

Deploying DNSSEC in Large-Scale Operations

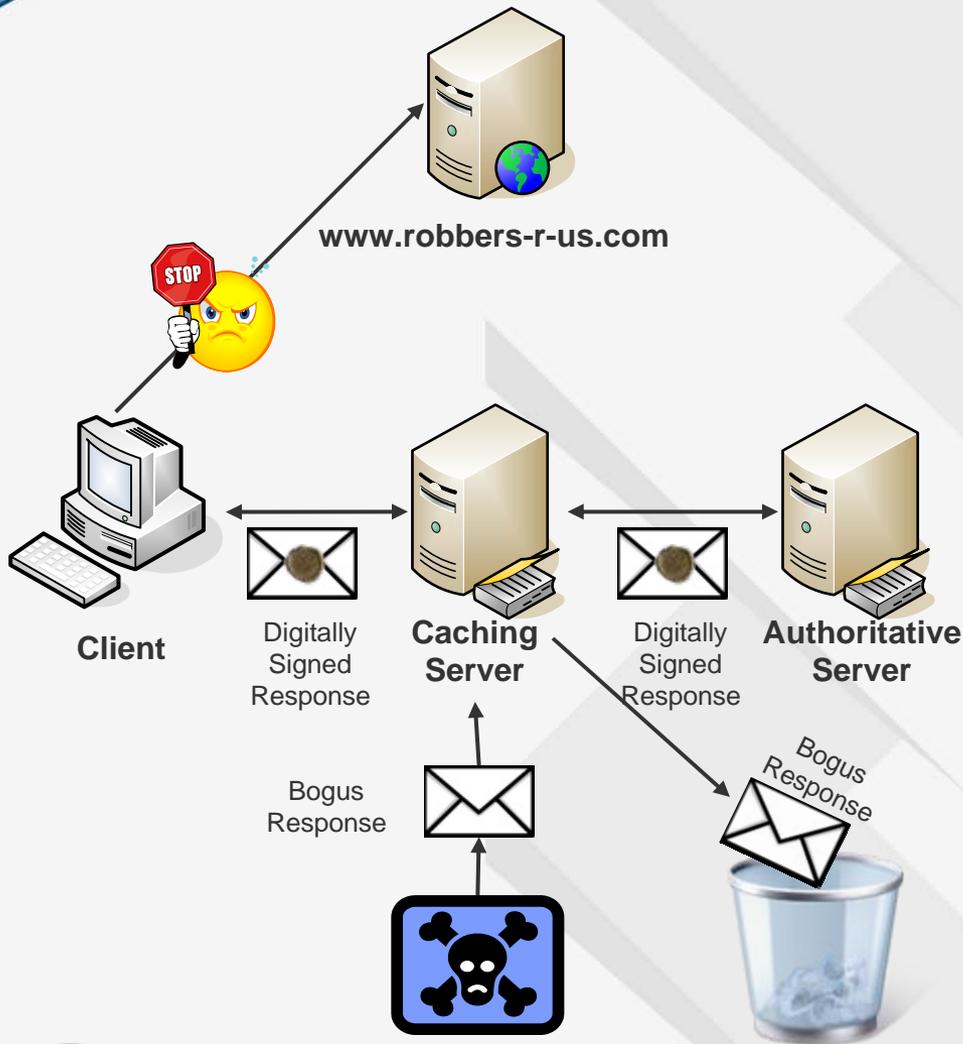
Joseph Gersch & Dr. Daniel Massey
CATCH Conference
March 4, 2009



SECURE 64

SOFTWARE CORPORATION

What Is DNSSEC?



What does it do?

- Validates the source of the DNS response
- Ensures the response has not been altered in transit
- Authenticates replies of non-existence

How does it work?

- Adds digital signatures to DNS responses
- Uses chains of trust to validate responses
- Identifies bogus responses

With DNSSEC, we are certain that a response is correct

Manual DNSSEC Deployment Steps

- **Generate keys and Insert them into zone files**
- **Sign and publish the zones**
 - generate NSECs
 - generate RRSIGs
- **Do process over and over again when data changes or when keys need to be replaced**



*OK for small deployments,
but begs for automation*



Dealing with Complexity

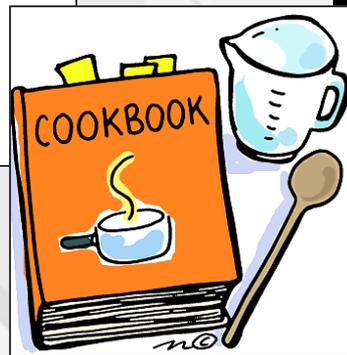
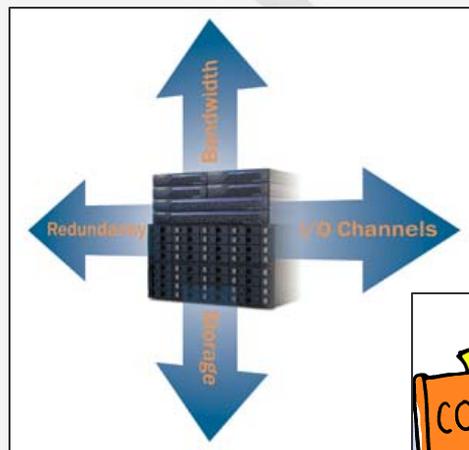


