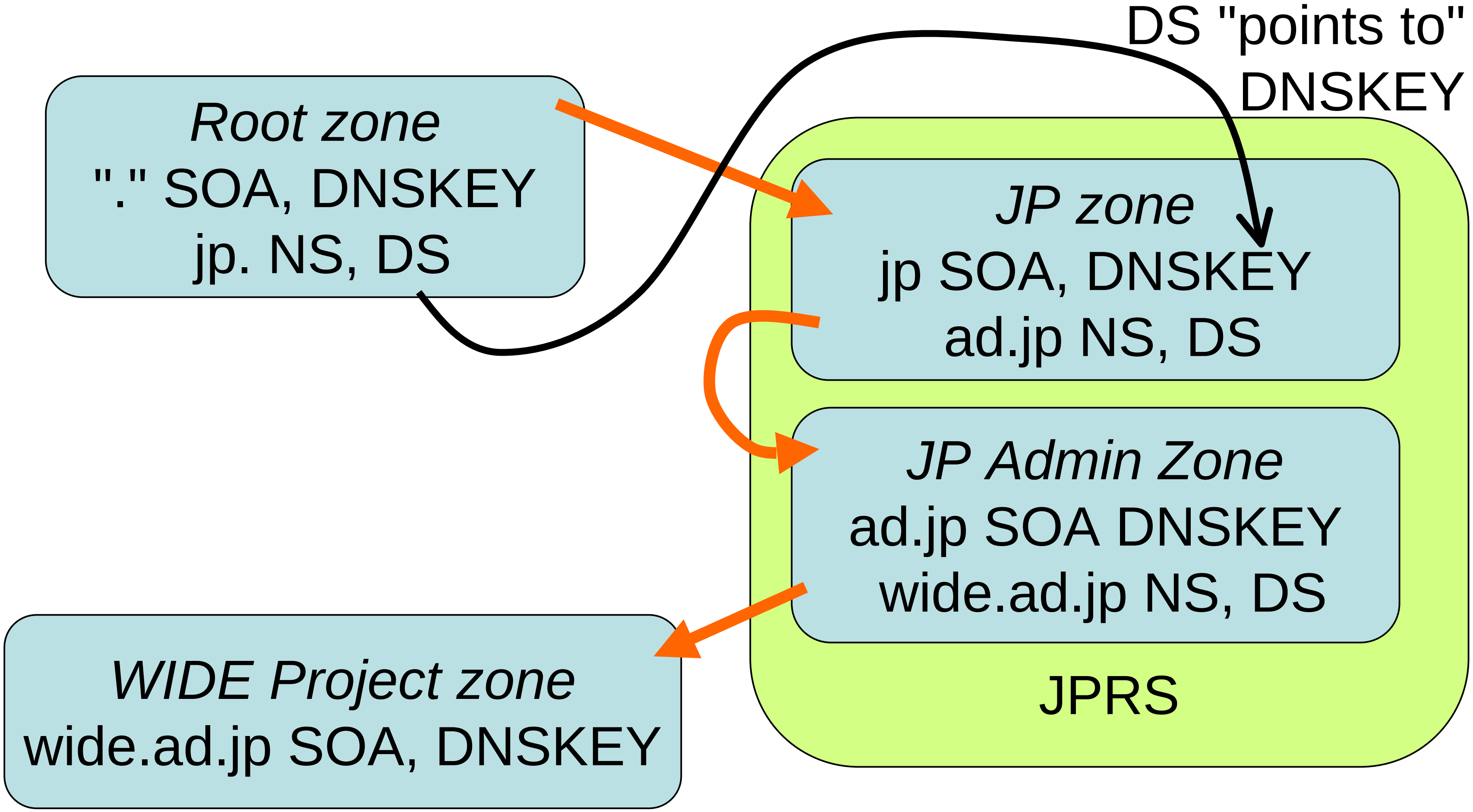
Agenda

- What is a Registry, how is it run?
- Steps Towards Internal DNSSEC
- Steps Towards External DNSSEC
- Tough Issues

Registries & DNSSEC

- Why cover this topic?
- DNSSEC needs a hierarchy of public keys
  - Root covers TLD
  - TLD covers next level, …
  - downward to data
- Registries enable building the hierarchy

DNS tree and DNSSEC



DS "points to" DNSKEY

Root zone
"." SOA, DNSKEY
jp. NS, DS

JP zone
jp SOA, DNSKEY
ad.jp NS, DS

JP Admin Zone
ad.jp SOA DNSKEY
wide.ad.jp NS, DS

JPRS

WIDE Project zone
wide.ad.jp SOA, DNSKEY

What is a Registry?

