DS Updates & Multi-Signer Coordination Episode 9

ICANN 75, Kuala Lumpur

Steve Crocker & Shumon Huque

steve@shinkuro.com

shuque@gmail.com

Two gaps in the DNSSEC protocol specs

- Automation of DS updates
  - Periodic key changes
  - New key in the child's zone requires new parent DS record
  - Registrar has access to parent
    - If Registrar is providing signed DNS service, conveying new DS to parent is easy
  - **But 3rd party DNS provider does not have access to the Registry**

- Multiple DNS Providers
  - Each DNS provider signs with its own keys (RFC 8901 Model 2)
  - Each must include ZSKs from the other providers
  - No defined way to share the keys
  - Needed for:
    - **Capacity and high reliability**
    - **Glitch-free transfer of a signed zone from one DNS Provider to another (Disruptions can be worse than expected)**

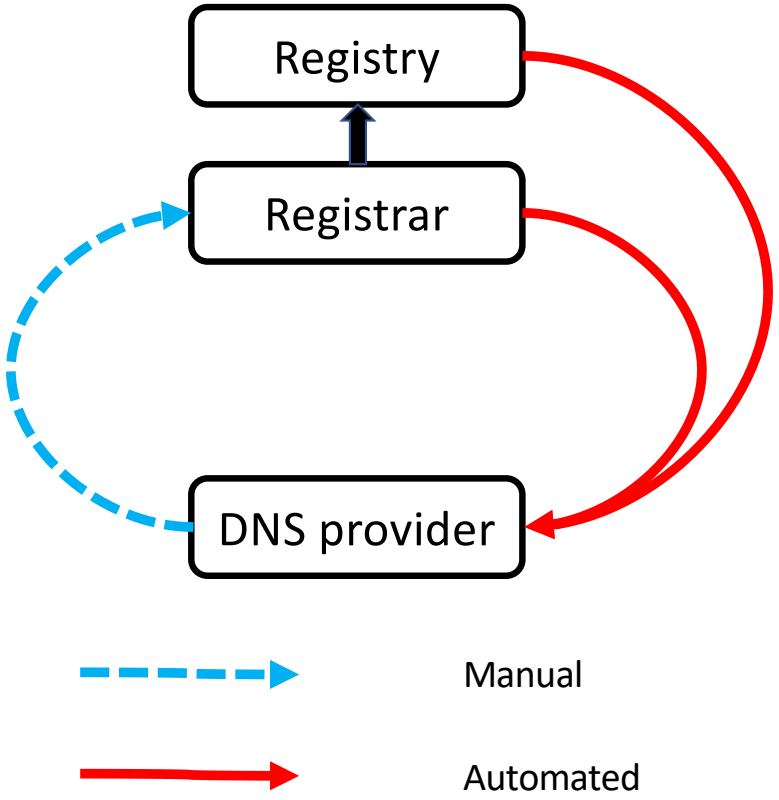
Agenda

#	Title	Speaker
3.1	Overview: DNSSEC Provisioning Automation	Steve Crocker, Shinkuro, Inc.
3.2	GoDaddy DNSSEC DS	Brian Dickson, GoDaddy
3.3	Automation of DS Management	Peter Thomassen, deSEC/SSE
3.4	MUSIC : Multi-Signer Controller - Status Update	Johan Stenstam & Roger Murray , Swedish Internet Foundation
3.5	Multi-signer DNSSEC with NS1 Managed DNS	Jan Včelák, NS1
3.6	Multi-Signer Testing: Testbeds and Scenarios	Steve Crocker, Shinkuro, Inc.