**Complicated?
Hey...What
could possibly
go wrong?**



What could go wrong...will go wRornG

- Wrong keys
- Expired Keys
- Stolen Keys
- Lose the Recipe
- Solution doesn't scale



Automation: the Secure64 DNS Signer



Simple

- Automated key management, rollover, signing, re-signing

Secure

- Malware-immune OS
- FIPS 140-2 compliant (pending)

Scalable

- High performance signing algorithms
- Incremental zone signing

Secure64 DNS Signer makes it easy to deploy DNSSEC correctly and securely

Simple to Configure

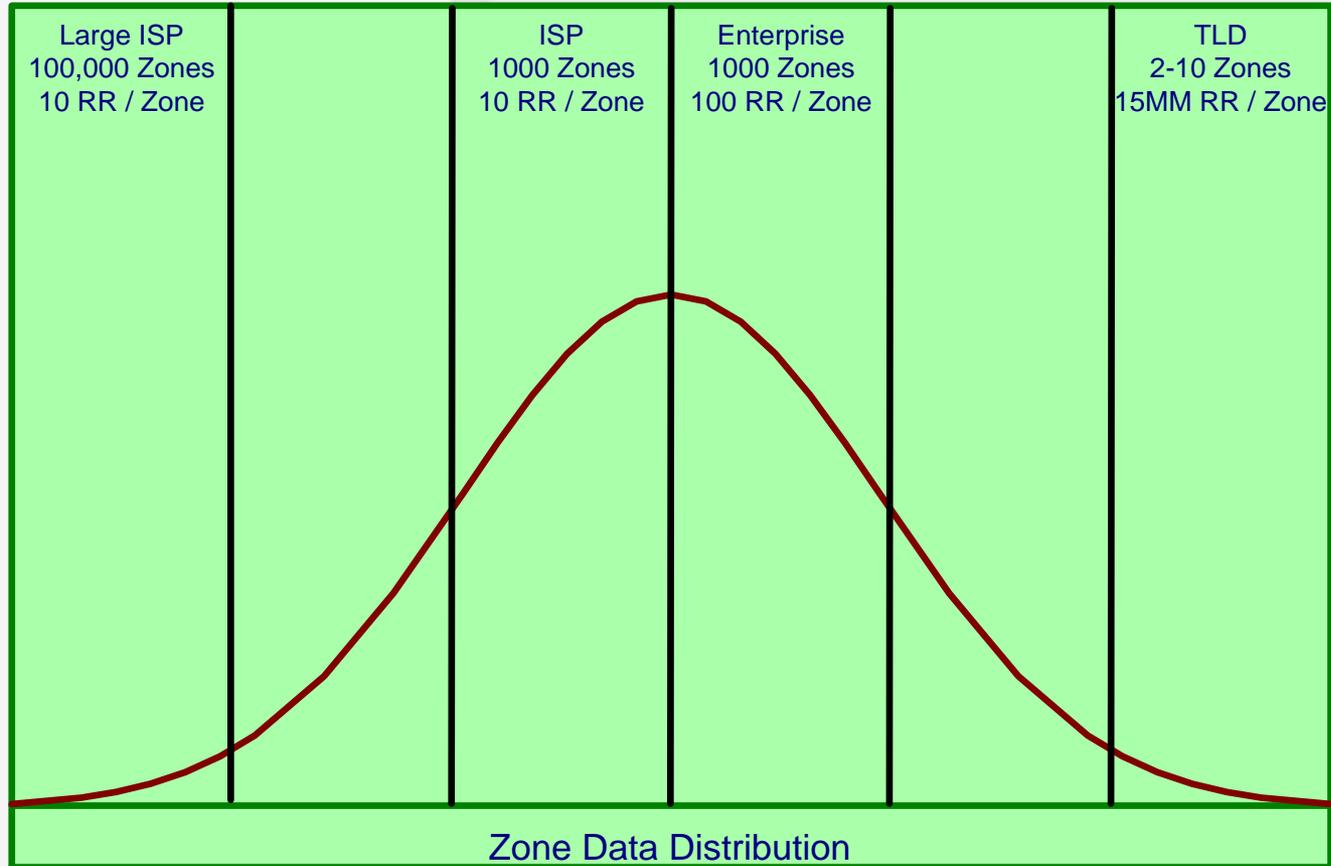
```
SERVER:  
  
# Default signing policy  
  
Dnssec-automate: ON  
Dnssec-notify: admin@mydomain.com  
Dnssec-ksk: 1024 RSASHA1  
Dnssec-ksk-rollover: 0 2 1 2,8 *  
Dnssec-ksk-siglife 7D  
Dnssec-zsk: 2048 RSASHA1  
Dnssec-zsk-rollover: 0 1 1 **  
Dnssec-zsk-siglife 7D  
Dnssec-nsec-type: nsec3  
Dnssec-nsec-settings: OPT-OUT 12 aabbccdd  
  
ZONE:  
Name: myzone.  
File: myzonefile  
Dnssec-nsec-type: nsec  
  
...  
Configuration file
```

