



Setting the Parameters *a DNSSEC* *Registrar Review*

**DNSSEC Industry Coalition
Webinar Series**

Brought to you by

**.ORG, The Public Interest Registry, Shinkuro, Inc. and
Dyn, Inc.**

The Cast of Characters

The first open gTLD to be signed



A .ORG registrar also providing DNS service for its registrants with a strong desire to support DNSSEC



Two organizations funded* to support the deployment of DNSSEC.



*The Department of Homeland Security Science and Technology (S&T) Directorate has funded SPARTA, Inc., dba Cobham Analytic Solutions, under contract FA8750-04-C-0229 and Shinkuro, Inc. under contracts FA8750-04-C-0269 and FA8750-10-C-0020. The information presented does not necessarily represent the views of the U.S. Government.

Opening Scene

- ▶ Our registry is ready for DNSSEC
- ▶ Our registrar wants to sign and serve zones for its registrants and accept DS records for those signing and serving elsewhere
- ▶ Some of our registrants want to click a button to have the zone the registrar serves for them signed while some merely want to provide their DS records
- ▶ DNSSEC tools have many settable parameters and it isn't clear which settings are right for our registrar and those in a similar situation

The Conflicts

- ▶ Multiple standards (NSEC vs. NSEC3)
- ▶ Recommendations from others (RFCs, NIST)
- ▶ One size (key size, signature lifetime) does not fit all
- ▶ Non-ubiquitous support for DNSSEC and its underlying standards (EDNS0)
- ▶ Additional computational requirements
- ▶ Legacy systems that have a limited understanding of DNS, let alone DNSSEC

We're not from the government, but they're paying us to help with

- ▶ A consistent set of DNSSEC parameters
- ▶ Suitable for small zones with guessable names
- ▶ Adequate cryptographic security
- ▶ Avoiding undue burden on
 - The registrar's infrastructure
 - ISPs and recursive resolvers
 - Last-mile connectivity
- ▶ Updates as DNSSEC adoption grows

The Resolution

- ▶ *[DNSSEC Operations: Setting the Parameters](http://dnssec-deployment.org/documents/SettingtheParameters.pdf)*
(<http://dnssec-deployment.org/documents/SettingtheParameters.pdf>)
- ▶ A work in progress
- ▶ Feedback: dnssec-parameters@shinkuro.com
- ▶ Most recent version: 2009-11-24 (03)

Analysis

During the time remaining we will go over *DNSSEC Operations: Setting the Parameters*, its recommendations, and the reasoning behind them. The paper contains more detailed explanations than are in this presentation.

DNS Settings

RR Type	TTL
SOA	1 day
NS	1 day
A/AAAA	\leq 1 day
DNSKEY	1 day

Max UDP packet Size	1492
SOA Expire Value	1 week
SOA Negative Cache Time	1 hour

DNSSEC Signature Settings

Algorithm	RSA w/SHA1
------------------	-------------------

Key Type	Key Length	Key Lifetime	Signature Lifetime	Re-Signing Period
KSK	1280 bits	4 years	4 weeks	2 weeks
ZSK	1024 bits	1 year	2 weeks	1 week

Jitter	1 hour
---------------	---------------

DNSSEC Negative Responses

Negative Response	Support			
NSEC	Default			
		Hash Iterations	Salt Size	Salt Lifetime
NSEC3	Optional	1	64 bits	Signature lifetime

DNSSEC Rollover

Key	Prepublication/ Signing Policy	Introduction Time for New Key	Retirement Time for Old Key
KSK	2K, 1S	1 week	4 weeks
ZSK	2K, 1S	4 days	2 weeks

2K, 1S means two keys and one active signature. Old keys must be removed to prevent DNSKEY answers from growing in size with each rollover.

Questions?

- ▶ You can ask questions now
- ▶ You can send questions to dnssec-parameters@shinkuro.com