Registries come in many forms:

- Name Registry, e.g., .edu, .jp, .kr, .cn, .tw
- Number Registry, e.g., APNIC
- Routing Registry, e.g., RADB
- Non-Internet Registries too

- We will stay with name registries and number registries ("Internet registries")

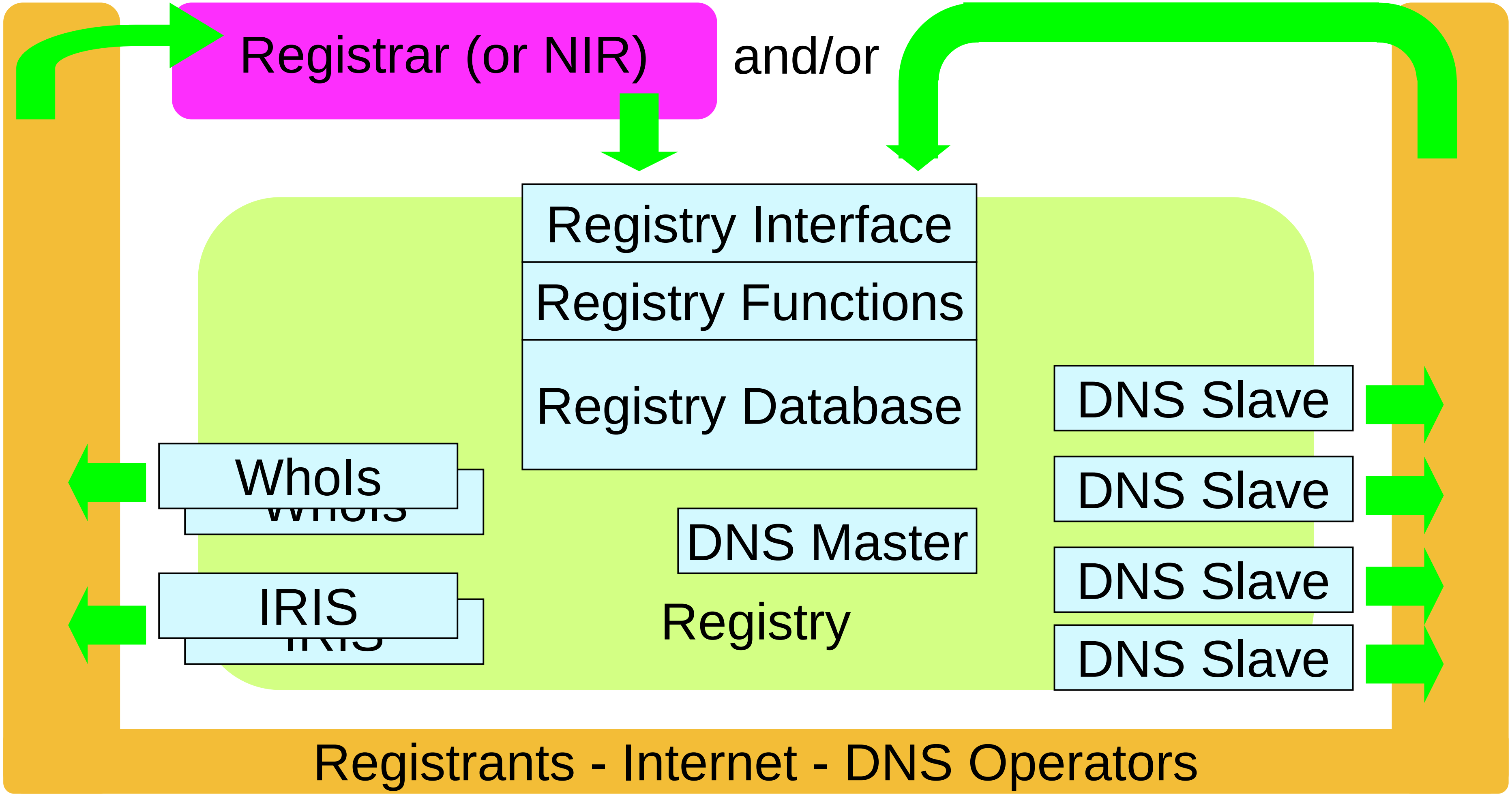
Others Involved

- Registrant = Whoever gets the name or address space
- DNS Operator = Whoever runs the DNS for the Registrant (sometimes the same)
- Registrar = A “retailer” for some Registries

Registry Environment

- The job of a registry is to relate resource (domain) to a user (registrant)
- Registries get requests
  - Directly from Registrants (and/or)
  - Indirectly via Registrars
- Registries supply publication services
  - WhoIs, IRIS, DNS, sometimes routing

Registry Context



Registrar (or NIR)