1-line automation

Optional parameters to override defaults
Can be applied system-wide or zone by zone

DNSSEC can be deployed in days, not months

Automation of Typical Deployments

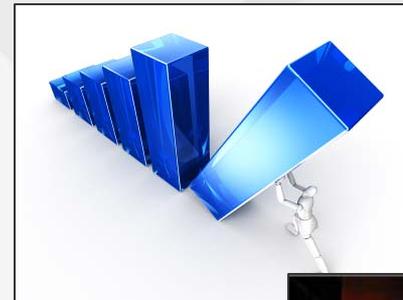
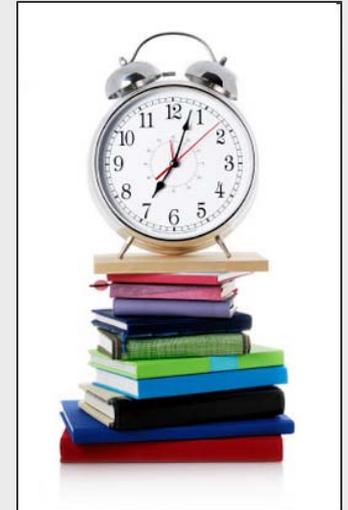


Design for the extremes and the small cases will take care of themselves



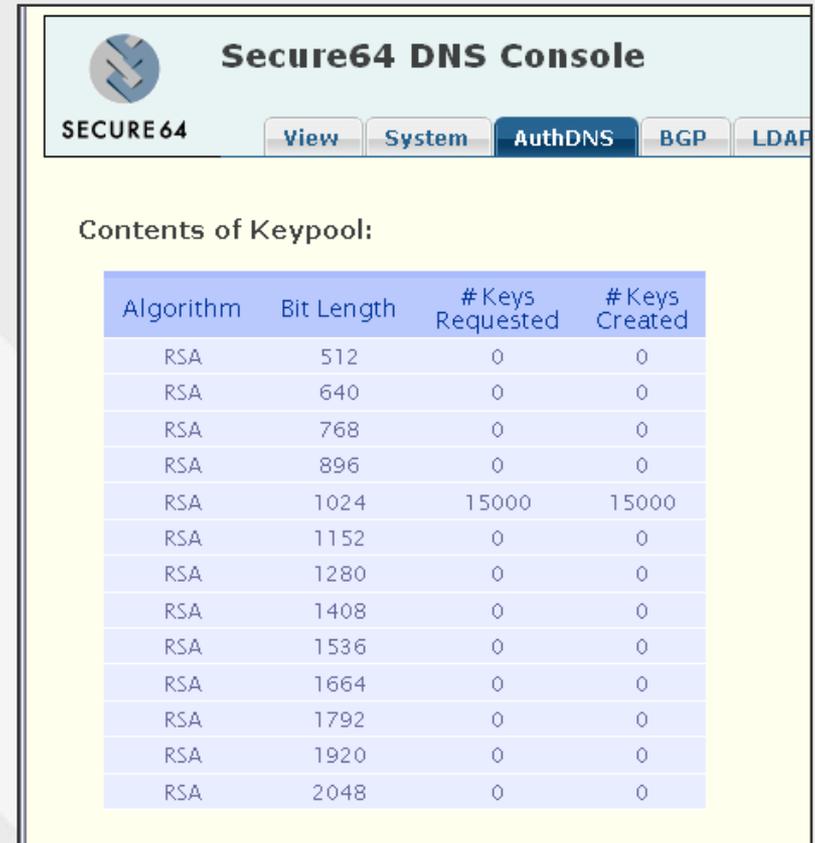
Challenges for Large-Scale Deployments

1. Key Generation for huge numbers of keys
2. Bulk Signing and Re-signing can take lots of time --- and you don't have enough time
3. Small Changes to Large Zones
4. Disaster Planning: Automatic & Secure Backup of Metadata
5. Chain-of-Trust Coordination



Key Generation & Management

- **Problem:**
 - time required to generate new keys when signing 1000's of zones
- **Example:**
 - 60,000 zones
 - 240,000 new keys
 - Time: 5 hours to 2.8 days (key-length dependent)
- **Strategies:**
 - Background task to pre-create unassigned keys in a key pool
 - Add crypto cores
 - Use shared keys (but this creates inter-zone dependencies)