DNSSEC – What a Registrar Needs to Know, Registrar Notes

Jeremy Hitchcock
Dyn Inc. / jeremy@dyn.com

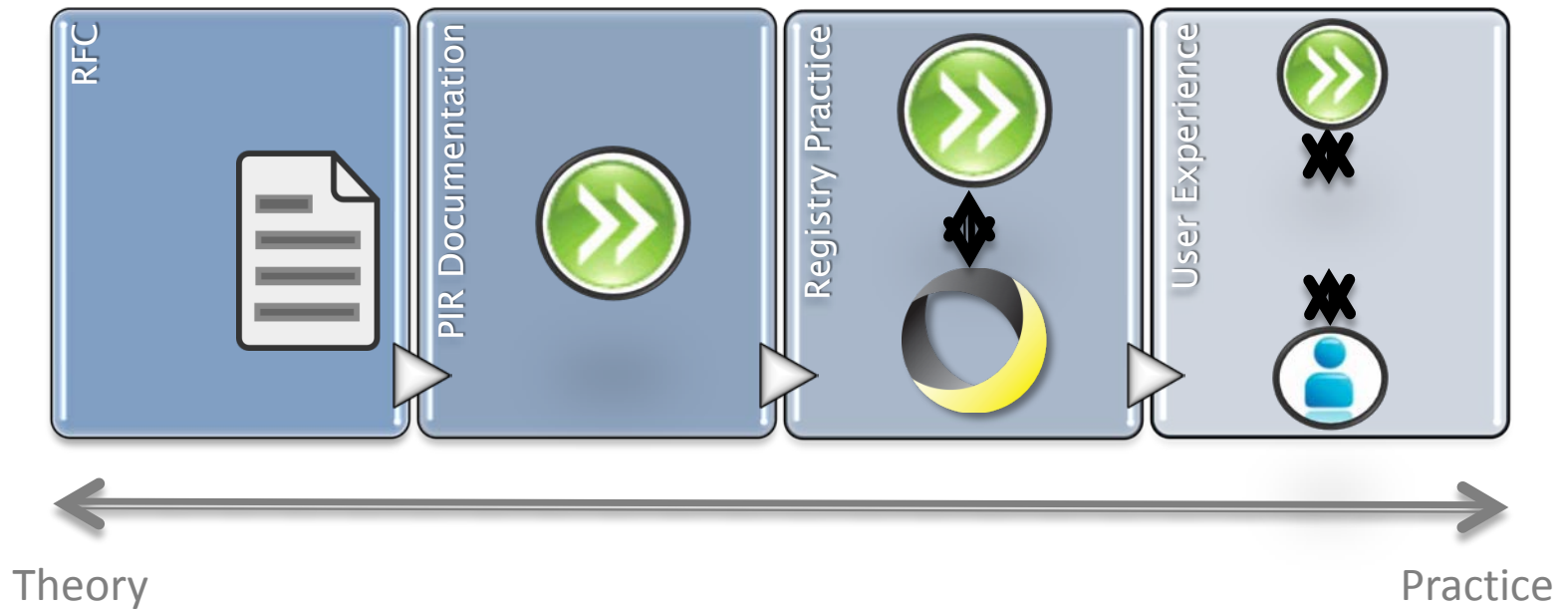
Goal

- ▶ Go over our story with DNSSEC
- ▶ Some lessons learned
- ▶ Poll DNSSEC knowledge/plans
- ▶ Answer questions

Dyn Inc (aka DynDNS.com)

- ▶ DNS operator first
 - Dynamic DNS to twitter.com (plus some [g|cc]TLDs)
- ▶ Registrar with about 50k registrations
- ▶ Allow managed DNSSEC on one system
- ▶ Allow DS keys/registry EPP on different system
- ▶ Plan both systems to do both operations

Going Down the Rabbit Hole



Started in March 2009

- ▶ Some conversations with DNSSEC transfers
- ▶ Did some internal testing with DNSSEC and NS
- ▶ Did DNS part first (DNSSEC key management)
- ▶ Added DS record EPP commands
- ▶ Spec is pretty fleshed out
 - Operational practices alright
 - Best practices still being worked on

DNSSEC and Auth DNS

- ▶ Most written about
- ▶ RFCs and BIND/NSD well documented
- ▶ TLDs have great operational experience
- ▶ Secure key management (HSM/software)
- ▶ Not doing NSEC3
- ▶ DS, RSIG, NSEC records

Example...

Search

Logged In as Support - Acting as: 5:dyn-jeremy

[Overview](#)
[Manage DNS](#)
[Manage Users](#)
[Manage Contacts](#)
[View Reports](#)
[Support](#)

sleepzero.org

 Serial: 8, [8 zone notes](#), Owner: [dyn-jeremy](#)

[Simple Editor](#)
[Services](#)
[Zone Options](#)
[Quick Tasks](#)
[General](#)
[DNSSEC](#)
[Freeze Zone](#)
[Delete Zone](#)

Zone Signing Keys

[+ Add a New Zone Signing Key](#)

Encryption Method	Key Expiration	Key Size	Actions
RSA/SHA-1	January 22 2010, 10:49:38 pm	1,024 bits	-- Select an Action ↓