DS Updates

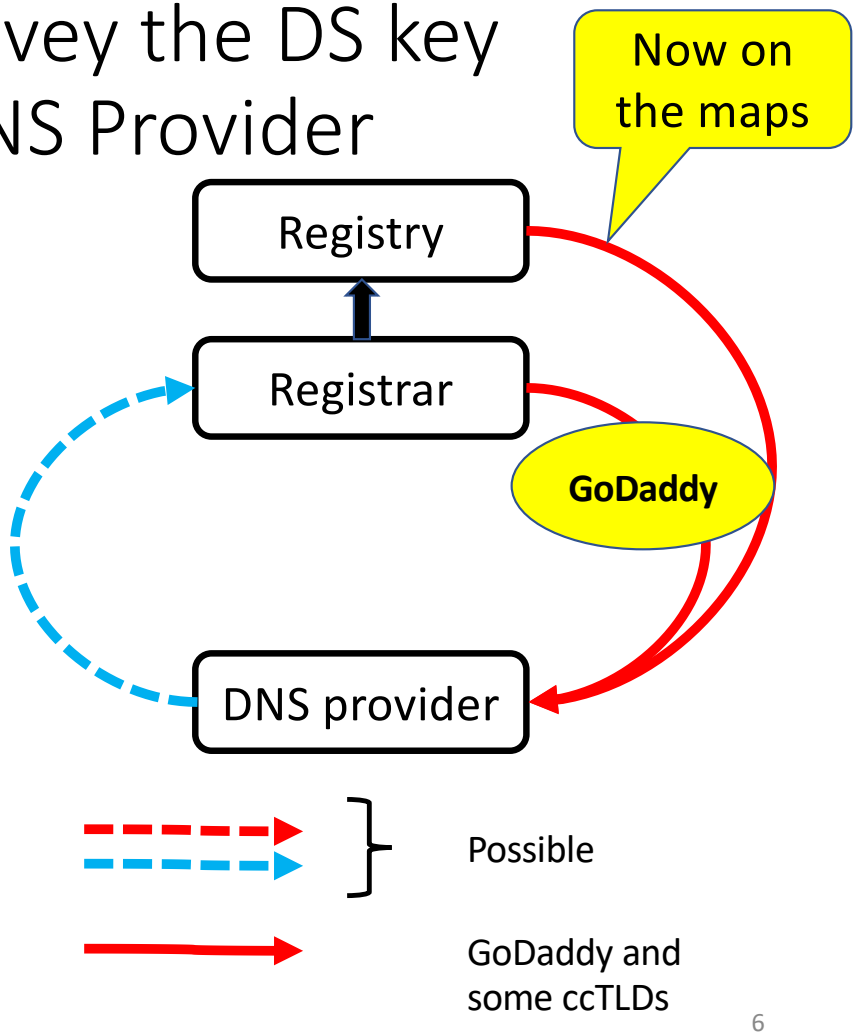
Possible Ways to Convey the DS key from 3rd party DNS Provider

	Direction	
Upper Side	Push (Calling) DNS Provider calls API at Ry, Rr	Pull (Polling) DNS Provider publishes CDS and/or CDNSKEY
Registry	1. Requires API	3. RFC 8078
Registrar	2. Requires API	4. RFC 8078