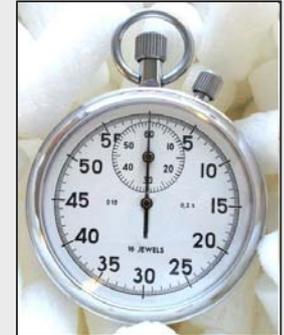


The screenshot shows the 'Secure64 DNS Console' interface. At the top, there is a navigation bar with tabs for 'View', 'System', 'AuthDNS' (which is selected), 'BGP', and 'LDAP'. Below the navigation bar, the text 'Contents of Keypool:' is displayed above a table. The table has four columns: 'Algorithm', 'Bit Length', '# Keys Requested', and '# Keys Created'. The data in the table is as follows:

Algorithm	Bit Length	# Keys Requested	# Keys Created
RSA	512	0	0
RSA	640	0	0
RSA	768	0	0
RSA	896	0	0
RSA	1024	15000	15000
RSA	1152	0	0
RSA	1280	0	0
RSA	1408	0	0
RSA	1536	0	0
RSA	1664	0	0
RSA	1792	0	0
RSA	1920	0	0
RSA	2048	0	0



Zone Signing: Time Constraints

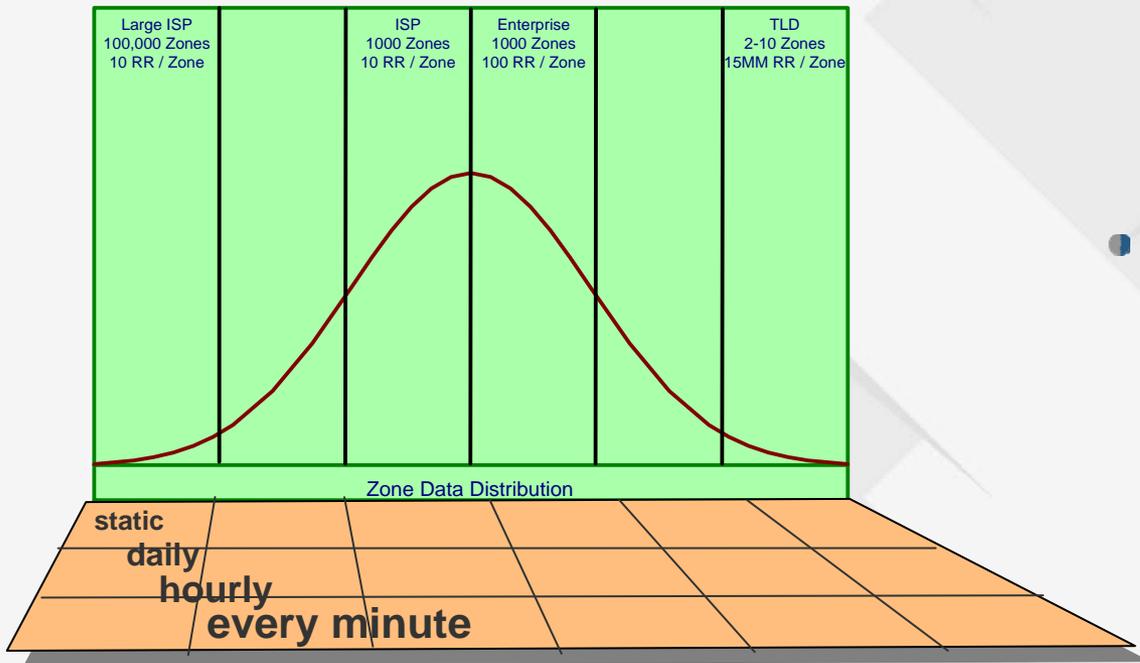


- **Problem: The time to sign a large zone or zone-list may take longer than the time available.**
- **Re-signing is needed to keep signatures valid before they expire**
- **Strategies:**
 - Stagger signing times
 - Partial signing within a zone, but this skews data and increases IXFR traffic

	Signing time (NSEC)	Signing time (NSEC3)
ISP 52,561 zones ~597,303 RRsets	6,769 Seconds (113 min)	3,931 seconds Opt-out 4,562 seconds Opt-in
TLD 14,310,000 records (primarily NS)	1,236 Seconds (20 min)	76.6 seconds Opt-out 1,447 seconds Opt-in



