High-Level Awareness of DNSSEC

Andy Linton asjl@nsrc.org

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Objectives

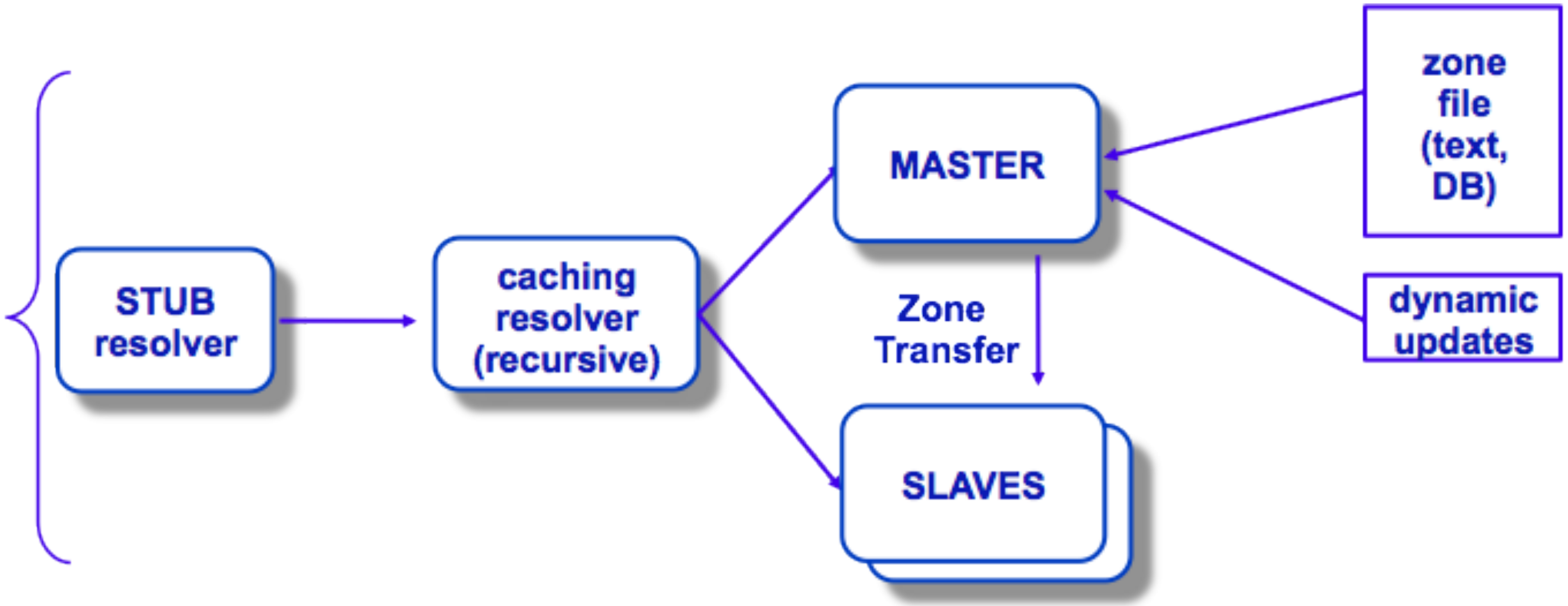
- Understand DNSSEC terminology
- Understand the threat models that DNSSEC is intended to address
- Appreciate the benefits of DNSSEC to sensitive applications
- Understand some of the operational and legal implications of DNSSEC