and/or

Registry Interface

Registry Functions

Registry Database

DNS Master

Registry

WhoIs

WhoIs

IRIS

IRIS

DNS Slave

DNS Slave

DNS Slave

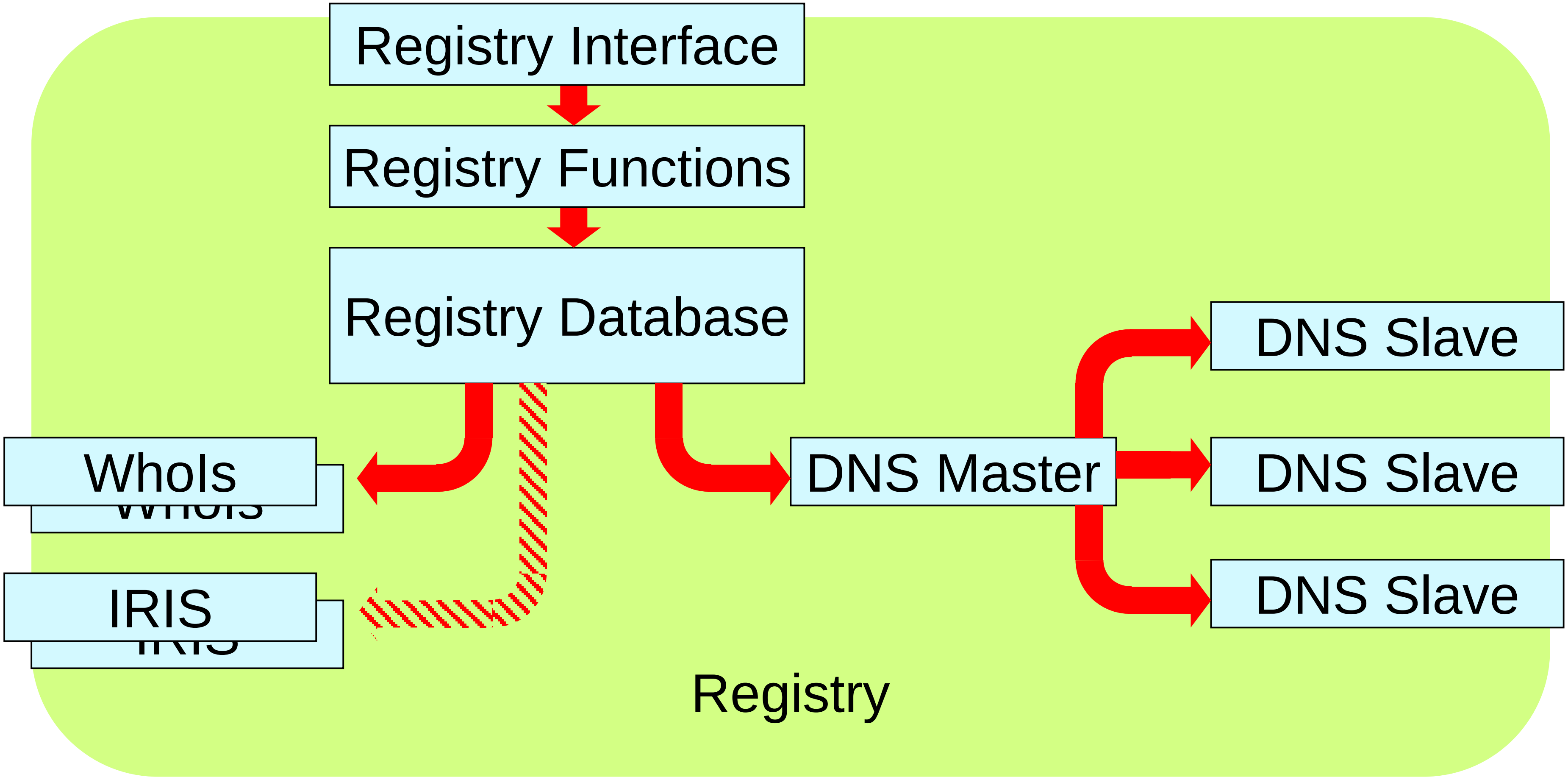
DNS Slave

Registrants - Internet - DNS Operators

Components of a Registry

- Registration Service
- Information Service
- DNS Service
- The “unseen” Database
  - – “heart” of a registry

Registry Internals



Registration Interface

- Getting Data Into a Registry
- The “Front Office”
- Important to DNSSEC
  - – This is how DNSSEC data will enter

Registry Functions

- Registries have business rules
  - Billing for actions
    - Is there money in an account?
  - Checks on registered data
    - Is the registration authentic? Authorized?
    - Are there 2-13 name servers?
    - Is the requested name appropriate?

Registration Database

- Tracks all data registered
  - Besides names, there is billing information, contact information, DNS servers, and more
  - Will need to store DNSSEC data too

Information Service

- WhoIs (now), IRIS coming/may come
- Displays information about a registration
  - Gives the contact for a domain name
  - Gives the contact for an IP address
- Might display DNSSEC data

Domain Name Service

- For a “name registry” this is the most vital operational service
- Usually - hidden master, publicly accessible slave servers
- DNSSEC will add new record types
  - DNSKEY, RRSIG, NSEC, and DS

Modes of Operation

- Direct or Indirect Relationships
  - Registrars?
- Registration Style and Protocol
  - Interactive or batch?
- DNS Update Frequency
