Multi-Signer Testing: Current Plans and Thoughts re Testbeds and Scenarios

Steve Crocker

steve@shinkuro.com

Organizing Testing and Observation

- Continuous, publicly visible multi-signer transitions

- Test the proof-of-concept Multi-Signer controller (MUSIC)
- Test the interfaces of the available DNS software packages and services
- Test the observation system

- Multiple volunteers; more welcome

Multi-Signer Processses and Steps

- A multi-signer process is a defined sequence of steps
- At present, two processes are defined in the multi-signer draft:
  - Adding a signing DNS operator
  - Removing a signing DNS operator
- The steps needed to add or remove a signing DNS operator consist of the actions needed to get all the signers “in sync”. Examples include:
  - Synchronizing DNSKEYs between two or more signers
  - Adding a CDS RRset to all signers
  - Etc.

Testers Wanted

- The MUSIC software is available for testing
- Current testing is taking place within IIS
  - Roger Murray
  - Johan Stenstam
- Additional testers are desired…
  - Please volunteer!

Future Multi-Signer Scenarios

- Scenarios
  - A sequence of transitions
  - Continuous repetition
- Observation of success and glitches
  - “glitch” = resolution or validation failure
- Demonstrate that glitches occur only when timing constraints are violated
- For further study
  - Interaction between key rollovers and multi-signer transitions

Open Issues for multi-signer testbeds

Current testbeds

- Key rollovers
  - Not during additions and removals
  - During additions or removals
- Parent needs to do CDS/CDNSKEY scanning
  - Currently run by hand