DNS Refresher

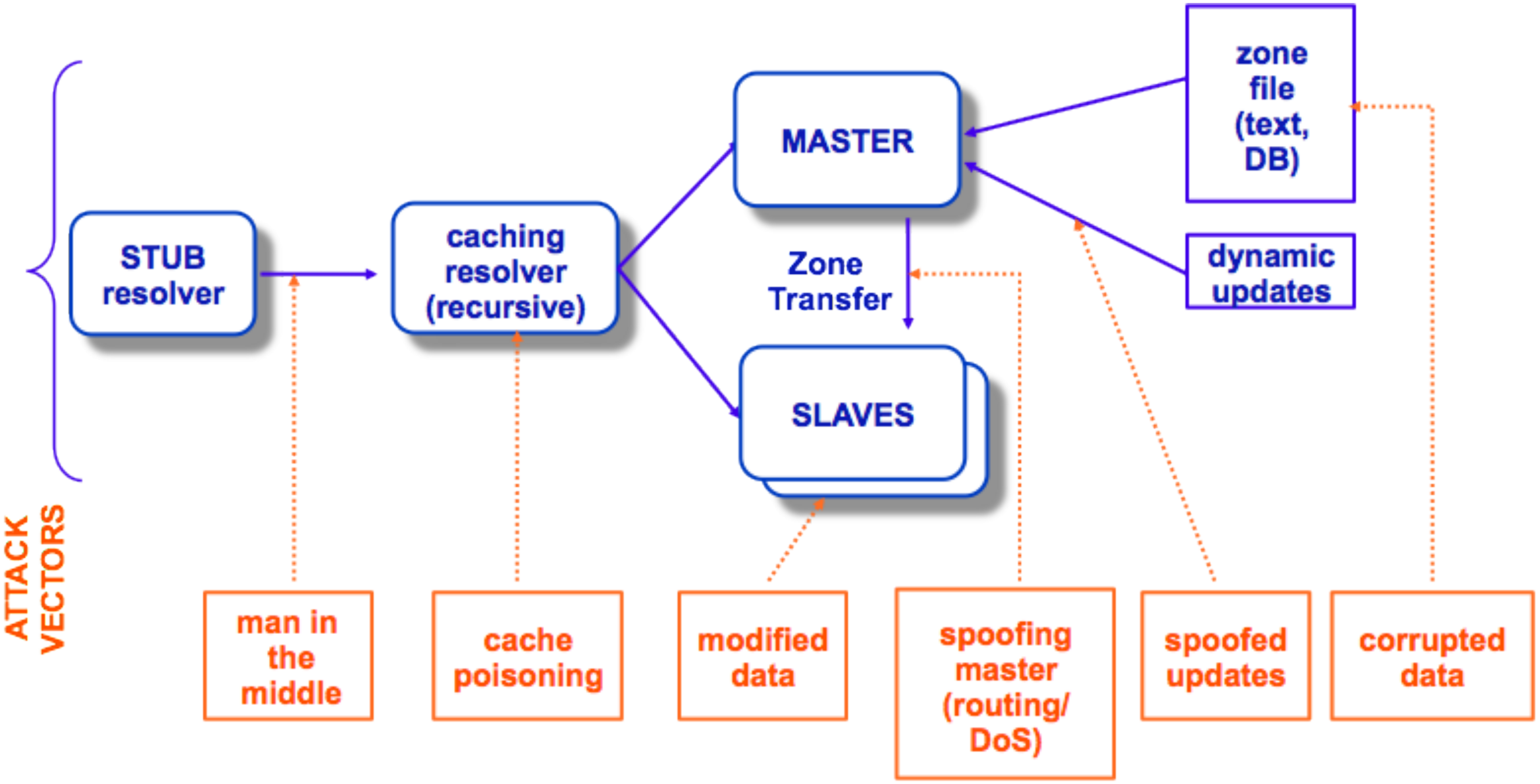
DNS Overview

- What is the DNS?
- What applications depend on the stable and secure operation of the DNS?
- What are the implications of a failure in DNS operations?

DNS Data Flow



DNS Vulnerabilities



DNS Vulnerabilities

DNS Vulnerabilities

- Cache-poisoning
- DNS interception
- Confidentiality
- Reliability
- Integrity
- Reflection attacks

Which of these does DNSSEC address?

Reflection Attacks

- DNS servers can act as very efficient packet amplifiers
  - Use of UDP, small queries, large responses
- DNSSEC makes DNS servers *better* packet amplifiers
  - Still lots of UDP, larger responses

Reliability

- In the grand scheme of things, DNSSEC does not help make your DNS more reliable
  - in fact it makes the DNS more brittle, and makes it harder to maintain reliable service

Confidentiality

- DNSSEC does not address confidentiality of queries or responses
  - anybody who can intercept a secure response can still see the details
  - there is no *encryption* here

Integrity, Authenticity

- DNSSEC provides a mechanism for *data* published in the DNS to carry cryptographic signatures
  - secure responses include signatures
  - clients receiving a secure response can tell whether it is authentic

Benefits of DNSSEC

Benefits to End-Users

- Users who validate will not see answers from the DNS that fail validation
  - might increase helpdesk load, but the alternative is infected computers, stolen bank details, etc
- Ongoing work to improve SSL security using DNSSEC-signed certificates
  - IETF “dane” working group

Benefits to Content Providers

- Reduce the risk that your content is being intercepted by unknown third parties
  - for end-users that validate, at least
- Demonstrate technical proficiency and security awareness

Three Slides about Cryptography

Cryptography

- Public Key Cryptography
  - X.509, PGP, ssh, DNSSEC
- (Public, Private) Key Pairs
  - use the private key to sign data
  - use the public key to verify signature

Private Key

- The private key needs to be kept private and secure
  - the degree of security depends on what the key is used for
  - a compromised key means you can no longer expect people to trust signatures
  - a signature from a compromised key is more dangerous than no signature at all