  - Immediate or, say, daily updates?

Environment

- Registries may interact with the public directly (for registrations)
- Some registries follow a “shared registry model”
  - Registrars provide interface
- RIRs and NIRs are a mixture of both

Direct Interface

- A registrant (“buyer of a name”) will contact the registry
- This is an “open to all” arrangement
- This is the original style of Internet registries
- Impact to DNSSEC
  - Direct contact between registry and registrant

Registrars

- “Retailers” of domain names
- Registrars will handle DNSSEC data
  - Need to add DNSSEC to registration requests
  - Will increase number of requests
- Registrars may bundle services, including DNS operations

Registration Interface

- How is it transferred?
- What is "it"?
  - DNSKEY appears in Registrant's zone
  - DS appears in Registry
  - What gets passed?

DNSKEY vs DS

- A DS RR is made from a DNSKEY
  - – DS RR holds a hash of the DNSKEY
- Who performs the hash function?
  - – Registrant/Registrar?
  - – Registry?
- This is a significant design choice
  - – Will address this on EPP slide

Asynchronous (Email)

- Some registries use formal template messages sent via SMTP
- Work flow is managed in mail folders
- Interface is "store and forward" not interactive
- This kind of interface is hindered by spam volume

Client-Server

- These interfaces consist of client software to send messages to a server
- Registries using this need to distribute software to registrants or registrars (more common)
- Security arrangements are usually pre-determined (certificates)