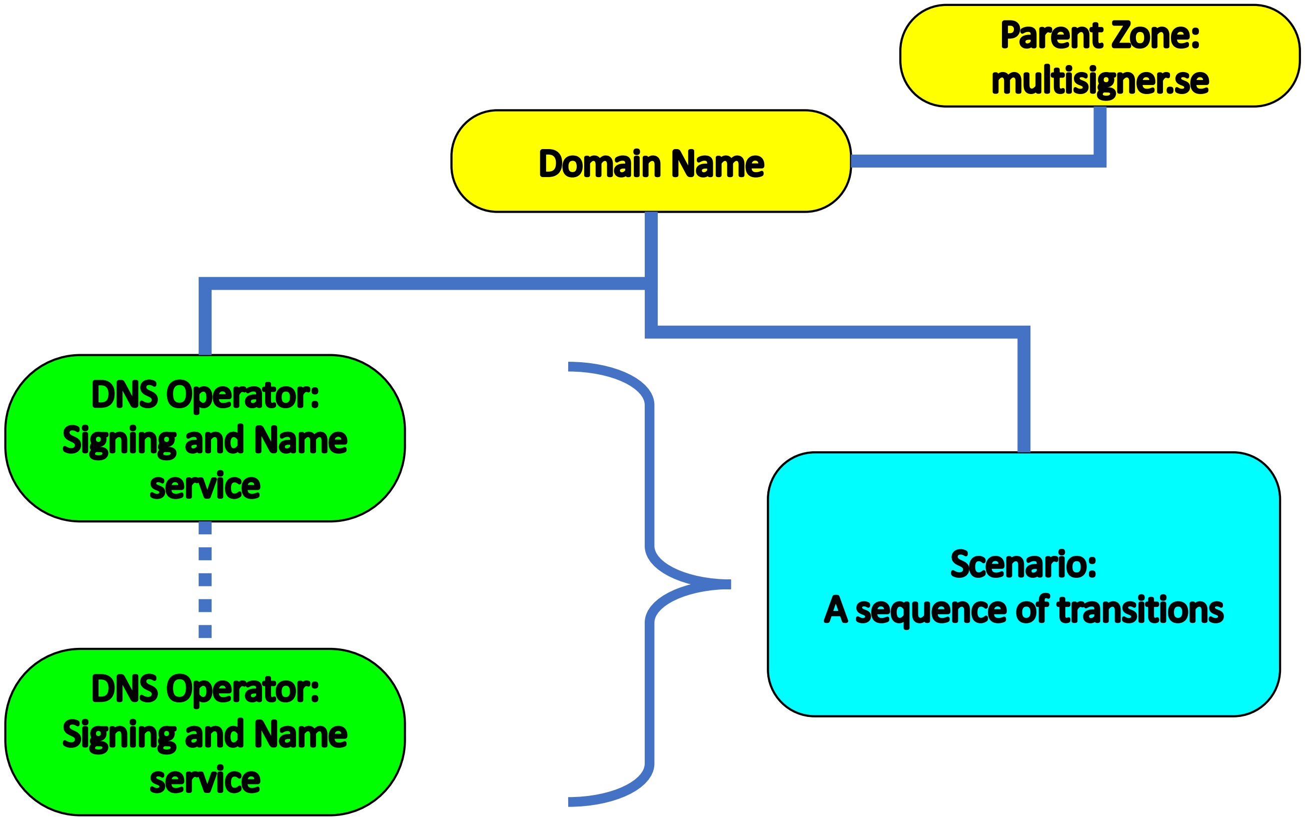
Production operation

- Parent needs automated CDS/CDNSKEY and CSYNC scanners for production operation

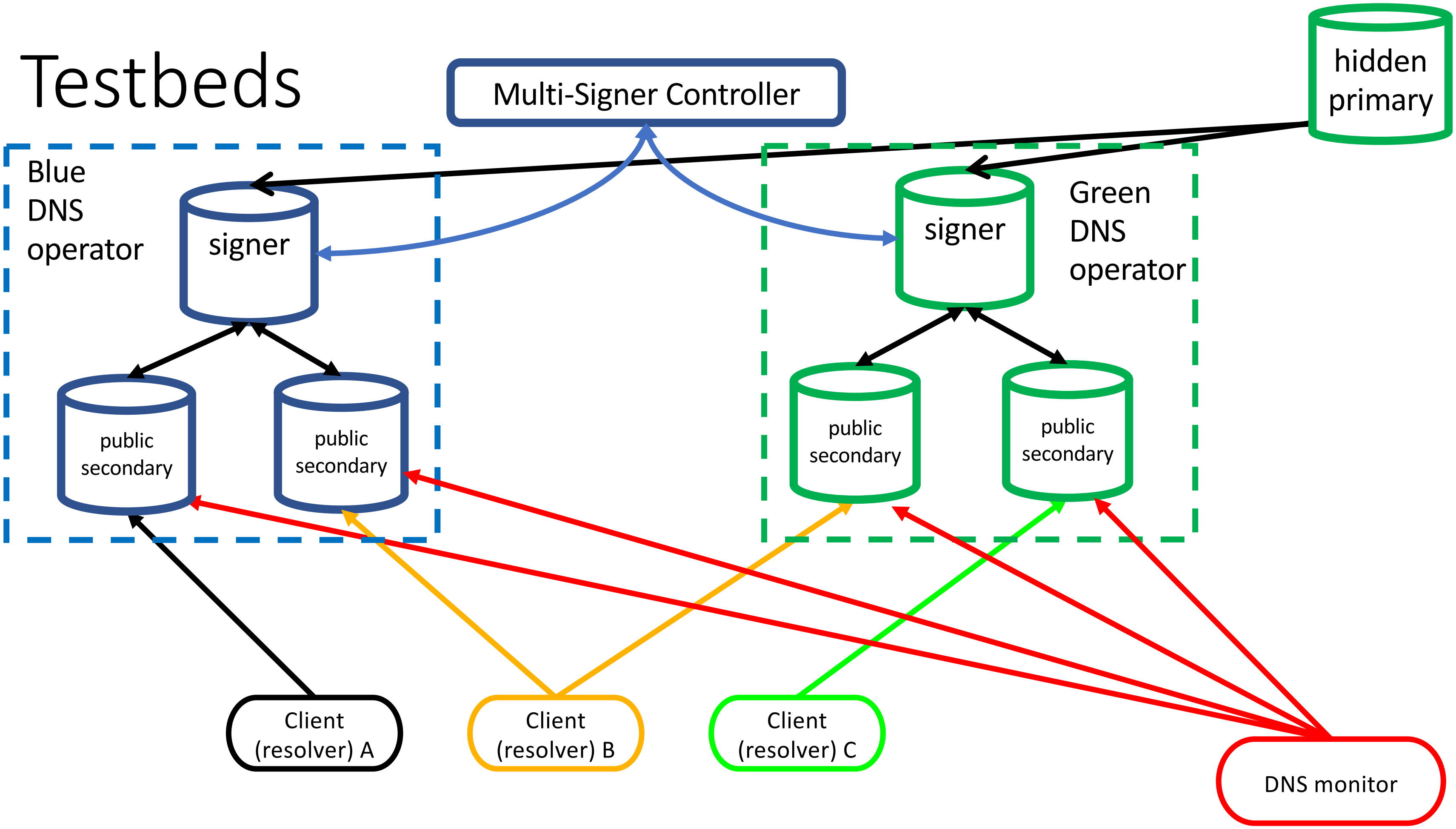
Changing the DNSSEC Keys In a Zone

- The DNSKEYs (i.e. the public keys) for a DNSSEC signed zone need to change now and then.
  - The changes will accomplish some type of goal
  - Other possible changes may break the zone (validation of zone data will fail).
- “Normal” DNSSEC Key Rollovers constitute a series of changes
  - With the goal of replacing the old keys with new keys
- Multi-signer processes constitute another set of changes
  - With the goal of synchronizing multiple “signers”
- Key rollovers and multi-signer processes must not break validation
  - But they are different changes, because the goals are different

Domain Names, Signer/Servers & Scenarios



Testbeds


Multi-Signer Controller
hidden primary
Blue DNS operator
signer
public secondary
public secondary
Green DNS operator
signer
public secondary
public secondary
Client (resolver) A
Client (resolver) B
Client (resolver) C
DNS monitor

(Future) DNS Signer/Server Attributes

- DNS Operator designation
- Operator, Point of Contact
- DNS Software package (interfaces)
- Nameservers

Testing is currently all in a single laboratory

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**	o	**Planned but not started**
❑	**In progress**	▨	**Not Planned**

Multi-Signer Controller Components

- A finite state machine
  - Understands the “add-signer” and “remove-signer” transitions
  - Each transition consists of several steps
  - Each step has defined pre- and post-conditions for the step to take place
- A continuously running “engine”
  - Maintains the FSM progress for each zone
  - Will automatically push zones to the next step when safe and correct to do so
- An API for management access, including operations like:
  - Add or remove “signers” (signing DNS services)
  - Add or remove zones
  - Check current transition status for each zone