Public Key

- The public key needs to be widely-distributed
    - it also needs to be accurate
- In DNSSEC, public keys are published as DNSKEY RRSets in the zone they are used to sign
- Trust anchors are published in the parent zone as DS RRSets

DNSSEC Protocol

DNS Considerations

- When using the DNS to distribute keys, we need to remember a few things
  - the DNS is widely-distributed
  - information does not update instantaneously
  - we need to think hard about TTLs and caches when constructing a suitable policy

Public Keys in the DNS

- In DNSSEC, we distribute public keys in the DNS itself
  - use the DNSKEY RRSet
  - supports different key sizes, cryptographic algorithms

RR Signing in DNSSEC

- Each Resource Record Set (RRSet) can carry zero or more signatures
  - signatures appear in an RRSIG RRSet with the same owner name
  - signatures have an inception and expiry time
    - we need to re-sign regularly

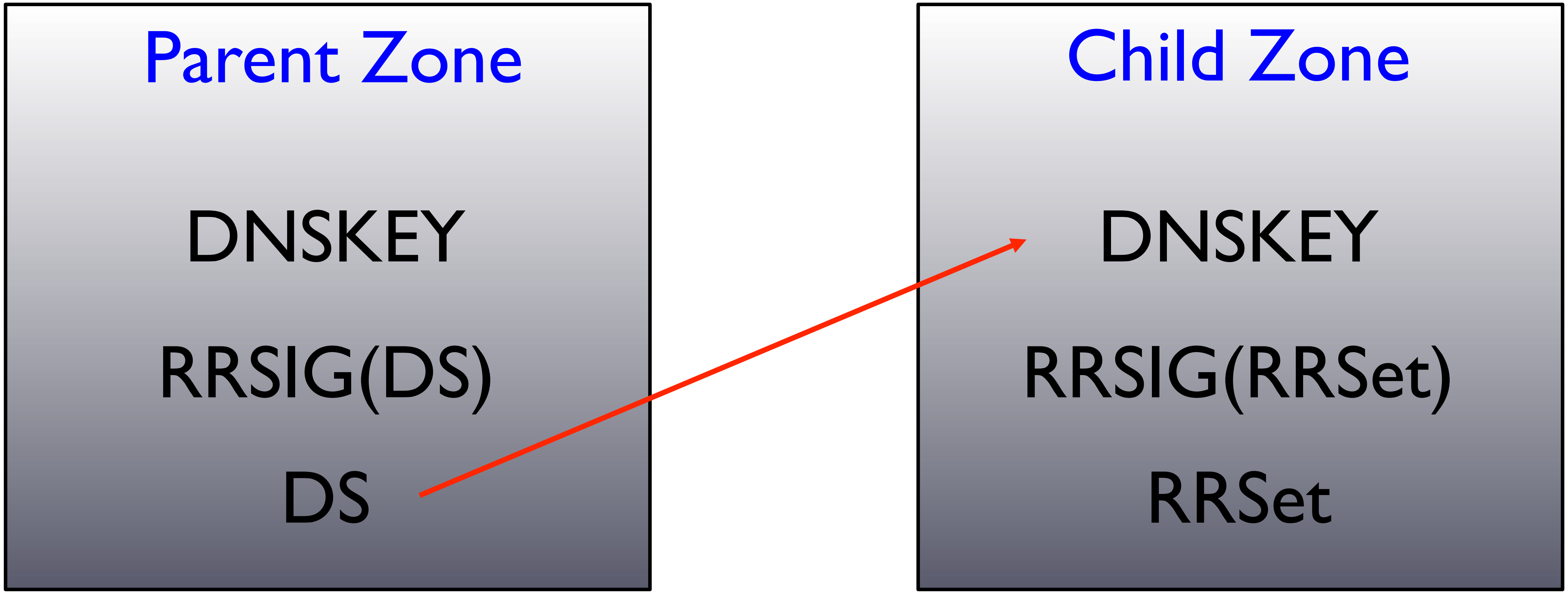
Chain of Trust

- If we can trust the public key which corresponds to the private key that made a signature, we can trust a signature
- If we can trust a signature, we can trust the data that is signed
- How do we trust the public key?

