.PR - Transitioning Registry Services with DNSSEC

James Galvin, Ph.D.
Director Technical Standards

ICANN San Juan

14 March 2018

Afilias℠

About Afilias

- Founded in 2000
- HQ – Ireland
- Global footprint
- 22M+ names
- 200+ TLDs

Business Lines

- Registry Operator
- Registry Services
- Secondary DNS

Afilias℠

TLDs Afilias is involved with…

Generic and New gTLD Examples

As Registry Operator

.info℠
.mobi
DOT pro
.bio
.移动
mobile

Generic, New TLD, and Country Code TLD Examples

As Registry Service Provider

.org
.asia
Connecting Asia with One Domain
KIM
MN
DOMAIN REGISTRY
.LC
.in
.au
.GLOBAL
.VEGAS
.ngo
.ong
.Me
dot bz
.AG
.iO

.pr

Agenda

- DNSSEC history
- Key Rollover Considerations
- Process
- Challenges
- Q&A

Agenda

- **DNSSEC history**
- Key Rollover Considerations
- Process
- Challenges
- Q&A

Role in DNSSEC History

- Started with DNSSEC in 2008
- Began signing TLDs in June 2009
- Found bug in DNSSEC extension to EPP
- Introduced accepting DS records June 2010
- Completed signing all TLDs and offered signed delegations soon after

Agenda

- DNSSEC history
- **Key Rollover Considerations**
- Process
- Challenges
- Q&A

Key Rollover Considerations

- Transitioning a TLD requires a KSK rollover
  - Best practice - do not want to go “insecure”
- Risks are high
  - Mistakes would make the TLD zone invalid
- Consider the attention to the root key rollover
  - Global risk versus regional risk

Agenda

- DNSSEC history
- Key Rollover Considerations
- **Process**
- Challenges
- Q&A

TLD KSK Rollover Process - Preparation

- Initialization
  - Exchange TSIG key material via encrypted email
  - Provide authoritative unsigned copy of zone
  - Generate KSK and ZSK for the zone
- Setup
  - Deploy zone in Afilias infrastructure
  - Add new ZSK and KSK to the old TLD zone
  - Request IANA add the new DS records to the root zone
  - Add new ZSK and KSK to the new TLD zone

TLD KSK Rollover Process - Execution

- Initiation
  - Add Afilias NS (and glue) records to the old TLD zone
  - Remove old NS records from the new TLD zone
  - Request IANA add the Afilias NS and remove dotPR NS records from the root zone
- Finish
  - Request IANA remove the old DS records from the root zone

Agenda

- DNSSEC history
- Key Rollover Considerations
- Process
- **Challenges**
- Q&A

Challenges (1)

- Best practices for "DNSSEC transition" is the "easy part"
- Gaining Operators should be ready for surprises
- The technologies via which zone content is published from Registry data (and non-Registry) data vary widely among surrendering operators
  - Afilias has seen everything from Windows/SQL/BIND to 15-year-old Sun servers supporting a ccTLD infrastructure

Challenges (2)

- The policies and rules for publication of zone content from registry data can vary among operators
  - Afilias requires a minimum of two nameserver objects
  - Some surrendering operators have published delegations with only one nameserver

Challenges (3)

- Reduce work via analysis, scope-reduction, and after-action debrief
  - Omitted from a past migration signed TLD-subzones which lacked delegations or DS-records published in parent TLD zone
- DNSSEC Operator transition is high-overhead work

Agenda

- DNSSEC history
- Key Rollover Considerations
- Process
- Challenges
- **Q&A**

Thanks for listening!
Questions?

James Galvin
jgalvin@afilias.info

https://afilias.info