DNSSEC Deployment: Big Steps Forward; Several Steps to Go

Rob Austein (sra@isc.org)

Steve Crocker (steve@shinkuro.com)

Suresh Krishnaswamy (suresh@tislabs.com)

Russ Mundy (russ@tislabs.com)

NANOG 32

DNSSEC
Deployment

REAL threats

- One-way SSL authentication tunnel
  - How do you know if you are communicating with the correct server?
- Online real-time data
  - What was the price of that stock again?
- Email dropboxes on servers operated by some random hosting company
  - Do you trust those MX records?

Why now?

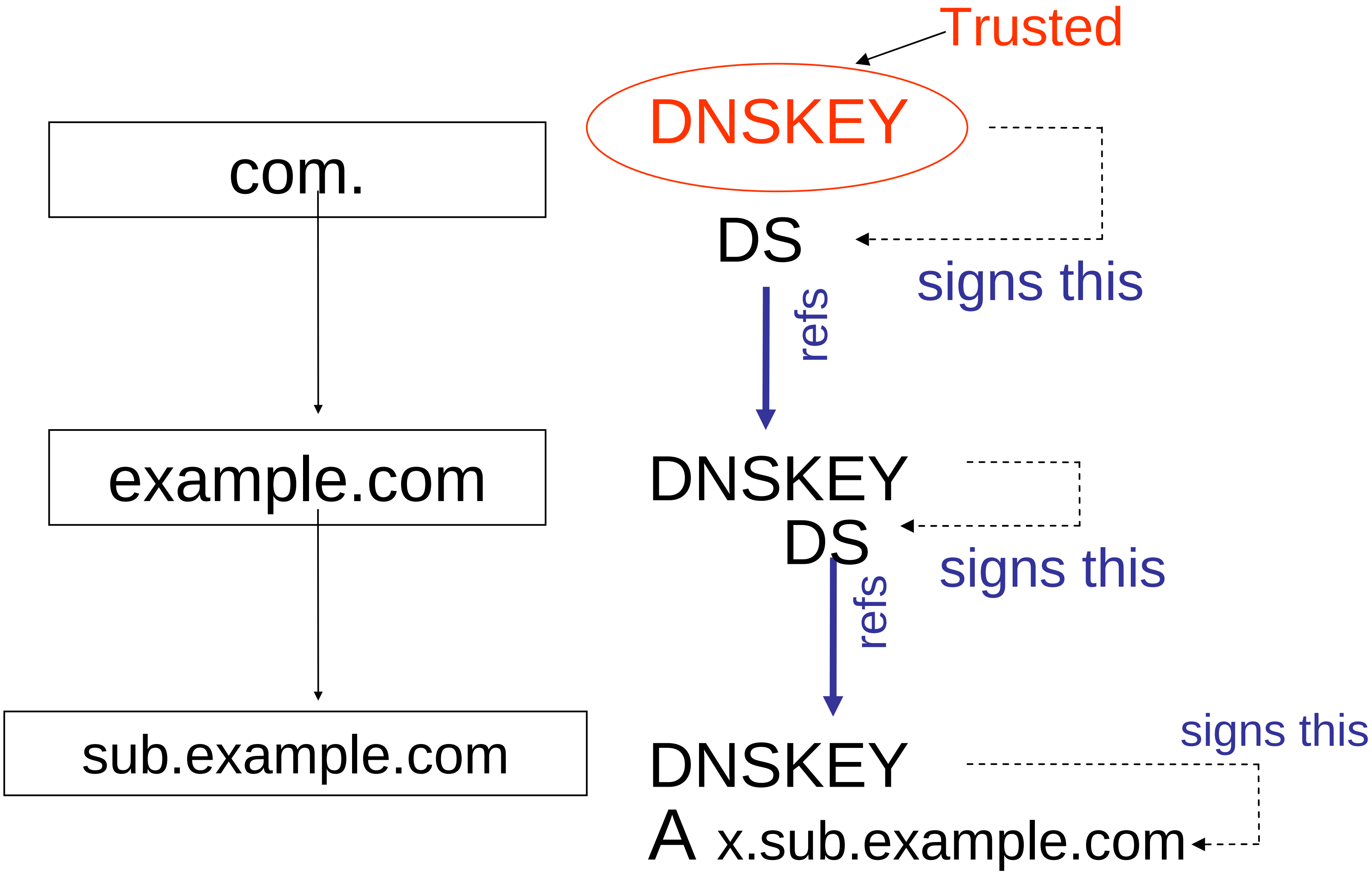
- DNSSEC protocol specifications are finally(!) complete*
- Big strides taken to make DNSSEC operationally viable
- Considerable time spent in making the specs robust
- Coordinated global effort to grow the deployed base