Delegation Signer

- DS is the Delegation Signer Resource Record
- it carries a hash of a public key
- it is signed
    - this is how we extend trust across delegations

Chain of Trust



Parent Zone

DNSKEY

RRSIG(DS)

DS

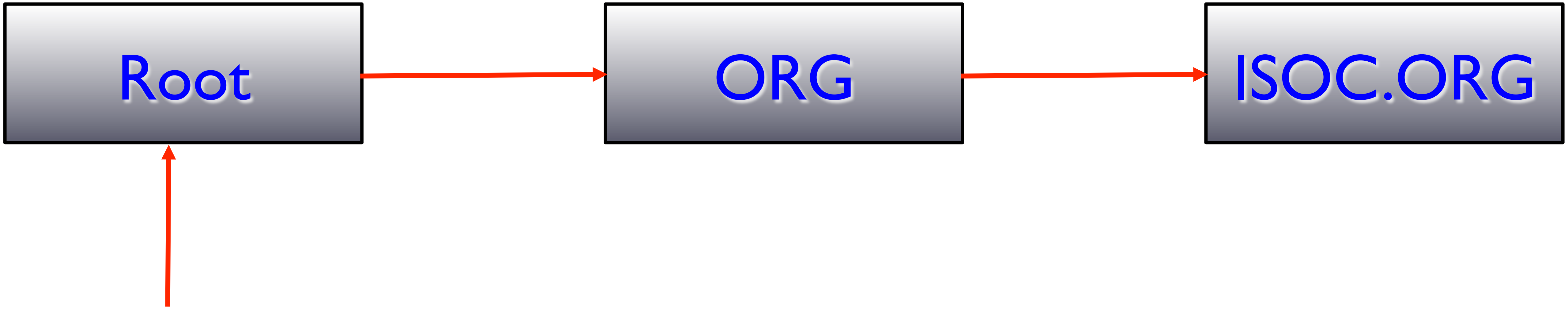
Child Zone

DNSKEY

RRSIG(RRSet)

RRSet

Chain of Trust



Root Anchor

- At some point a validator needs to install a trust anchor into its software
  - root zone trust anchor
  - http://www.iana.org/dnssec/

One DNSKEY RRSet with two keys

- Common practice in 2010 is to use two different DNSKEY RRSets per zone
  - ZSK – Zone Signing Key
    - used to sign the data in the zone
  - KSK – Key Signing Key
    - used to sign the DNSKEY RRSet