RRP, others

- Registry-Registrar Protocol
- Developed by Verisign
- Used in .com and .net
- Led to the development of the IETF standard EPP
- Other protocols are in use, not as widespread (e.g., Payload 2.0 SRS)

Web-based

- Like mail, sometimes layered on mail
- Because web clients are anonymous these make use of certificates for identification and authentication
- This makes them behave less like mail interfaces and more like client-server
  - There is a prearranged agreement in place

EPP

- Extensible Provisioning Protocol
- IETF Proposed Standard, documented in 2004
  - RFC numbers 3730 thru 3735
- XML based, runs over TLS
- Written in context of a shared registry model (registrars)

EPP and DNSSEC

- EPP is extensible
- IETF draft document for inclusion of DNSSEC
  - draft-hollenbeck-epp-secdns-06.txt
  - http://www.ietf.org/internet-drafts/
  - "-06" will increment from time to time
- Tests are being conducted with this definition

EPP on "DNSKEY vs DS"

- EPP is leaning towards the transmission of the DS as the primary means of registering DNSSEC data
- The rationale is
  - Simplifies the registry, core functions
- DNSKEY is an optional feature of DS
  - In case a registry wants to collect it

EPP-SECDNS Field Test

- A short-term trial conducted in November 2004
- Registrar-Registry
  - Alice's Registry <-> NeuStar
  - dnssectrial.us was the test zone
- Worked, comments supplied were fed into the current draft