*** "This time for sure!" -- Bullwinkle J. Moose**

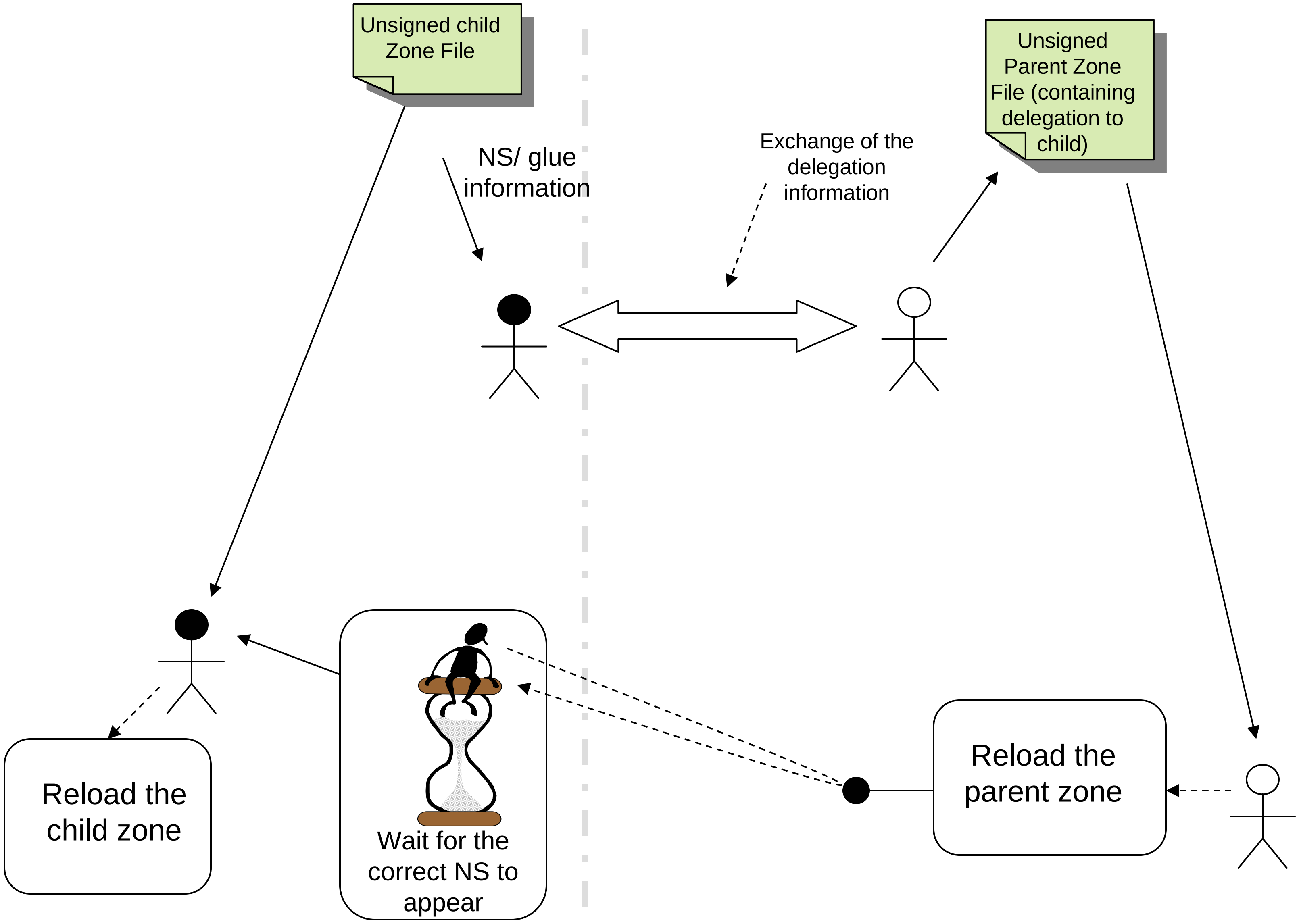
DNSSEC Services

- Protocol Extensions to DNS provide
  - Data Integrity
  - Origin Authentication of DNS data
  - Authenticated Denial of Existence
- Meta-protocol elements (TSIG, SIG(0)) provide channel security
  - Secure zone transfer
  - “Last Hop” security
- DNSSEC **does not** provide confidentiality of data
- DNSSEC **does not** protect against DoS attacks

End-to-End protection



Typical DNS operations



Unsigned child Zone File

NS/ glue information

Exchange of the delegation information

Unsigned Parent Zone File (containing delegation to child)