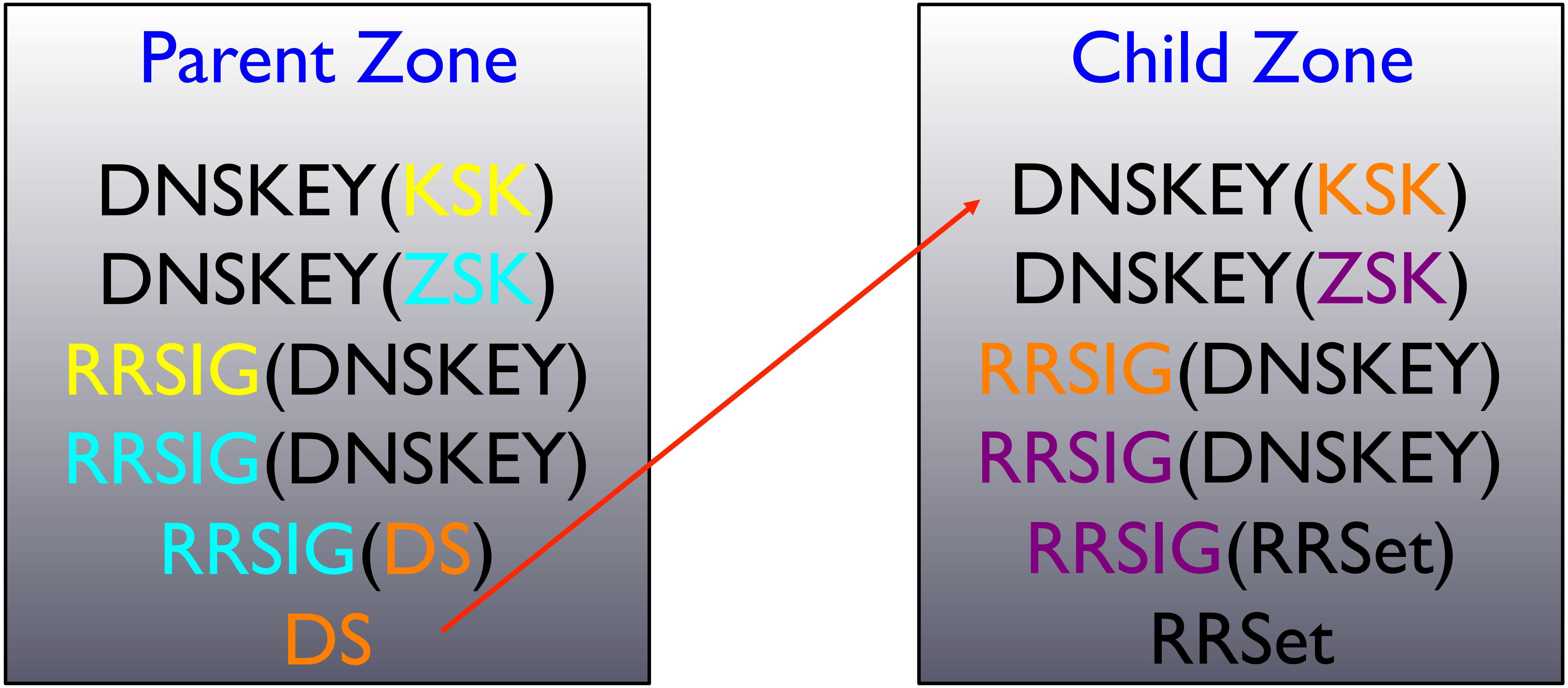
ZSK

- Since we need to re-sign the zone regularly, the ZSK needs to be on-line
- The ZSK is the key that is used most often by validators, so we can make it smaller and save some CPU
- We can change the ZSK we are using regularly without involving others

KSK

- The KSK is the key that corresponds to the DS record in our parent zone
- We need to use the KSK to sign the ZSK, and then we can put it away in a safe place
  - no need to keep the KSK on-line
  - changing the KSK involves talking to our parent (update DS record)

KSK and ZSK



Parent Zone

DNSKEY(KSK)
DNSKEY(ZSK)
RRSIG(DNSKEY)
RRSIG(DNSKEY)
RRSIG(DS)
DS

Child Zone

DNSKEY(KSK)
DNSKEY(ZSK)
RRSIG(DNSKEY)
RRSIG(DNSKEY)
RRSIG(RRSet)
RRSet

DNS Transport

- Plain old DNS was optimised to work over UDP with small packets (512 bytes)
  - fall-back to TCP
- Modern DNS supports larger messages over UDP (EDNS0, RFC 2671)
- DNSSEC means larger DNS messages
  - beware of faulty assumptions in firewalls!
    - Cisco PIXes and ASA can still cause problems with ”fixup”

Signing Things that Are Not There

- Verifiable deniability of existence
  - you can’t sign something that’s not there
  - use NSEC or NSEC3 records to cover the gaps
  - sign the NSEC and NSEC3 records
    - More on this later...

DNSSEC for ISPs

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Validate

- The most effective step you can take to encourage DNSSEC uptake as an ISP is to validate responses
  - DNSSEC-signed zones are fairly new, so expect this to cause some non-zero (but manageable) amount of helpdesk load
  - Comcast is an example of a large ISP (in the US) who has taken this step

DNSSEC for Registries and Hosting Providers

Sign your Zones

- All the zones you serve can be signed
  - think about key rollover
  - think about key compromise scenarios, and what processes you will follow when you detect them
  - think about how you can detect compromises, and monitor signatures

Key Management

- need to implement secure key storage, management procedures
- need to sign your zones
- registries need to accept DS records from users (how?)
- need to publish DS records to parents (how?)

NSEC and NSEC3

- If you’re signing a zone, you have to use one of these. Which one?
- Simple rule of thumb
    - if you are happy for anybody in the world to obtain a copy of your zone, and your zone is not very big, use NSEC
    - if you normally don’t allow (e.g.) zone transfers to random people, or if you have a large zone to sign, use NSEC3

Key Management

- DNSSEC has many parameters to consider, including:
  - key rollover schedule
  - signature duration
  - choosing appropriate TTL for the zone data
  - key size
- Those will be determined by your *policy*
- You must determine them for your own organisation, via a risk and operational assessment
- Don't blindly copy the policies of another organisation!

Key Management

- How do we keep the ZSK secure?
- How do we keep the KSK secure?
  - important questions
  - no simple answers here
  - requires risk analysis, consultation, maybe audit
  - again, a matter of policy
    - hybrid models possible
      - HSM for KSK, software for ZSK

Communication

- Communicate with your customers
  - explain benefits/risks of DNSSEC
- Communicate with end-users
  - demonstrate how to validate responses
  - explain operational changes (firewalls, TCP, response sizes)

Legal Aspects

Legal Aspects

- Deployment of DNSSEC involves trust in procedures and policies
  - otherwise why trust signatures?
- DNSSEC Policy and Practice Statement (DPS)
  - a public attestation of procedures and policies
  - can be used as the basis for audits

DNSSEC Practice Statements

- A Framework for DNSSEC Policies and DNSSEC Practice Statements
  - http://tools.ietf.org/html/rfc6841
- DPS for the Root Zone KSK Operator
  - https://www.iana.org/dnssec/
- Also review published DPS documents from TLDs who have already deployed DNSSEC