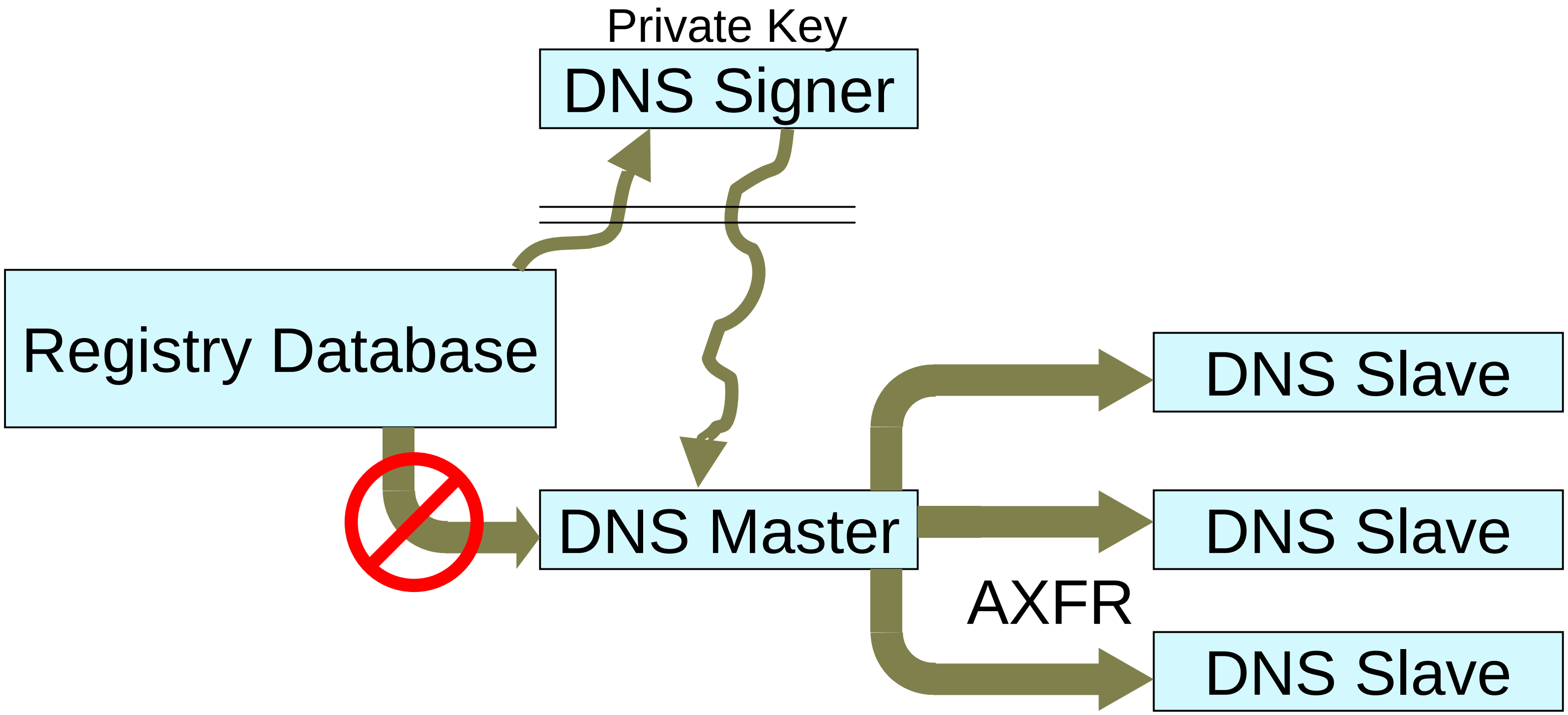
Frequency of DNS Updates

- DNSSEC is defined to allow the signing process to be off-line
- This was done when updates were done once or twice a day
  - Time enough to transfer files over "air-gap"
- Modern registries update DNS in minutes of a name's registration

Batch Updates

- If a zone is updated only a few times a day
  - "Dump" the zone file from the database
  - Sign the zone file, off-line
  - Push the zone file to DNS servers
- The major decision is whether the whole zone is signed or are signatures "recycled"

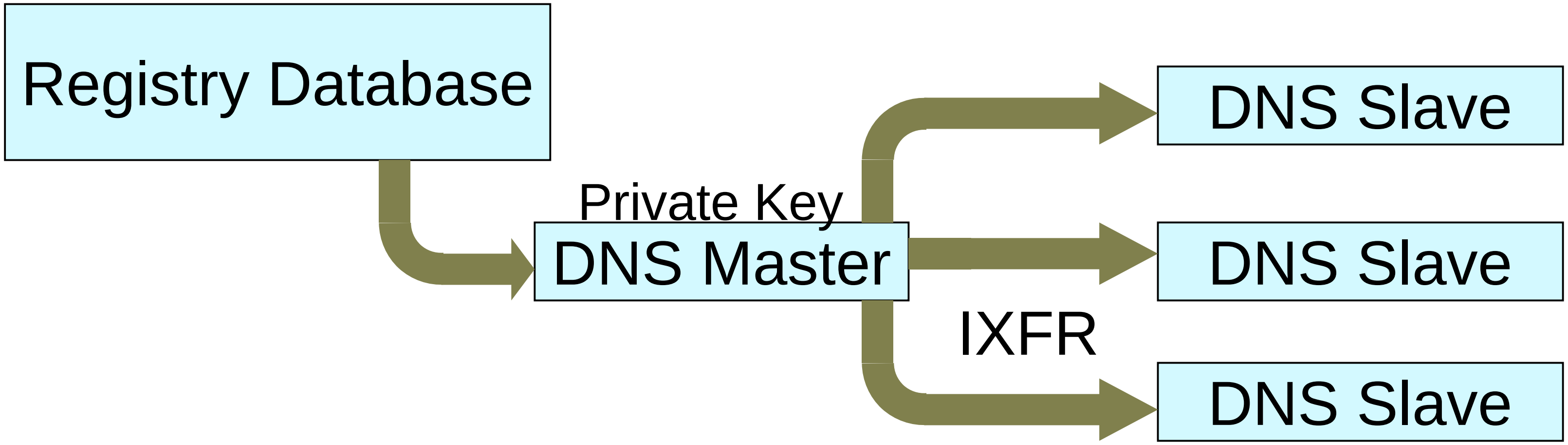
Off-line, batch signing



Incremental Updates

- Quickly-refreshed, large zones need to make use of incremental updates
  - If one name is added to a million name zone, you'd rather ship the new name around, not the million + one names
- DNS has two incremental updates
  - Dynamic Update
  - Incremental Zone Transfer