Reload the child zone

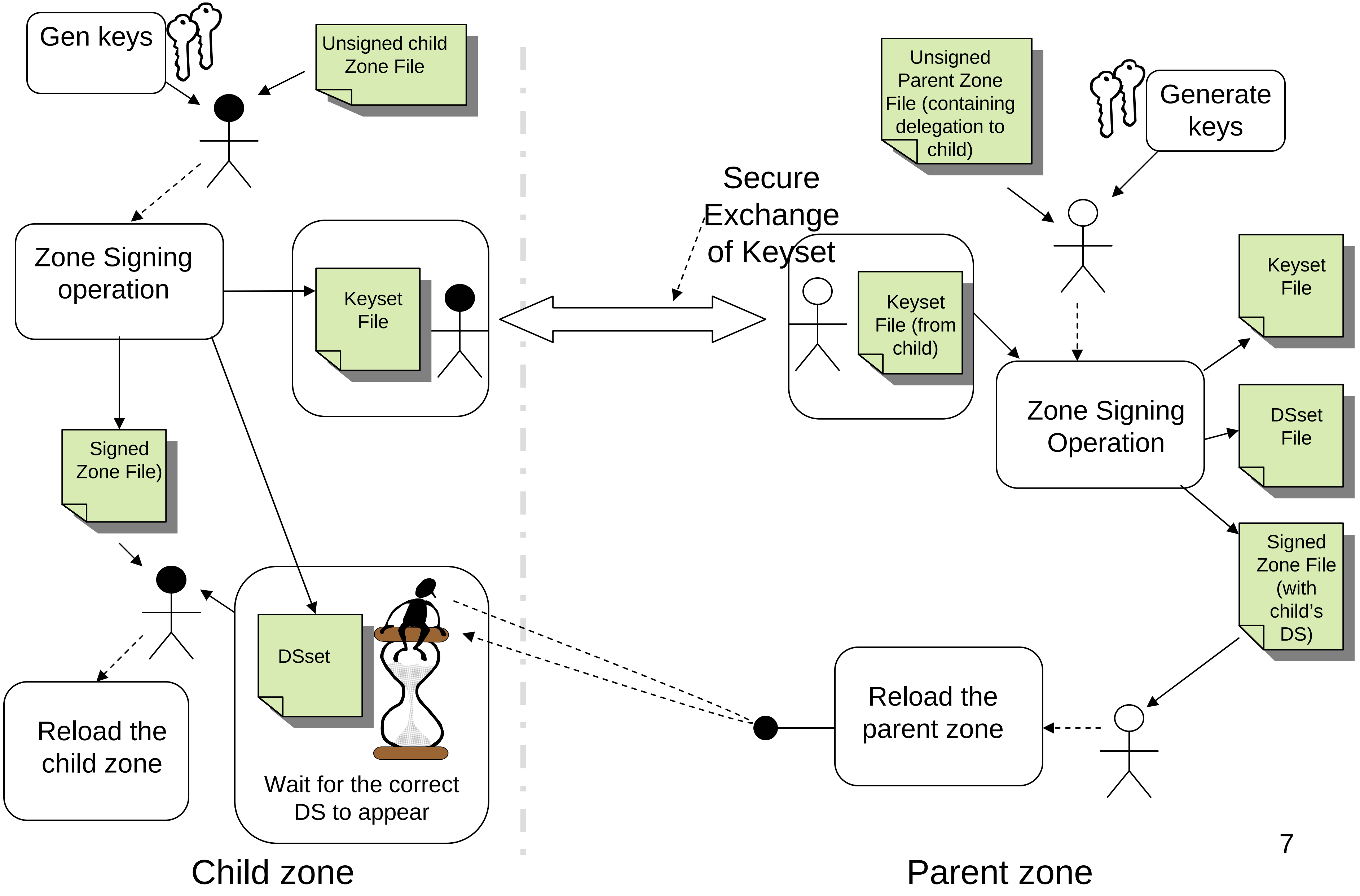
Wait for the correct NS to appear

Reload the parent zone

Child zone

Parent zone

Typical DNSSEC operations



Gen keys

Unsigned child Zone File

Zone Signing operation

Keyset File

Signed Zone File)

Reload the child zone