DPS

- .SE's DNSSEC Practice Statement
  - www.iis.se/docs/se-dnssec-dps-eng.pdf
- .CL's DNSSEC Practice Statement
  - http://www.nic.cl/dnssec/en/dps.html
- .NET DNSSEC Practice Statement
  - http://www.verisigninc.com/assets/20100925-NET+DPS-FINAL.pdf

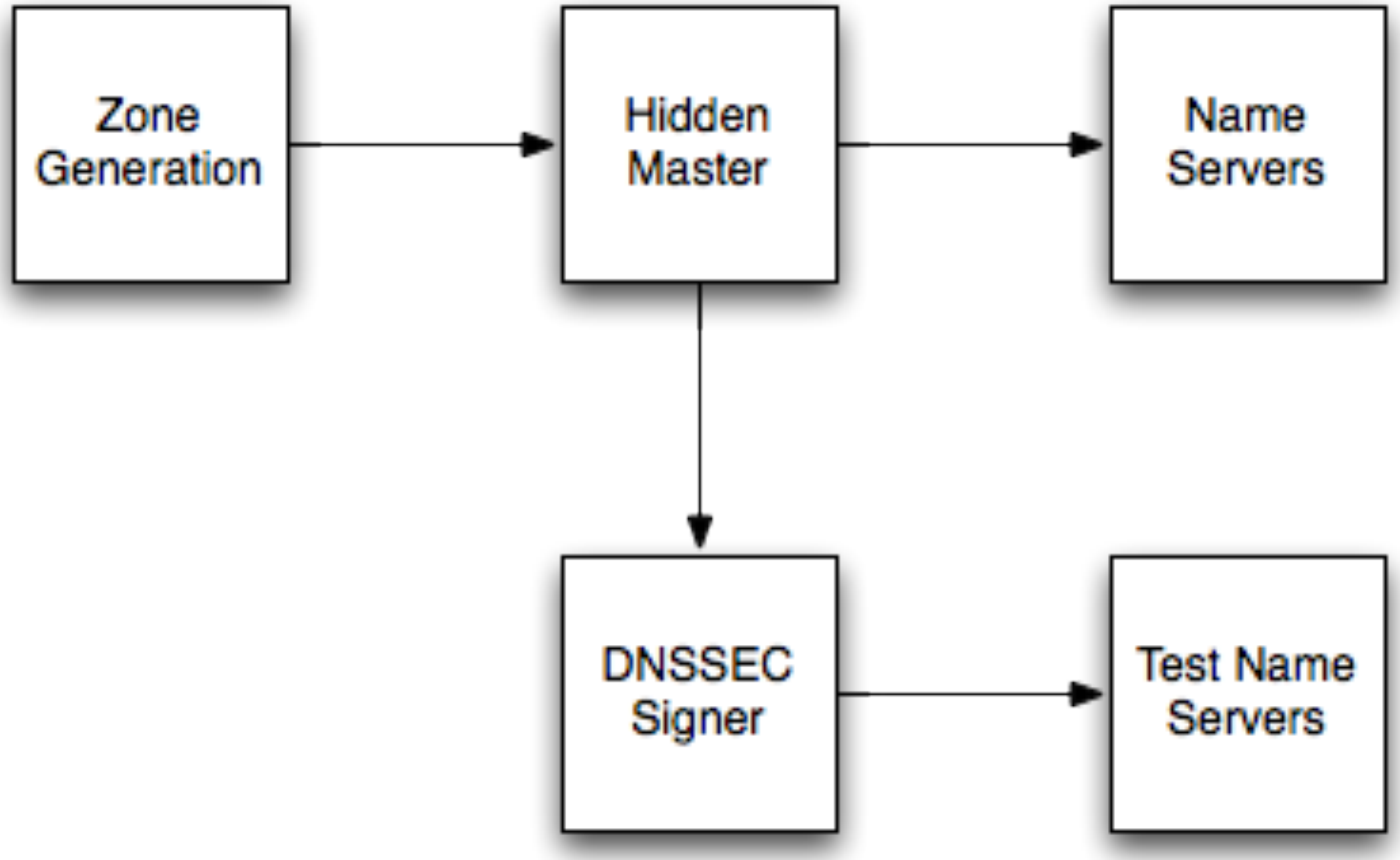
Migration Strategies for Registries and DNS Hosting Companies