Dynamic Signing



Registry Database

Private Key

DNS Master

DNS Slave

DNS Slave

DNS Slave

IXFR

Steps Towards DNSSEC

- Internal Deployment
  - Setting up key management procedures
  - Signing the zone like a registrant would
- Opening for Registration
  - Accept DS or DNSKEY records
  - Sign those into the zone
  - A new "service"

Signing the Registry Zone File

- Steps
  - Key Management plan
  - Signing the zone
  - "Recycling" signatures and incremental signing
  - Securely transferring the zone from master servers to slave servers

Key Management

- Public key cryptography works on key-pairs
  - Private key, held secret and signs data
  - Public key, distributed and verifies data
- Private keys need to be protected and "the wear out"
- Public keys need to be published

Private Keys

- Protection is important
  - Anything verified by the public key is tied back to this key
- Lifetime
  - The more often a key is used, the easier someone can "guess" it
  - A guessed (or exposed/stolen) key is "worse than worthless"

Public keys

- Needs to be available to all who verify signatures
- Widespread distribution
  - Where ever it is needed, on-demand
- Reliable distribution
  - Make it harder for "false" public keys

ZSK and KSK

- Operational tests have lead to ZSK and KSK names for keys
- ZSK = Zone Signing Keys
  - Often used, discarded frequently
- KSK = Key Signing Keys
  - Rarely used, passed up to parent
- KSK's are what DS records point to

Zone Signing

- Starts with key management plan and a zone signer
- Need to distribute signed zone securely
- Other considerations
  - – Use of dynamic update
  - – Incremental zone updates

Zone Signer Application

- Functions
  - – Sign RRSets
    - Cryptographic operations
  - – Add NSEC (authenticated denial) records
  - – Include DS RRSets for registrants

Hardware Assist for Signing

- Protects private key
  - Key memory isn't accessible
- Speeds processing
  - Processor built for cryptography

Recycling Signatures

- Reuse of previous signatures
  - E.g., sign daily, with weekly expiration
- To do this, the output of the signer has to be fed back to the database, or otherwise used as input for the next signing operation

Zone Transfer Security

- Plain zone transfers are not secure
- Management VPN
  - Firewall or VPN client/server encrypts all traffic
- TSIG
  - DNS protocol (application level) protection

Opening Service to Registrants

- Chief service is signing delegation information
- For large zones, incremental signing is needed
- Dynamic update and incremental zone transfers are needed too

Signing Delegation Information

- Currently a registry has an NS RRSet for a domain name or names for networks
- Delegations will now feature a DS RRSet
  - Registry is authoritative source (unlike for the NS RRSet)

Incrementally Signing a Zone

- Completely signing a large zone will take a long time
  - One or two signatures per name
- Sign only what is new, what has expired
  - Means retaining old(er) signatures

Signing Dynamic Updates

- Dynamic Update can be used to push changes into DNS
  - Ought to be done securely
- Private key is needed on the "true" master server
  - Protection is an issue, workload
- Also need incremental zone update

DNSSEC Data Flows

- Registration
- Database
- Information Services
- DNS
- DNS Monitoring

Registration of DNSSEC Information

- Registration today -
  - – Name, Contact Information, Name Servers
- DNSSEC
  - – DS or DNSKEY
  - – Could also include "data lifetime"

DNSSEC in the Database

- For name registries
  - – DS or DNSKEY for each registration
  - – May be multiple keys
- For number registries
  - – DS or DNSKEY set for each reverse-map zone, not just each network

DNSSEC in Information Services

- Optional to DNSSEC
- Useful for debugging and checking registered data
- Could show any DNSKEY records collected, with just DS in zone
- Also could show any "time based" data

DNSSEC in DNS Zone File

- DNSSEC will add
  - RRSIG for top of zone RRSets (SOA, etc)
  - NSEC and RRSIG for all names in zone
  - DS and RRSIG for all names with DNSSEC in zone
- Zone file gets bigger
- Bandwidth needed gets bigger

DNSSEC “Health” Checks

- Some registries automate cleaning the DNS, e.g., lame delegation checking
- What is needed for DNSSEC?
  - – Verify that each DS RR refers to an available DNSKEY, with correct hash
  - – Verify that all DNSKEYs that are supposed to have DS records do so
- "Fixes" ought not be automatic

Protection of DNSSEC Flows

- Assuming Internal Security
  - Integrity of the internal components of a registry is important, but assumed here
- Securing Input
  - Is registration authentic and authorized?
- Securing Output
  - Is published data protected?