DSset

Wait for the correct DS to appear

Secure Exchange of Keyset

Unsigned Parent Zone File (containing delegation to child)

Generate keys

Keyset File (from child)

Zone Signing Operation

Keyset File

DSset File

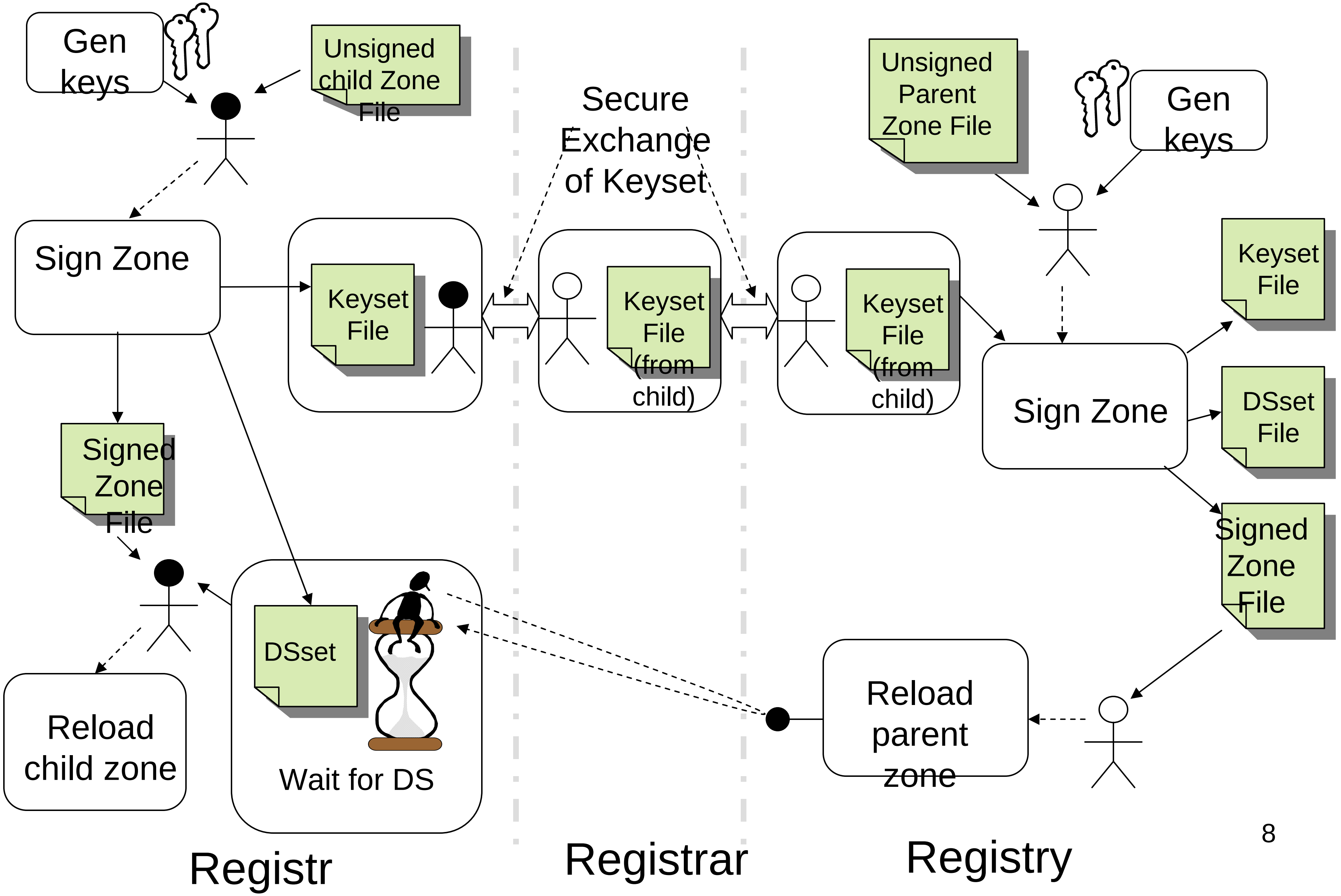
Signed Zone File (with child's DS)