UNIVERSITY OF OREGON

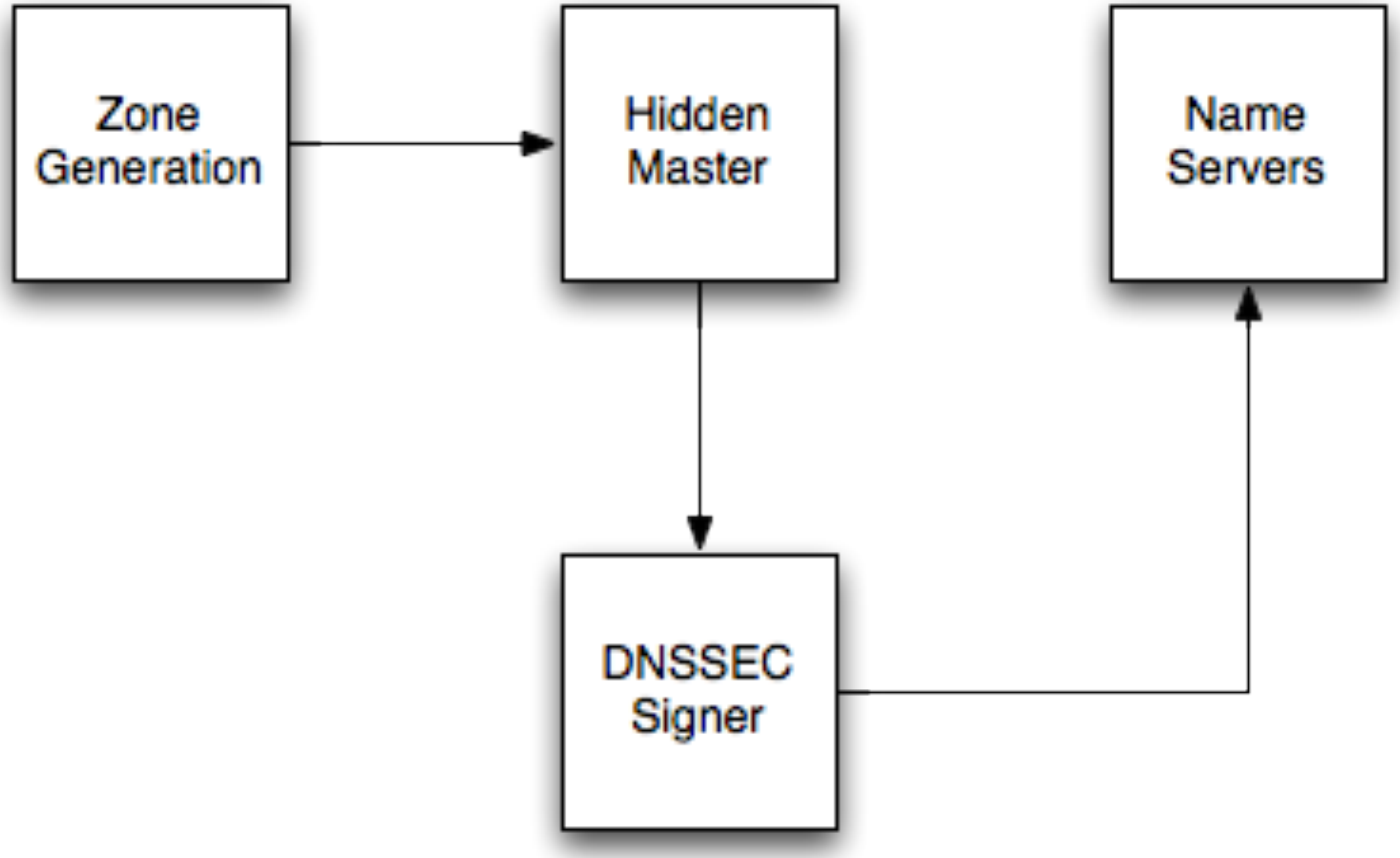
NSRC
Network Startup Resource Center

Migration

- For registries and hosting providers, DNSSEC can be deployed without radically changing your existing systems
  - registries will need to deploy a means of publishing trust anchors as DS RRSets, however



Zone Generation
Hidden Master
Name Servers
DNSSEC Signer
Test Name Servers


Zone Generation
Hidden Master
Name Servers
DNSSEC Signer

Streamlined Operations

- Remember, DNSSEC makes you zones more brittle and fragile than they were before
  - need to have excellent reliability in registry and DNS operations (verification of output, monitoring, etc...)
  - need to have emergency procedures to update DS RRSets in your zones