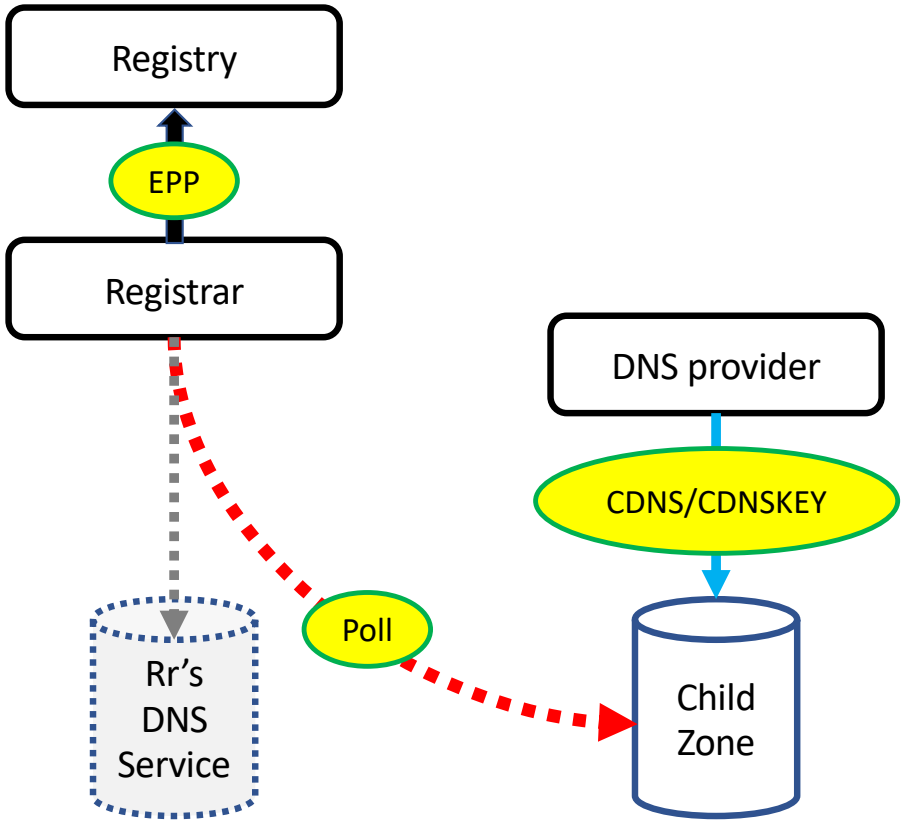
Possible Ways to Convey the DS key from 3rd party DNS Provider

	Direction	
Upper Side	Push (Calling) DNS Provider calls API at Ry, Rr	Pull (Polling) DNS Provider publishes CDS and/or CDNSKEY
Registry	1. Requires API	3. RFC 8078
Registrar	2. Requires API	4. RFC 8078



Possible Ways to Convey the DS key from 3rd party DNS Provider

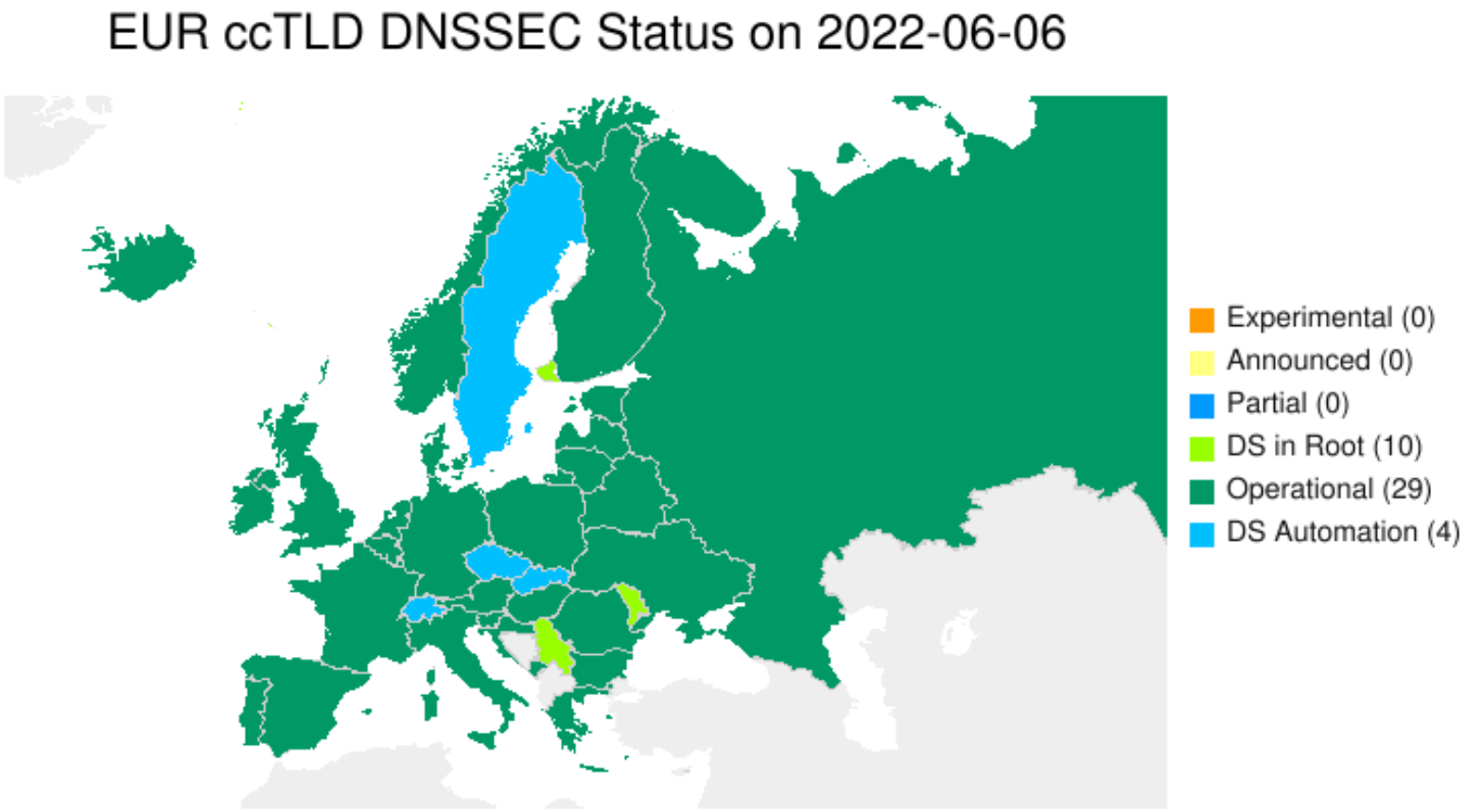
	Direction	
Upper Side	Push (Calling) Call Rr or Rt API	Pull (Polling) Publish CDS/ CDNSKEY
Registry		
Registrar		4. RFC 8078