Automation must Accommodate Dynamic Data



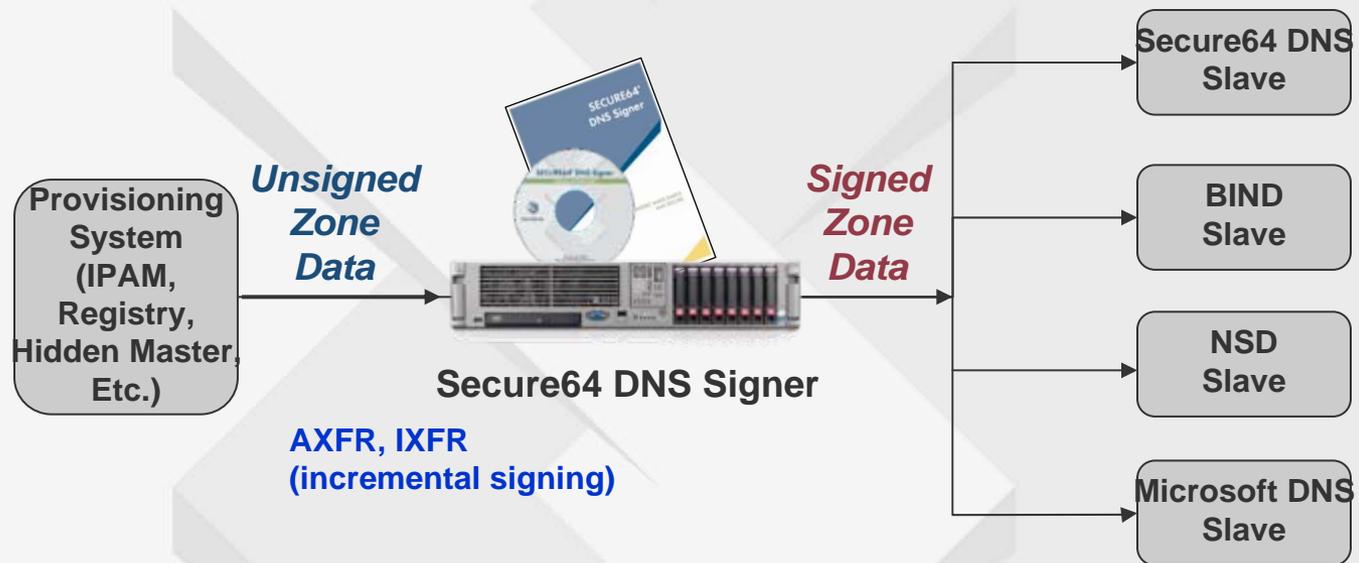
- **ISP's & TLD's:**
 - new customers result in new delegations
 - TLD with millions of RRs update once per minute
- **Enterprise:**
 - Active Directory & DHCP changes DNS data every time someone turns on a laptop

What is the allowed duty cycle for signing?



Incremental Signing for Dynamic Data Updates

Problem: Dynamic updates once per minute in a 14 million record zone. Can't afford a 20 minute duty cycle to re-sign the zone.

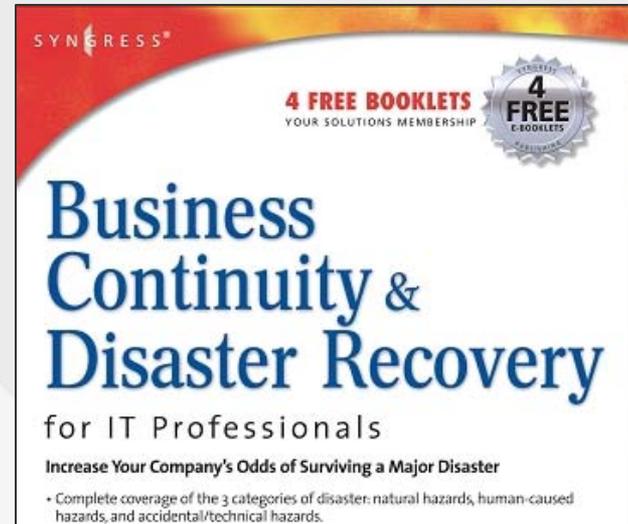


Strategy: an Inline signer will convert a single transfer of an incremental "A" record into an IXFR to slaves of 8 transactions to fix the NSEC chain and RRSIGs