Reload the parent zone

Child zone

Parent zone

Registrant-Registrar-Registry Setup



Registrant (Enterprise) view – What is different?

- Key gen and Key mgmt
- Zone signing operations
- Nameserver provisioning
- Need to securely transmit DNSSEC-related info to registrar
- Security from validating resolvers to non-validating stubs
- Incident handling

Registrar view – What is different?

- Need to securely receive DNSSEC-related information from the registrant
- Need to securely transmit DNSSEC-related info to registry
- Incident handling

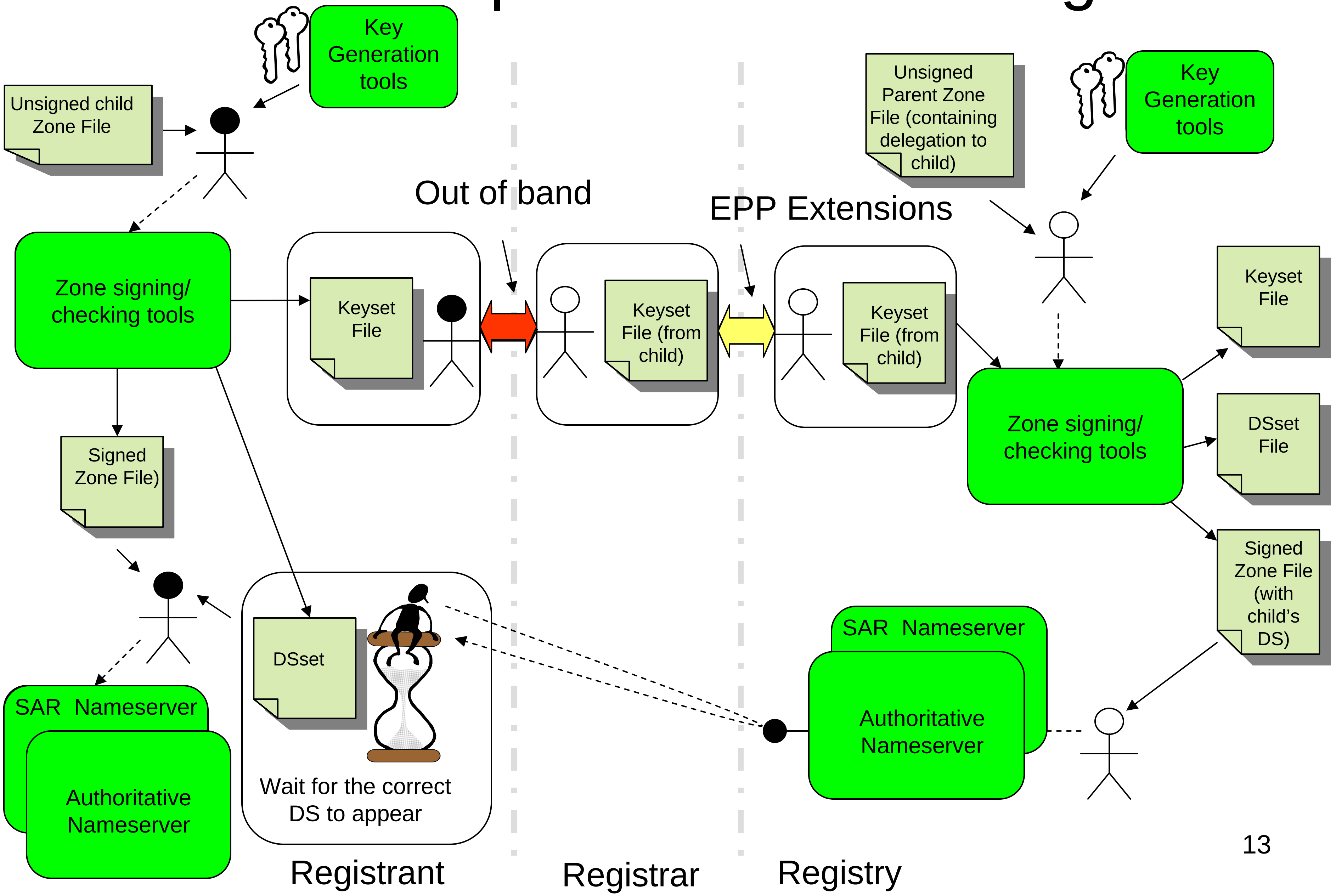
Registry view – What is different?