Key Signing Keys

[+ Add a New Key Signing Key](#)

Encryption Method	Key Expiration	Key Size	Actions
RSA/SHA-1	July 28 2010, 10:49:23 pm	2,048 bits	-- Select an Action ↓

Delegation Signer Records

[↓ Download .txt format](#)

Expiration	Key Tag	Algorithm	Digest Type	Digest
July 28 2010, 10:49:23 pm	17917	5	1	CC8EB33C421B1829EBF5449D741D661C4F4A0C1B

DNS Key Records

[↓ Download .txt format](#)

Flags	Protocol	Algorithm	Public Key
257	3	5	AwEAAempX/kP3+oxCu9eSGt5Nag1U+8oTIvGYImfy/EUzwBIhgP7HvtzjKmF

Notifications [View task timeline](#)

Contact

billing_jeremy (Jeremy F) ↓

Send notifications

- When a key is created
- When a key expires
- Weeks before a key expires

[Update DNSSEC](#)
[Remove DNSSEC](#)

Output

```
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 1  
;; WARNING: recursion requested but not available
```

```
;; QUESTION SECTION:
```

```
sleepzero.org.      IN      A
```

```
;; ANSWER SECTION:
```

```
sleepzero.org.      3600    IN      A          204.13.248.107
```

```
sleepzero.org.      3600    IN      RRSIG     A 5 2 3600
```

```
20091123214939 20091024214939 13911 sleepzero.org.
```

```
H4pnVbaf aDGP+dQEol Gh7yt QWpj yKR0Zr sZPpRHP0f myVJg// ERUO4n
```

```
EEA3hKrgj vhULj 8VHj BNg9i f t z9VJAM75wki +WKdAz63WSL2+3+Kt R4c
```

```
Uf EKYZnLQU9xql nxr mHUoEGO3EON8ql 3YgTLQ r l or 14i eKu05nM Yuq yJU=
```

Output

```
$ dig @ns1.p26.dynect.net sleepzero.org dnskey +short
256 3 5 AwEAAAdsDDf9p7eEVo/WuGuChdCRwmMUMGcke3smNBB5QT6yWxsQ nQ
  CE3Dy0Pn4Vz9znvDN7BPDp+hCkp90r rbj scW+Si yT4bE4c6aSWI cQc2
  rKRpeY32bsuFZCR6aUPOMkPgZ1Ap0Ui euZYf vj s8j m6RncyCU4Ti LHo hYxa+JDd
257 3 5 AwEAAemPX/ kP3+oxCu9sSGt 5Nsg1U+8oTI vGYI mf y/ EUzwBI hqP7Hvt z
  j KmFoBg9E53caD/ eo3dpt eZ5al vM7dq8spi VxSj ZUERgf a49yLGxYacz
  Wn4FeCsLkMBq0f 6PDCmk2K4HkoHCPV1i PDI i D3Vt VDa0F3kj DzR8Mp8n
  3qhl EXI 9xO72MDkbmexf t / Sr t CohxnyOd29KoOz3e9R9nNdUnExQJI Mv
  qJ5l d3Cnzq5Su4w27O6bbYHPnKTheFzf 41UCVHz355QM F4aqgpxLOe
  ThZFCE0Q0nhYXHXpT9OPsxr Zxl dBnf k4qZ+7JDwxCi / 9QGhqkmwBpWsj
doKQXCNQb0s=
```

DNSSEC and EPP

- ▶ EPP extensions are simple
- ▶ It's *expected* all registries similar
- ▶ Just another piece of data
- ▶ Testing with registry

My Account

My Services

Dynamic DNS Pro
Internet Guide

SLA

Premier Support

Zone Level Services

Domain registration and
transfer, DNS hosting,
MailHop services

Host Services

Dynamic DNS hosts,
WebHop URL Forwarding

Spring Server VPS

MailHop Outbound

Recursive DNS

Network Monitoring

SSL Certificates

Renew Services

Auto Renew Settings

Sync Expirations

Account Settings

Billing

 [My Cart](#)
[0 items](#)

Search

Search

DNSSEC DS Records

[↑ Zone Services](#)

When you are signing a zone on your nameserver to enable DNSSEC, the Delegated Signer (DS) resource record must be propagated to the parent of the zone (in this case, the TLD registry) in order for establish a chain of trust to your zone. The DS record contains a digest of your DNSSEC Key Signing Key (KSK), and acts as a pointer to the next key in the chain of trust. Here, you can create up to three DS records at the TLD registry:

1. The current DS record.
2. The next DS record to use in the future after the current record expires.
3. An expired record, which is useful during the process of changing DS records.