Registrar polls for CDS/CDNSKEY records.

GoDaddy now testing

ccTLDs now implementing CDS/CDNSKEY Scanning



Actions and Issues

- GoDaddy now testing scanning of customer zones
- SSAC exploring recommendation of DS automation support

- Issue: Scanning is time-consuming. Doesn’t scale well

DS Management Score Card

24 Feb 2022	CDS/CDNSKEY Scanning	DS Bootstrapping
Designed	✓	✓
Specifications	RFC 8078	draft-thomassen-dnsop-dnssec-bootstrapping
In Progress	.CL, GoDaddy	.CL, GoDaddy, CoCCA and others
Done	Several ccTLDs	

DNSSEC:
Multi-DNS Provider Coordination & Glitch-Free Provider Change

“Glitch-Free” = No loss of resolution AND no loss of validation

Multi-Signer Software Project

The Swedish Internet Foundation

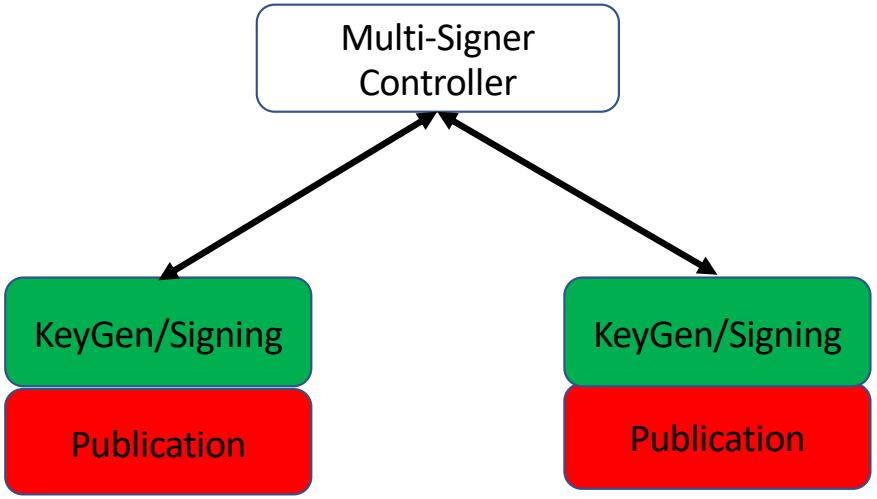
deSEC

Salesforce

George Mason University

Shinkuro, Inc.