- Need to securely receive DNSSEC-related information from the registrar
- Need to create the secure delegation in the parent zone
- Key generation and Key management operations
- Zone signing operations
- Nameserver provisioning
  - Size of zone data increases because of signatures
  - More computational power needed (crypto operations can take time)
  - Synchronized time (signatures have temporal dependency)
- Incident handling

Summary of existing DNSSEC tools

- Key generation tools
- Zone signing tools
- Zone checking tools
- Authoritative name server implementations
- Security-aware recursive (SAR) name server implementations

Tools – present and missing



Various Ongoing Work

- Creation of tools, especially for troubleshooting and key management
- Development of policy and procedure guidance documents
- Creation of DNSSEC-aware end systems and applications
  - Need to define requirements and policies
  - Solving “last-hop” issues
- Trust anchor key rollover and distribution
- Prevention of zone walking

Enterprise-wide Experiments

- “Shadow” deployment efforts are ongoing
  - Mirroring DNSSEC operations in a non-production namespace to evaluate operational impact
- Workshops conducted for operators to gain familiarity and build faith in existing set of tools and procedures
- Some sites are already running signed DNSSEC zones

EPP extensions for DNSSEC

- EPP allows registrars with different operational models to access multiple registries via the same protocol
- Provisioning of DNS security extensions (DNSKEY, RRSIG, DS)
- Work In Progress

Registry-level Experiments

- NLnet (.nl) – Netherlands
  - http://www.nlnetlabs.nl/dnssec/
- NIC-SE (.se) – Sweden
  - http://dnssec.nic-se.se/
- JPRS (.jp) – Japan
  - DNSSEC field test in conjunction with ENUM trial (http://jprs.jp/en/)
- Verisign (.net DNSSEC pilot) – U.S.
  - http://www.dnssec-net.verisignlabs.com/
- Verisign DLV (.com/.net) – U.S.
  - http://www.dlv.verisignlabs.com/

Application-level Experiments

- SSH
  - Out-of-band verification of server public keys by looking up the fingerprint in the SSHFP resource record in DNS (http://www.ietf.org/internet-drafts/draft-ietf-secsh-dns-05.txt)
  - Implementation in openSSH
- IPsec
  - Using the IPSECKEY RR to store data such as the public key and the gateway information for creation of IPsec tunnels (http://www.ietf.org/internet-drafts/draft-ietf-ipseckey-rr-11.txt)
  - ipseckey patch for BIND-9.3.0

Hard(er) Problems

- Privacy – Not originally a goal
- Root key – Politically charged
- Killer app – Will DNSSEC be a “must have”
- Too many “trust anchors” until tree is filled in

DNSSEC Resources

- The DNSSEC deployment Working Group home page
  - http://www.dnssec-deployment.org
- Comprehensive DNSSEC resource page
  - http://www.dnssec.org
- Software
  - BIND 9.3.0 (http://www.isc.org)
  - NSD (http://www.nlnetlabs.nl/nsd/)
  - Net::DNS::Sec (http://www.ripe.net/disi/)