Securing the Registration Interface

- Authentication
  - Verify that the registration request is from the entity that is named in the request
  - Is the registrant really the registrant?
- Authorization
  - Is the registration request to be allowed?

Securing the DNS Zone File

- Database to Hidden master
  - Done on a protected network
  - Incremental updates can be protected with Secure Dynamic Update
- Hidden master to slave servers
  - VPN, encrypted tunnels
  - TSIG protection of AXFR and IXFR

Performance Burden of DNSSEC

- Data Held and Produced
  - – This will impact the interface to registrants and registrars
  - – Also internal data capacity
- Data Transferred
  - – This will impact the data published by a registry to the general Internet

Demand on a Registry

- Sources of demand
  - Registration requests
    - DNSSEC key refreshes will raise this
  - Amount of data held
    - DS records will add to this, DNSKEYs ever more so
  - Internet traffic
    - Internet activity is not related to registrations

Volume of Data Held in Database

- Per object transactions increase as keys are refreshed
  - Change more than name servers
- Data stored also increases
  - Maybe 100's-1000's of bytes per object
  - But multiply that times number of objects
- More data to backup, transfer, etc.

Volume of Data Held in Zone File

- Zone files grow considerably
- Incremental updating is needed
- Memory use by (some) name servers is a limitation

Bandwidth Impacts

- DNSSEC messages are larger than DNS messages
  - Must use EDNS0
- Also more frequent if verification data is needed

Tough Issues for Registries

- Non-technical considerations
- Deploy? When?
- Making it payoff

Balance Stability & Innovation

- Registries play key role in Internet
  - Rocking the boat has large ripple effects
  - For operations "as expected" is better than "an adventure"
- But innovations in Internet need improvements at registries
  - Internet is not "done"
  - Needs security, other features

Need for Stability

- Stability is important
  - With a solid foundation, other components can innovate
  - Protocols are sensitive to changes in timing - TCP congestion management
- Cost efficiency is also important
  - Limits testing though

Need to Innovate

- DNSSEC is one innovation
  - Supplements overall security
  - Payoff if the top of the tree is signed, i.e., the root, TLDs, second level domains
- Other innovations
  - IPSEC, Internationalized (non-ASCII) Domain Names

What to do?

- Registries need to participate in workshops, test environments
  - Not alone and not just other registries, but in collaboration with community
- Registries need to carefully manage innovation
  - It is just a hard job

DNSSEC Payoff

- Chicken-and-Egg problem
- Enabling Registration

Chicken-and-Egg

- Which came first, chicken or the egg?
- Which comes first, a DNSSEC registry or a DNSSEC application?
- DNSSEC applications are in the works
  - IPSEC Key and SSH Keys
  - But no substantial payoff until there are DNSSEC registries

Enabling Registrants

- The reason for registries to pursue DNSSEC now
  - Shapes the protocol for operational efficiency
  - Enables registrants to make use of DNSSEC applications
  - Fosters development of other applications
- Balanced against stability, of course

Conclusion

- Status of the DNSSEC Specification
- Testing Plans
- EPP work

DNSSEC Document Status

- In RFC Editor Queue as of Feb 4:
  - http://www.ietf.org/internet-drafts/
    - draft-ietf-dnsext-dnssec-intro-13.txt
    - draft-ietf-dnsext-dnssec-records-11.txt
    - draft-ietf-dnsext-dnssec-protocol-09.txt
- Waiting for Proposed Standard publication

DNSSEC Resources

- http://dnssec.net/
  - Links to many resources, deployment plans
- http://dnssec-deployment.org/
  - New website, group pushing for DNSSEC adoption

Presenters

- Edward Lewis
  - ed.lewis @ neustar.biz
- Jakob Schlyter
  - jakob @ rfc.se

Questions?

- We are open for discussion…