Cross-Signing: Communicating ZSKs & KSKs



Registrant coordinates using a Multi-Signer Controller

Multi-Signer Operational* Demonstrations

* Operational = Repeatable

- Adding a DNS operator
- Key rollover in one of the operations
- (Concurrent key rollover – will it work?)
- Removal of an operator
- Observation of glitch-free operation for each of the above

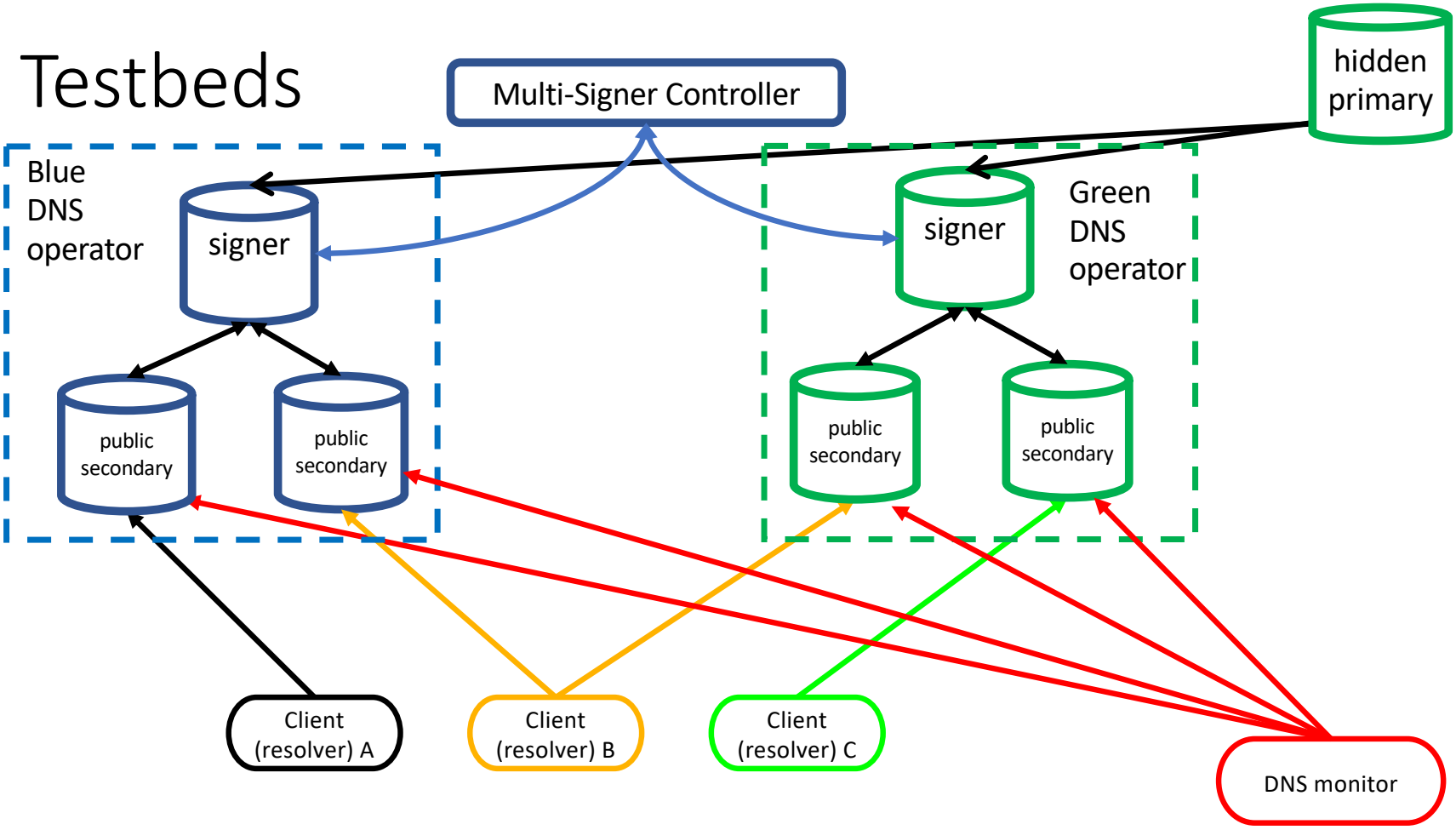
- Repeat of each, violating the timing constraints
- Observation of glitches when timing constraints are violated