Note: For urgent DS record changes, please contact support.

Key Tag:	<input type="text"/>	Delete DS Record
Key Hash Algorithm:	<input type="text"/>	
Digest Type:	<input type="text"/>	
Key Digest:	<input type="text"/>	

Submit as urgent?	<input type="checkbox"/>	Urgently Delete DS Record
Maxium Signature Life:	<input type="text"/>	
Include public key data?	<input type="checkbox"/>	
Key Data Flags:	256 (Zone Signing Key)	
Key Data Protocol:	3	
Key Data Algorithm:	<input type="text"/>	
Public Key Data:	<input type="text"/>	

[Create Additional DS Record](#)

Save DS Records

Output

```
$ dig @A2.ORG AFI LI AS- NST. INFO. sl eepzer o. org +dnssec
```

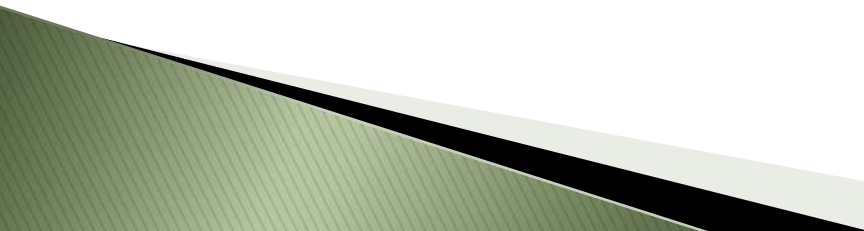
```
sl eepzer o. org.          86400    IN       DS       17917 5 1  
CC8EB33C421B1829EBF5449D741D661C4F4A0C1B
```

```
sl eepzer o. org.          86400    IN       RRSIG    DS 7 2 86400  
20091215181210 20091201171210 53990 or g.  
hz/ FVéql u4Ww2xpCFj sT6b7bAgi x5ey6Mrl l wBkcFHH1pEr WP8zMU20C  
7EvcsN9t 3Bvg/ PvEx5BKi Unby489wp6Q0Yi 46w563DwoE7pf dt ey5l XT  
t j FSPX4Cay/ xqVdpk0BOl 6hVAZOz uJh/ 0O A6AMKqKRXqx1RaSNI R1l 4 +D8=
```

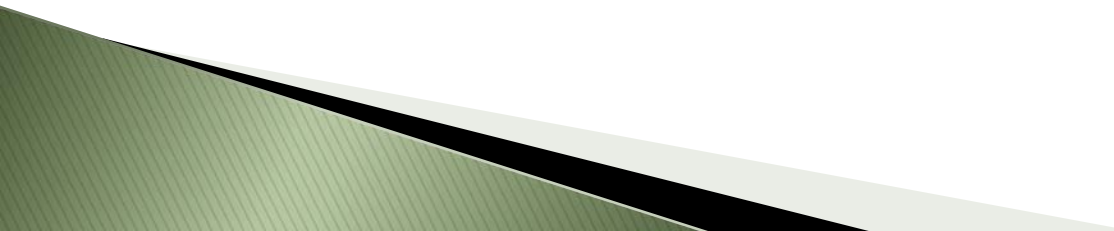
Putting the Two Together

- ▶ Next steps: both systems to get both
- ▶ System is all in-house, same as you?
- ▶ Transfer testing is ongoing
 - ccTLDs have done this for years, requires registrar cooperation
- ▶ Key rollover and registry operations separate
 - Bit of a mess since DNS drives registry operation

The Customer and DNSSEC

- ▶ Maybe not so much?
 - ▶ A few customers actually using it to try out
 - ▶ Solid single digit percentage of resolvers have do bit set (DNSSEC ok), active validation?
 - ▶ Has to be easy, tools to validate
 - ▶ Makes DNS more brittle
- 

Poll

- ▶ How many have heard DNSSEC demand?
 - ▶ How many have had had no DNSSEC demand?
 - ▶ How many are rolling DNSSEC out now?
 - ▶ How many in 3–6 months?
 - ▶ How many in 6–12 months?
 - ▶ Currently have no DNSSEC plans?
- 

Questions?

Jeremy Hitchcock
Dyn Inc. / jeremy@dyn.com

Thank you!

Lauren Price
The DNSSEC Industry Coalition
Feedback lprice@pir.org