The Long Road to Multi-Signer Operation

Steve Crocker

Edgemoor Research Institute

12 March 2025

Signer

- A Signer is…
  - A DNS Operator
  - That generates its own keys, and
  - Signs the zone it is serving

Two Problems

- Transition a Running Zone from one Signer to another
  - How to transition a running, signed zone from one operator to another
  - Where each operator has its own keys
  - Without losing resolution or validation

- Key Roll by Unaffiliated Child Signer
  - Signer rolls its key. The parent needs a corresponding DS record
  - If the Signer is part of the Registrar, the Registrar uses EPP to convey the new record to the parent.
  - But what if the Signer is not part of the Registrar

Multi-Signer Operation

- Originally motivated by transfer of signed, running zone from one operator to another with no loss of resolution or validation
  - “Glitch-free” and “Ripple-free” transition

- PIR (.org) wanted to make sure it would be possible for a registrant to change registrars, i.e. avoid lock-in

2010 - 2012

- Manual transfer demonstrated around 2010 when the root was signed

- Multiple scenarios
  - DNS provider part of or not part of the registrar
  - Change of registrar vs same registrar
- Transfer sequence took many hours.
- Scenario 8Aa->Bb takes 21 manual steps!!

Scenario 8

- “This scenario tests just the transfer of Registrar and DNS service. It is assumed that other services, e.g. mail and web, are provided on separate machines and do not need to be transitioned.“

- Initial State: domain name is registered via A and operating on a1 and a2

Scenario 8 Configuration

Scenc	8AaBb	Transfer of DNS operation for a signed zone
Actors		Each operator is associated with a different registrar
R	PIR/Afilias	
H	Shinkuro	This scenario tests just the transfer of Registrar and DNS service. It is assumed that other services, e.g. mail and web, are provided on separate machines and do not need to be transitioned. Initial State: domain name is registered via A and operating on a1 and a2
A	Dyn	
B	NBC	
aa	Dynect	
bb	NBC	
FQDN	ssecxfr01040-8AaBb.o	
NS	a1, a2, b1, b2	

Scenario 8

Steps 1-4

Scenario	8AaBb	Transfer of DNS operation for a signed zone
Actors		Each operator is associated with a different registrar
R	PIR/Afilias	
H	Shinkuro	This scenario tests just the transfer of Registrar and DNS service. It is assumed that other services, e.g. mail and web, are provided on separate machines and do not need to be transitioned. Initial State: domain name is registered via A and operating on a1 and a2
A	Dyn	
B	NBC	
aa	Dynect	
bb	NBC	
FQDN	ssecxfr01040-8AaBb.o	
NS	a1, a2, b1, b2	

entry format

Step	Date/Time	Notes	actor	Action	Expected Result
					Observed Result

Step	Date/Time	Notes	Acto	Actions	Results
1		3	H	Request authorization to transfer from A	
2			H	Request Registar B to transfer Registrar and operate zone	Positive Ack from Reg B
3			B	Send authorization for transfer to R	
4			R*	Change Registrar and send nofication to both A and B	B authorized to change parent

Scenario 8

Steps 7-12

Step	Date/Time	Notes	Acto	Actions	Results
7			A*	Add ZSKs to the zone's keyset	
8			B*	send EPP command to add new DS records to the parent	
9			R*	add the new DS records to the parent	query shows new DS records at the parent
10			H	Wait for the later of two sequences: ZSK to appear in c, then for the maxTTLof ZSKs, and, after the DS records appear at the parent, wait for the DS TTL.	
11			H	Tell A to replace name servers with b1, b2 in the child.	Positive Ack from A
12			H	Tell B to replace name servers with b1, b2 in the parent.	Positive Ack from B

Scenario 8

Steps 15-21

15		2	H	Wait for b1, b2 to appear in a and in parent	b1, b2 appear in both a and parent
16			H	Wait max(TTLs on the NS sets)	No visible result. Caches are presumably drained throughout the net
17			H	Tell a to turn off service	a Acks
18			a*	a turns off service	a servers respond to queries with "notauth"
19			H	Tells b to remove old DNSKEYs and tells B to remove old DS records from parent.	
20			b*	DNSKEYs from a are removed from b's zone	query shows records gone
21			B*	Send EPP command to remove old (a's) DS records from the parent	query shows DS records gone

Summary of Manual Transitions

- 21 scenarios (about half were without DNSSEC)
- Each one worked
- Tedious and lengthy
- Human needed access into registrars and DNS operators

- In a transfer situation, one DNS provider gains and the other loses.
  - The losing provider does not have much motivation to cooperate.