Multi-Signer Big Picture

✓ Done
❑ In progress
○ Future
• Unspecified/Mixed

- ✓Protocol (RFC 8901)
- Software
  - Multi-Signer Controller
    - ❑ Design
    - ❑ Implementation
  - DNS Server Interfaces
    - ❑ BIND, PowerDNS, …
  - Services/Operations
    - ❑ deSEC, NS1, Neustar …
- Analysis
  - ✓Text
  - ○ Proof
- Observation
  - Longitudinal
  - Real-time
    - ○ System Design
    - ○ Deployment
    - ○ Experiments
      - ○ Positive
      - ○ Negative

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

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

Multi-Signer Score Card

3 Mar 2022	Designed	In Progress	Done
Specifications	✓	**draft-wisser-dnssec-automation**	**RFC 8901** **RFC 8078**
Multi-Signer Controller	✓	✓	
Name Server Software Capabilities	✓	**Knot**	**PowerDNS, BIND**
DNS Service Provider Capabilities	✓	**NS1, Neustar, Cloudflare**	**deSEC**
Documents			
Observation & Analysis	✓	✓	
Demonstrations			

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

References

DNSSEC Provisioning Automation "Episodes" Standing Panel at ICANN DNSSEC Workshops

Episode	Date	Meeting	DNSSEC Provisioning Automation Sessions
1	11 Mar 2020	ICANN 67 "Cancún"	https://tinyurl.com/5dwxfz2v
2	22 Jun 2020	ICANN 68 "Kuala Lumpur"	https://tinyurl.com/m8eraezu
3	21 Oct 2020	ICANN 69 "Hamburg"	https://tinyurl.com/f8ma6347
4	24 Mar 2021	ICANN 70 "Cancún"	https://tinyurl.com/bj69sn87
5	14 Jun 2021	ICANN 71 "The Hague"	https://tinyurl.com/t2fcefr6
6	27 Oct 2021	ICANN 72 "Seattle"	https://tinyurl.com/32aeptd3
7	9 Mar 2022	ICANN 73 "San Juan"	https://tinyurl.com/yzyb29s9
8	13 Jun 2022	ICANN 74 The Hague	

Internet Society DNSSEC Maps

https://www.internetsociety.org/deploy360/dnssec/maps/

Episode 1: 20 March 2020 “Cancún”

#	Title	Speaker	TinyURL
	Steve Crocker will outline the problems and the space of possible solutions	Steve Crocker, Shinkuro, Inc	https://tinyurl.com/4w2eck8j
	DS Automation		
	Registry:	James Galvin, Afilias; Erwin Lansing, DK; and Gavin Brown, CentralNic for SK	
	Multisigner Project		
	Registrar	Brian Dickson, GoDaddy; Jothan Frakes, PLISK; and Ólafur Guðmundsson, Cloudflare	
	DNS Provider	Ólafur Guðmundsson, Cloudflare	

Episode 2: 22 June 2020 “Kuala Lumpur”