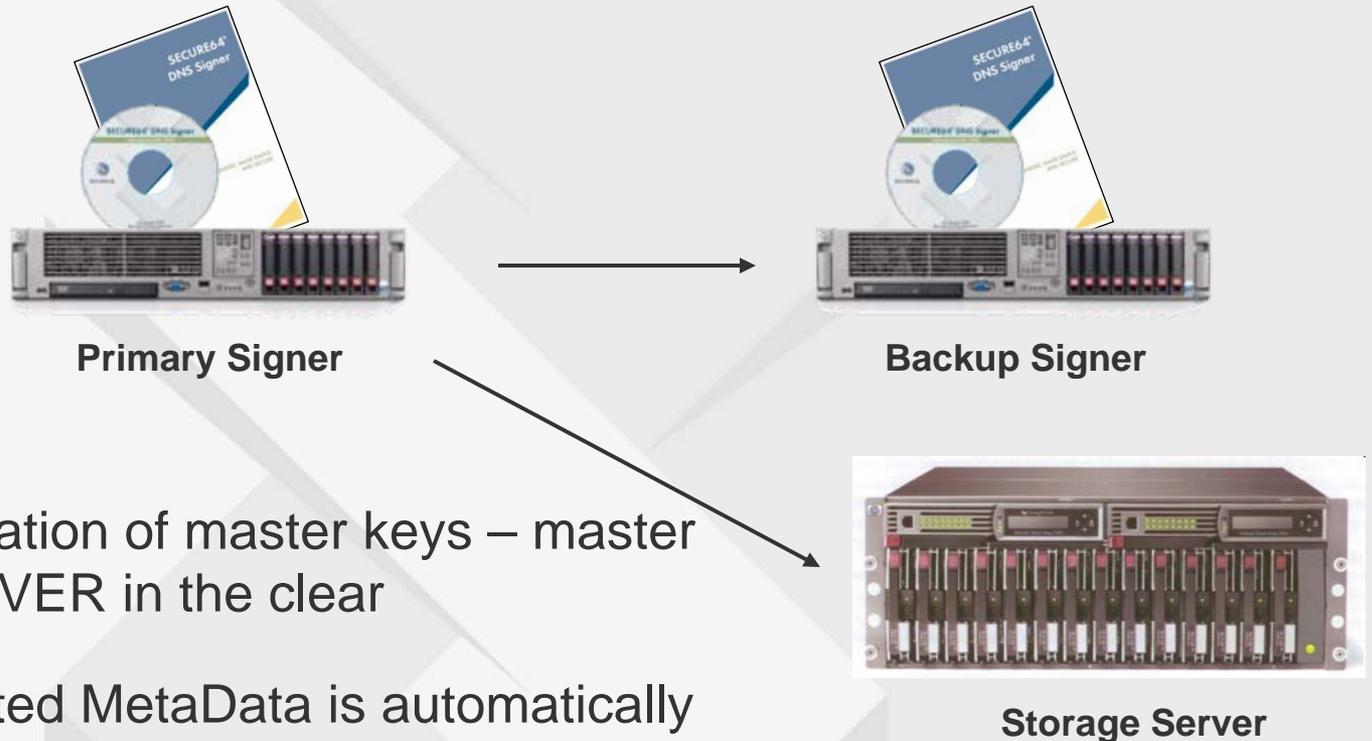


Disaster Recovery

- DNSSEC MetaData:
 - Signing Keys – private & public
 - Serial # tracking
 - key rollover state
 - Chain-of-trust info
- Don't forget to back it up
- Don't forget to encrypt it
- Automation with TPM prevents INSIDER attacks