Problems Encountered

- Each Signer had to agree to accept keys from the other signer.
  - No motivation for the Losing Signer to cooperate
- Three types of caching resolvers
  - Parent Centric
  - Child Centric
  - Sticky Child Centric
    - In principle, a Sticky Child Centric might delay seeing the change indefinitely

Interest in Multiple Signers

- Shumon, et al focused on multiple signers
  - RFC 8901
- Multiple signers provide additional robustness
  - This changes the value proposition
- Transfer of a Signed zone is just the edge case
  - Add a new signer
  - Brief wait until everything is stable
  - Remove old signer
- Cooperation of Signers to accept external keys still required

Automation of Transitions

- Long delay before design started
- Primary effort came from .SE
- Design of a multi-signer controller (Music)

Evolution of Software and Services

- Nameserver Software Capabilities

- DNS Service Provider Capabilities

Name Server Software Capabilities

22 Aug 2022	BIND			Knot 3.2.0			PowerDNS			(Others TBD)					
	C	D	R	C	D	R	C	D	R	C	D	R	C	D	R
Add DNSKEY records	✓	✓		✓	✓		✓	✓	✓						
Remove DNSKEY records	✓	✓		✓	✓		✓	✓	✓						
Add CDS/CDNSKEY records	✓	✓		✓	✓		✓	✓	✓						
Remove CDS/CDNSKEY records	✓	✓		✓	✓		✓	✓	✓						
Add CSYNC record	✓	✓		✓	✓		✓	✓	✓						
Remove CSYNC record	✓	✓		✓	✓		✓	✓	✓						

C = Command Line Interface – not usable

D = Dynamic DNS

R = Rest API

✓ **Complete**

❑ **In progress**

o **Planned but not started**

Not Planned

DNS Service Provider Capabilities

24 August 2022	deSEC			NS1			Neustar			Cloudflare			(Others)					
	C	D	R	C	D	R	C	D	R	C	D	R	C	D	R	C	D	R
Add DNSKEY records			✓		❑	❑		❑	❑			✓						
Remove DNSKEY records			✓		❑	❑		❑	❑			✓						
Add CDS/CDNSKEY records			✓		❑	❑		❑	❑			❑						
Remove CDS/CDNSKEY records			✓		❑	❑		❑	❑			❑						
Add CSYNC record			✓		❑	❑		❑	❑			o						
Remove CSYNC record			✓		❑	❑		❑	❑			o						

C = Command Line Interface – not usable

D = Dynamic DNS

R = Rest API

✓ **Complete**

❑ **In progress**

o **Planned but not started**

Not Planned

Automation of Multi-Signer Transitions

- Multi-signer group formed (Mid 2021?)
- Music – centralized controller (Early 2022 to 2023)
  - Access into foreign Signers
  - Possible conflict with key rollovers

- DS Automation
  - Polling for CDNS/CDNSKEY records
  - Pushback: scaling, delay

About cross-organization communication

- Push: Sending system has write access into receiving system
  - Requires access c]]]]redentials.
- Pull: Receiving syste]]m scans for info posted by Sending system
  - Solves access crede]ntial problem, but scales poorly and imposes potentially lengthy delays.

- Breakthrough: Generalized Notify
  - Sending system sends a “pulse” to Receiving system
  - Receiving system retrieves data from Sending system

Distributed Multi-Signer

- The centralized control model of Music required access to all Signers.
- This turned out to be a showstopper
- A distributed model is now being designed
- Zone owner controls the configuration via HSYNC records
  - HSYNC record introduces a signer and specifies key parameters
    - Contact details for inter-organization communication
    - Etc.

Status and Issues

- Design is in progress
- Implementation and testing to follow
- Issue: Do key rolls have to be suspended during onboarding of a new Signer?
  - Hopefully not

- Regular reports in this forum