#	Title	Speaker	TinyURL
	DS Updates and Multi-Signer Coordination	Steve Crocker, Shinkuro, Inc	https://tinyurl.com/vzu58xzv
	DS Automation		
	Multi-Signer DNSSEC	Shumon Huque, Salesforce, Inc	https://tinyurl.com/6sche46m
	Multisigner Project		
	Support for Multi-Signer DNSSEC	Paul Ebersman, Neustar	https://tinyurl.com/4kmcxmfw
	GoDaddy DNSSEC Signing and DS Updates	Brian Dickson, GoDaddy	https://tinyurl.com/bev24h6u
	Managing DNSSEC via API	Jothan Frakes, PLISK	https://tinyurl.com/w6ce9mu9
	Automated DNSSEC in CZ	Jaromír Talíř, CZ.NIC	https://tinyurl.com/dphwhby4
	Support for and adoption of CDS in .CH and .LI	Oli Schacher, SWITCH	https://tinyurl.com/22c6t6sn

Episode 3: 21 October 2020 “Hamburg”

#	Title	Speaker	TinyURL
I.	Overview: Framing the Issues	Shumon Huque and Steve Crocker	https://tinyurl.com/44dttx7p
II.	• SE DNSSEC History Present Future	Ulrich Wisser, SIF*	https://tinyurl.com/35m44a67
	• Deploying DNSSEC in a Large Enterprise	Han Zhang & Allison Mankin, Salesforce	https://tinyurl.com/jn8d9cv8
	DS Automation		
III.	• DS Automation	Shumon Huque, Salesforce	https://tinyurl.com/nnma8aau
	• DS Automation: Non-technical Considerations	James Galvin Ph.D., Afilias, Inc	https://tinyurl.com/p692jjzu
	• GoDaddy DNSSEC DS – Current and Proposed DS Update Methods	Brian Dickson, GoDaddy	https://tinyurl.com/8d695va9
	• Gathering the Childrens DS’	Mark Elkins, Posix	https://tinyurl.com/59697hm5
	• Evolving the DNSSEC Deployment Maps	Dan York, Internet Society	https://tinyurl.com/ytz9xw8k
	Multisigner Project		
IV.	• DNSSEC Census: Are DNSKEY Transitions Working?	Eric Osterweil, George Mason Univ	https://tinyurl.com/7tzwr6hr
	• Automating Multiple Signers	Shumon Huque, Salesforce	https://tinyurl.com/va53mwy8
V.	• Action Items:	Steve Crocker	https://tinyurl.com/2zykj7zs

*SIF = The Swedish Internet Foundation

Episode 4: 24 March 2021 “Cancún”

#	Title	Speaker	TinyURL
4.1	Panel Overview	Steve Crocker, Shinkuro, Inc	https://tinyurl.com/msaakbud
	DS Automation		
4.2	DS Automation at GoDaddy	Brian Dickson, GoDaddy	https://tinyurl.com/hwx6hy52
	Multisigner Project		
4.3	Intro to Multisigner Project Foundations	Shumon Huque, Salesforce	https://tinyurl.com/4cwcndrr
4.4	Multisigner Protocols	Ulrich Wisser, SIF*	https://tinyurl.com/v4y727sj
4.5	Multisigner Testbed	Ulrich Wisser, SIF*	https://tinyurl.com/cm3uuhk3
4.6	Multisigner Multisigner support at deSEC	Peter Thomassen, Secure Systems Engineering	https://tinyurl.com/eyymfh2z
4.7	DNSKEY Transition Observatory	Ravichander, Osterweil, GMU	https://tinyurl.com/vdwpj4wp
4.8	Anatomy of DNSSEC Transitions	Osterweil, Tehrani, Schmidt, Waehlisch	https://tinyurl.com/ssfxwr3x

*SIF = The Swedish Internet Foundation

Episode 5: 14 June 2021 “The Hague”

#	Title	Speaker	TinyURL
3.1	DNSSEC Provisioning Automation Overview	Steve Crocker, Shinkuro, Inc	https://tinyurl.com/5a66kvpx
	DS Automation		
3.2	CDS scanning at RIPE NCC	Ondřej Caletka, RIPE NCC	https://tinyurl.com/t673a7px
3.3	The State of DNSSEC Automated Provisioning	Wilco van Beijnum, University of Twente	https://tinyurl.com/ntv5um3k
	Multisigner Project		
3.4	Multi-Signer Project Overview and Status	Ulrich Wisser, SIF*	https://tinyurl.com/4uyvps4u
3.5	BIND DNSSEC Provisioning Interfaces	Matthijs Mekking, Internet Systems Consortium	https://tinyurl.com/56p3pye7
3.6	PowerDNS DNSSEC Provisioning Interfaces	Peter van Dijk, PowerDNS	https://tinyurl.com/vracytyp

