Removing Impediments to DNSSEC Deployment

Duane Wessels & Casey Deccio

February 11, 2015

A Problem

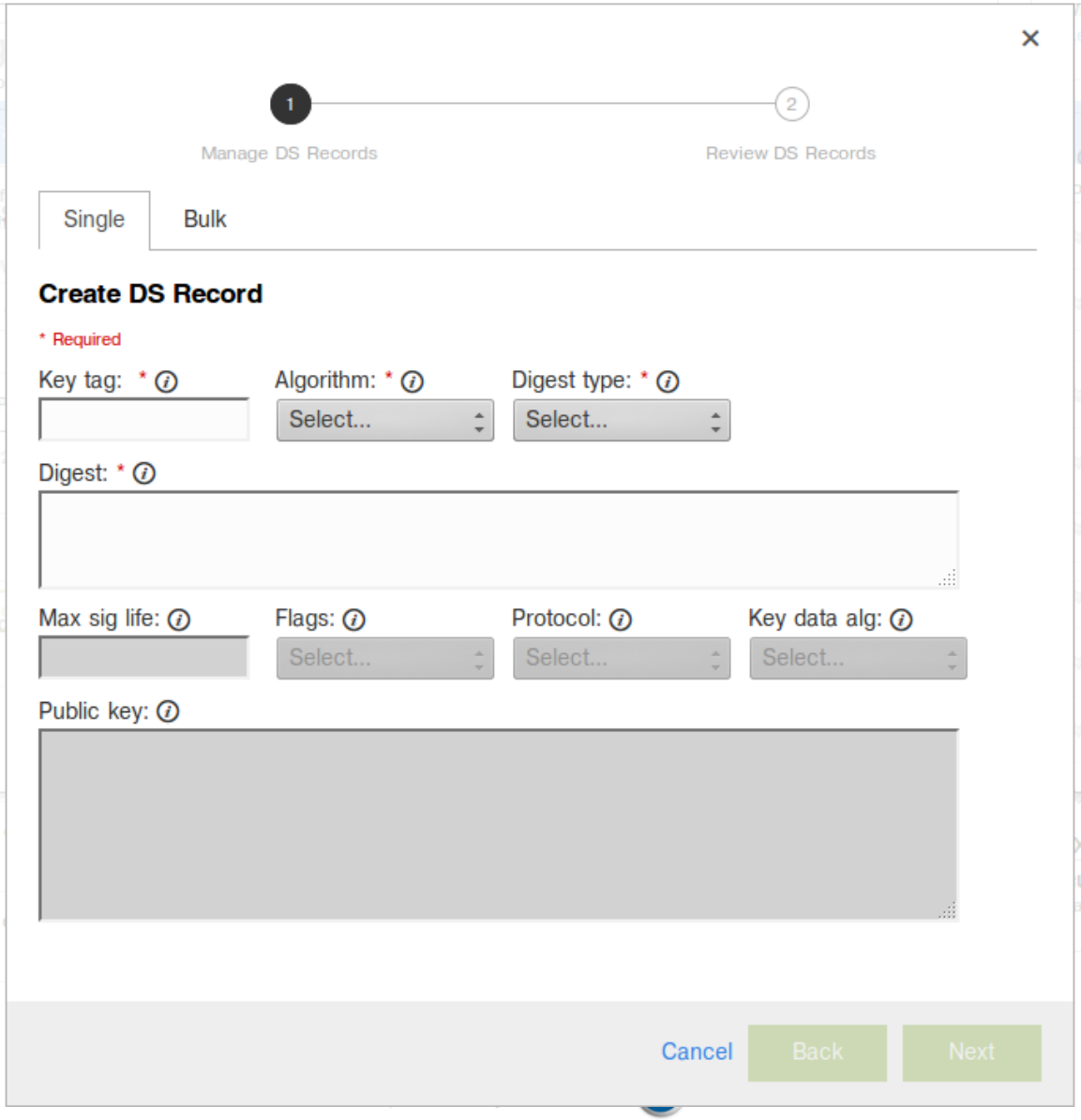
For some, the Registry-Registrar-Registrant model is an impediment to scalable deployment of DNSSEC.

DS Records

- DNSSEC “glue” between zones.
- Cryptographic hash of the child zone Key Signing Key.
- Not understandable by humans.
  - Which of the following DS records are valid?

```
example.com.   86400   IN      DS      31689 8 2
CDE0D742D6998AA554A92D890F8184C698CFAC8A26FA59875A990C03 E576343C

example.com.   86400   IN      DS      31589 5 1
3490A6806D47F17A34C29E2CE80E8A999FFBE4BE

example.com.   86400   IN      DS      31589 8 2
CDE0D742D6998AA554A92D890F8184C698CFAC8A26FA59875A990C03 E576343C

example.com.   86400   IN      DS      31589 8 2
CDE0D742D6998AA554A92D890F8784C698CFAC8A26FA59875A990C03 E576343C

example.com.   86400   IN      DS      31589 8 2
CDE0D742D6998AA554A92D89OF8184C698CFAC8A26FA59875A990C03 E576343C
```

Entering a DS Record via Registrar



Key Rollovers Are Hard

- RFC 6781: “Regardless of whether a zone uses periodic key rollovers or only rolls keys in case of an irregular event, key rollovers are a fact of life when using DNSSEC.”
- In some cases, rollovers are avoided entirely due to the complexity.
- A KSK rollover requires interaction with the Registrar (i.e., parent zone).
- Rollovers require special attention to details and, ideally, experience.

Third-Party DNS Operators

- DNS services are often outsourced to third-party operators.
- Operators are not a party to the RRR model and not allowed to interact with the Registry.
  - Although sometimes the Registrar is the DNS Operator.
- Today, operators rely on Registrants to publish DS and other records.

In Other Words…

To increase DNSSEC Deployment, we should explore solutions to streamline the processing of crypto data

What If...

What if… Registrants weren't required to submit crypto data through Registrars

- A simpler, and more stable, alternative to DS records?
- Perhaps a name or a "pointer."
  - Easy to understand
  - Changes infrequently
- But which is treated like a DS record.
  - Authoritative in the parent
  - Signed
- Enabling a not-strictly-hierarchical chain-of-trust.

What if… Registries could take data directly from Registrants

- RFC 7344 “Automating DNSSEC Delegation Trust Maintenance.”
- draft-ietf-dnsop-child-synchronization: “Child To Parent Synchronization in DNS.”
- Bootstrapping problem because child zones must be signed.

What if… Registries could accept data directly from DNS Operators

- Bring Operators into the ecosystem.
- Beneficial to more than just DNSSEC.
- Work in progress along these lines.
- Good for Registrants using third-party operators, but what about everyone else?

In Summary

- A few different, but complementary, approaches to making DNSSEC easier for end users and Registrants.
- Different tradeoffs and benefits.
- All require protocol or process changes.
- Would like your input and feedback.

VERISIGN®