DNSSEC Key Rollovers and Transfers

Combining DNSSEC and Registration Transfers in gTLDs

James Galvin, Ph.D.
Afilias

ICANN 50 London
DNSSEC Workshop
25 June 2014

Context for the Problem

- Objective is to ensure a valid zone during transition from an old service provider to a new service provider
- However, if you are:
  - gTLD or TLD that complies with gTLD rules
- Then:
  - Problem when DNS services are tightly-coupled with registration services

DNSSEC only Transfer

- Deploy new signed zone with new key(s) at new DNS service provider
- Pre-publish new KSK through registrar
- Change NS records
- Discontinue service at old service provider

Registration Transfer With Bundled DNS

- Registrant contacts new registrar
- New registrar requests transfer on behalf of registrant
- Old registrar receives request
  - Removes second level name from TLD zone
- Wait for 5 day grace period to expire
  - **Domain goes dark as TTLs timeout**
- New registrar changes NS records

Peek at an Overlay

	Registrant contacts new registrar
Deploy new signed zone with new key(s) at new DNS service provider	
Pre-publish new KSK through ***old*** registrar	
Change NS records	
	New registrar requests transfer on behalf of registrant
Wait for transfer to complete	
	New registrar changes NS records
Discontinue service at old service provider	

Where are the Issues?

	Registrant contacts new registrar
Deploy new signed zone with new key(s) at new DNS service provider	
Pre-publish new KSK through ***old*** registrar	
Change NS records	
	New registrar requests transfer on behalf of registrant
Wait for transfer to complete	
	New registrar changes NS records
Discontinue service at old service provider	

Needed Functionality

- Should be able to deploy DNS/DNSSEC in advance of registration in new registrar
- Should be able to add new registrar KSK through old registrar
  - Export new key from new registrar
  - Import new key through old registrar
- Should continue DNS services at old registrar for a period of time:
  - After NS record changes
  - During and after registration transfers

What It Should Look Like

- Registrant contacts new registrar
  - Deploy new signed zone
  - Export new KSK record and new NS records
- Registrant changes at old registrar
  - Import new KSK record
  - Push new NS records to the registry
- Registrant initiates registration transfer at new registrar
- Wait for registration transfer to complete
  - New registrar pushes NS records to the registry
  - Discontinue DNS service at old registrar