*SIF = The Swedish Internet Foundation

Episode 6: 27 October 2021 “Seattle”

#	Title	Speaker	TinyURL
6.1	DNSSEC Provisioning Automation Overview	Steve Crocker, Shinkuro, Inc	https://tinyurl.com/5n7fccdv
6.2	Recent DNSSEC Automation Developments in .CZ	Jaromír Talíř, CZ.NIC	https://tinyurl.com/2ddcukaj
6.3	CDS & CDNSKEY Verification in Zonemaster	Mats Dufberg, SIF	https://tinyurl.com/4jr3nyzx
6.4	Authentication Bootstrapping of DNSSEC Delegations	Peter Thomassen, deSEC	https://tinyurl.com/mswzz84x
6.5	DNS Resolver Observatory	Pouyan Tehrani, Freie Universität Berlin	https://tinyurl.com/mry4rrmr
6.6	Introduction to CSYNC	Ulrich Wisser, SIF	https://tinyurl.com/yxhf22a5

*SIF = The Swedish Internet Foundation

Episode 7: 9 March 2022 “San Juan”

#	Title	Speaker	TinyURL
3.1	Overview: DNSSEC Provisioning Automation	Steve Crocker, Shinkuro, Inc.	https://tinyurl.com/4nxjzucn
	DS Automation		
3.2	GoDaddy CDS Support Update	Brian Dickson, GoDaddy	https://tinyurl.com/5n7hs98s
3.3	CSYNC implementation	Ulrich Wisser, SIF	https://tinyurl.com/589m8uw2
3.4	Authenticated Bootstrapping of DNSSEC Delegations	Nils Wisiol, deSEC, Technische Universität Berlin	https://tinyurl.com/5e65sdpp
3.5	SSAC DS Automation Work Party	Steve Crocker, Shinkuro, Inc.	https://tinyurl.com/p9f3auyu
	Multi-Signer Project		
3.6	Making MUSIC with DNSSEC	Johan Stenstam, Roger Murray, SIF	https://tinyurl.com/2turpbuh
3.7	RFC Adjustments for Multi-Signer	Shumon Huque, Salesforce	https://tinyurl.com/3cvuspnp
3.8	DNS(SEC) Views	P.F. Tehrani, et al, Weizenbaum Institute / Fraunhofer FOKUS	https://tinyurl.com/566t57s2

*SIF = The Swedish Internet Foundation

Episode 8: 13 June 2022 The Hague

#	Title	Speaker	TinyURL
5.1	Overview: DNSSEC Provisioning Automation	Steve Crocker, Shinkuro, Inc.	https://tinyurl.com/bdcwym2c
	DS Automation		
5.2	GoDaddy DNSSEC DS	Brian Dickson, GoDaddy	https://tinyurl.com/bw95csdu
5.3	Updating Secure Delegations in the DNS Root Zone	Kim Davies, ICANN/PTI	https://tinyurl.com/yzkuthnu
5.4	Update on Authenticated DNSSEC Bootstrapping	Peter Thomassen, deSEC/SSE	https://tinyurl.com/ea7vdr4e
5.5	SSAC DS Automation Work Party	Steve Crocker, Shinkuro, Inc.	https://tinyurl.com/5235c7he
	Multi-Signer Project		
5.6	Making Music with DNSSEC: Status Update; The Need to Avoid False Notes	Johan Stenstam, Swedish Internet Foundation	https://tinyurl.com/46bz9yh6
5.7	Provisioning Multi-Signer DNSSEC with Cloudflare	Christian Elmerot, Cloudflare	https://tinyurl.com/4cz36r5b

Thanks!