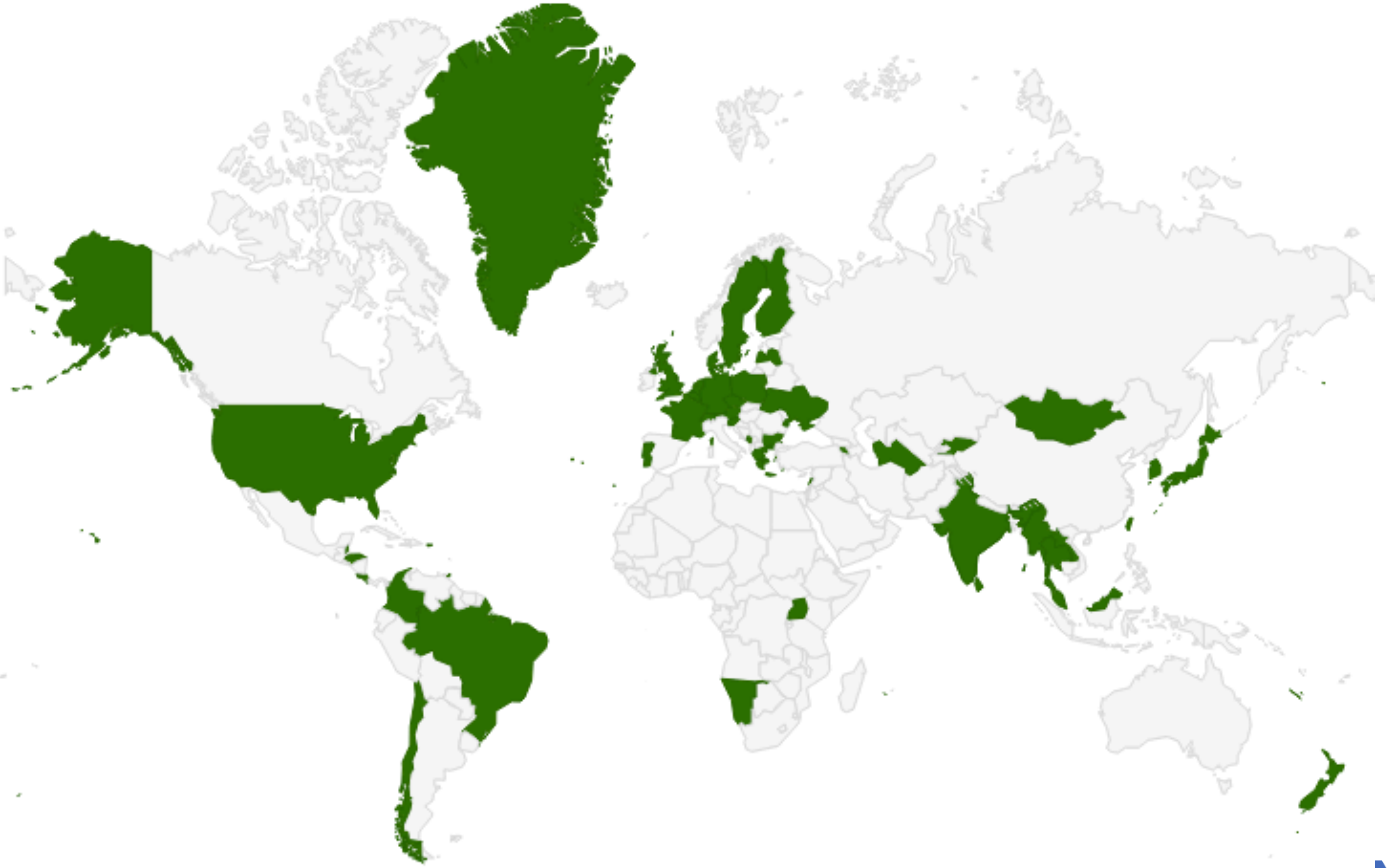
State of DNS Deployment, June 2013

Deployment

- Root zone was signed in July 2010
- 111 TLDs out of 317 are signed;
  - 107 TLDs have trust anchors published as DS records in the root zone;
  - 3 TLDs have trust anchors published in the ISC DLV Repository.
- ARPA, BE, BG, BIZ, BR, CAT, CH, CL, CZ, DK, EDU, EU, FI, FR, GOV, INFO, KG, LI, LK, MUSEUM, NA, NL, NU, NZ, ORG, PM, PR, PT, RE, SE, TF, TH, TM, UK, US, …
- http://stats.research.icann.org/dns/tld_report/

Deployment

http://www.icann.org/en/news/in-focus/dnssec/deployment-tlds



Resources

Open-Source Software

- BIND9
  - http://www.isc.org/
- NSD
  - http://www.nlnetlabs.nl/projects/nsd/
- Unbound
  - http://unbound.net/
- OpenDNSSEC
  - http://www.opendnssec.org/

Mailing Lists

- dnssec-deployment mailing list
  - http://www.dnssec-deployment.org/
- dns-operations mailing list
  - http://www.dns-oarc.net/
- Ongoing protocol work
  - IETF dnsop, dnsext working groups