Secure MetaData Backup & Recovery

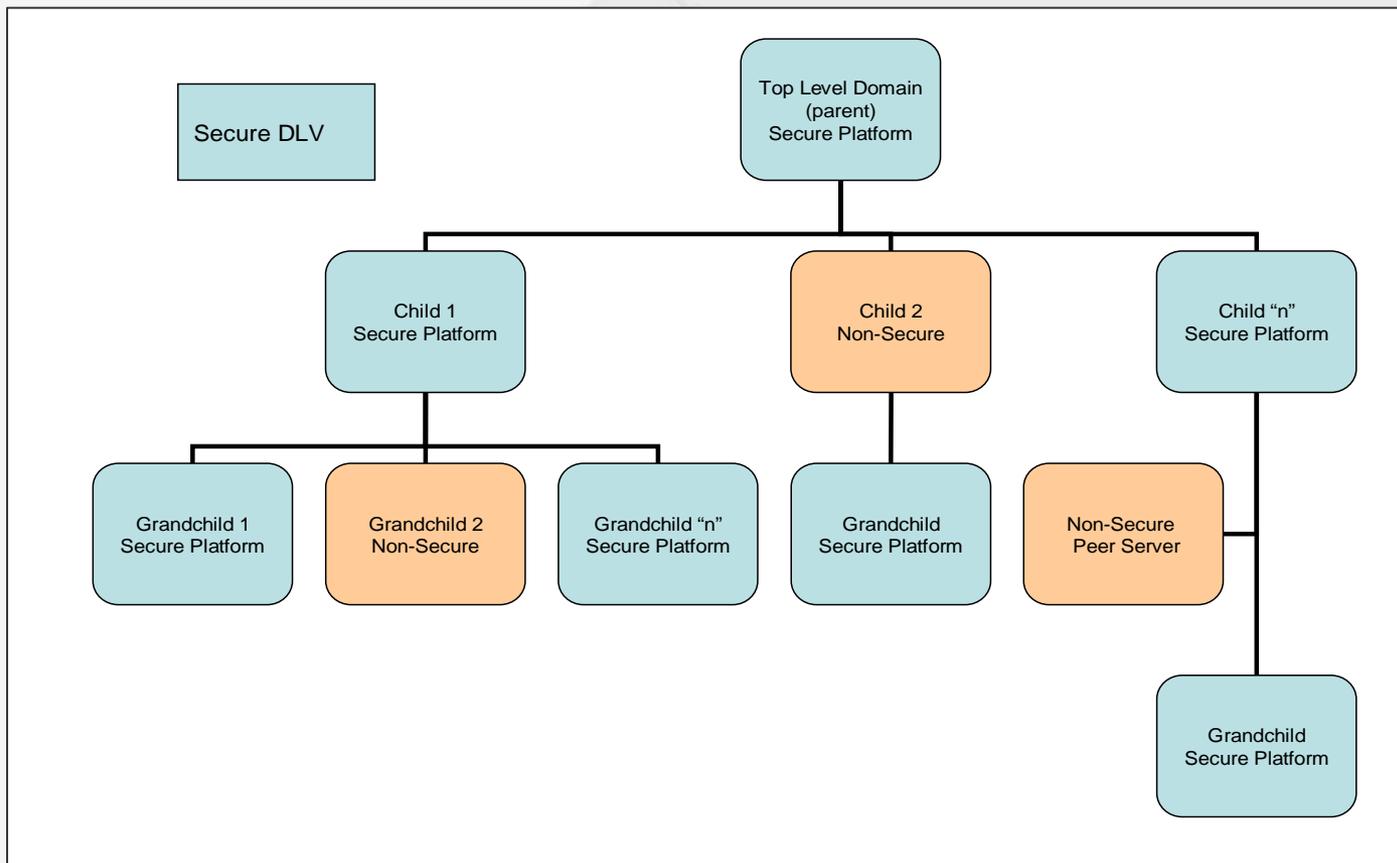


- Secure migration of master keys – master keys are NEVER in the clear
- Only encrypted MetaData is automatically sent to backup storage server
 - Automatic after each re-signing



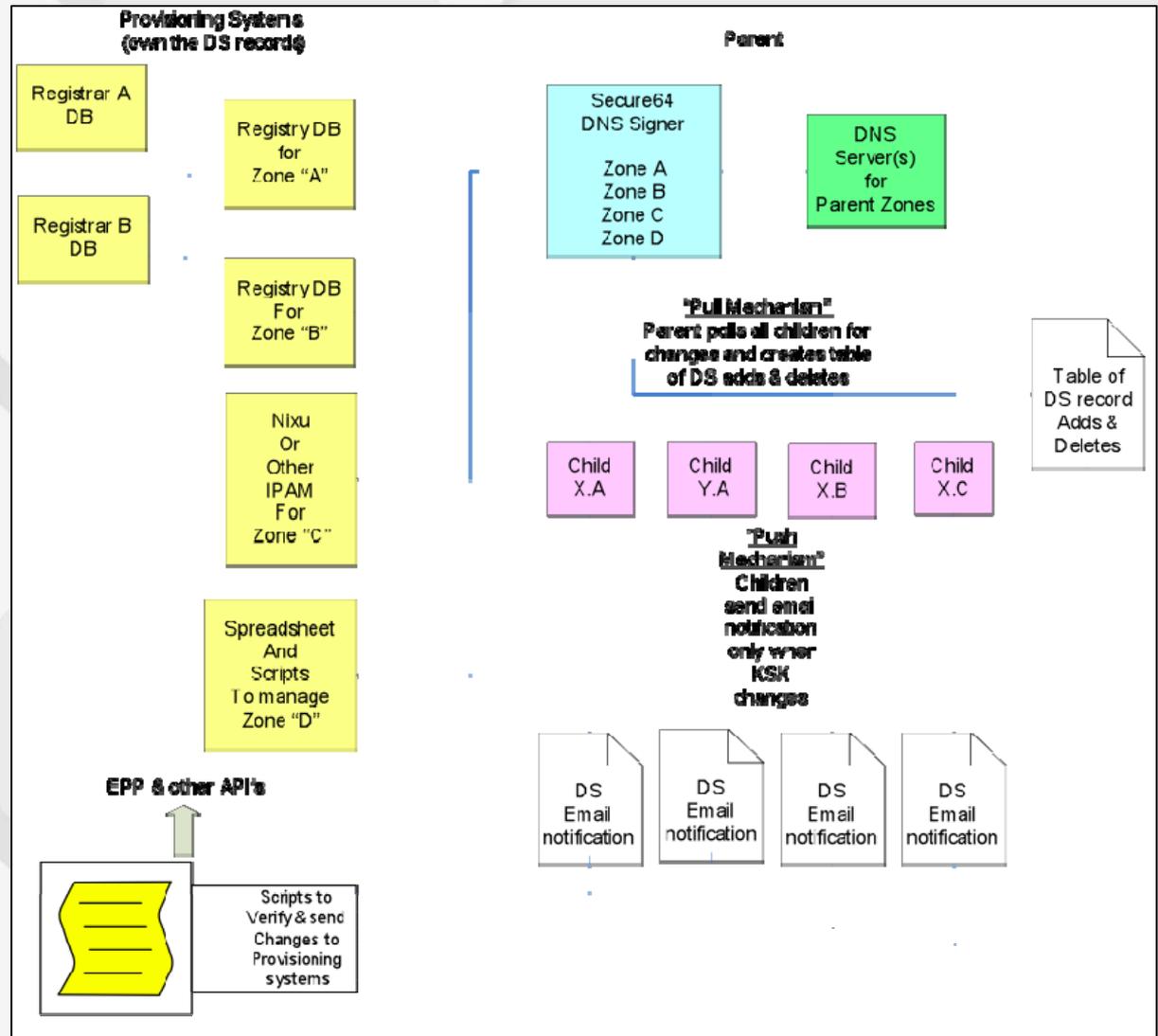
Managing the Chain of Trust

- Automation of Parent-Child DS records
- Management of trust relationships



Parent-Child Synchronization

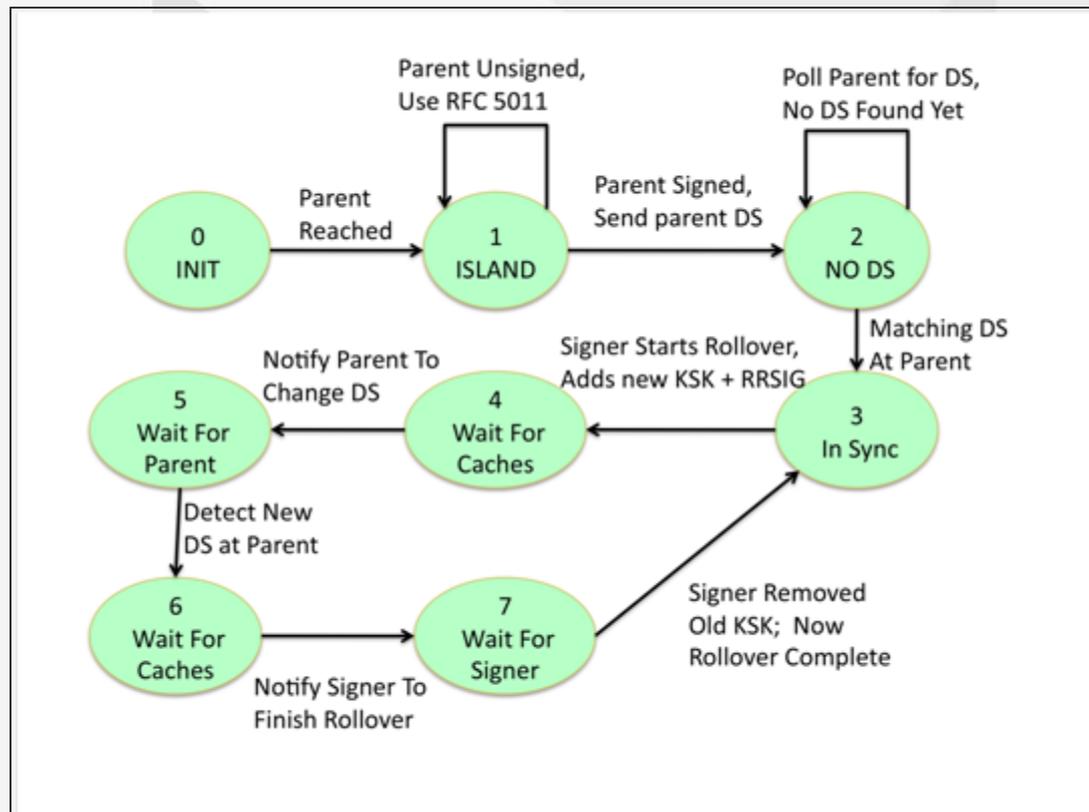
- **Parent Polls Children**
 - Millions of queries for a TLD
- **Child Polls Parent**
 - Allows full automation of KSK rollover
- **Rogue DS records can be detected and corrected.**



Automating the Chain-of-Trust

- **Publish DS and DNSKEY records**

- send to parent if parent is signed
- send Trust-Anchors to TAR if parent isn't signed



Conclusions

- Automation is the only viable deployment method for medium- to large-scale deployments of DNSSEC
 - Simplicity, Correctness, Scalability, Security, Audit
- Automation is evolving to better handle the issues discussed
 - Key Generation
 - Bulk Signing
 - Small Changes to Large Zones
 - Metadata Management (including backup & recovery)
 - Chain-of-Trust Synchronization



Thank You! For More Information

- Secure64 web site: www.secure64.com
- Search YouTube for “Secure64” to view some useful DNSSEC tutorials
- Sign up to access to an online signing engine to try it out with your own data
- Contact Adam.Tice@Secure64.com for
 - Copies of this presentation
 - Schedule a demo of our automated DNSSEC solution
 - DNSSEC whitepapers, newsletters, case studies
 - Invitation to hands on training workshops (NIST, HP)

