

ICANN DNSSEC and Security Workshop DNSSEC Provisioning Automation Panel Episode 13

ICANN 79, San Juan, PR

Steve Crocker and 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)**

Provisioning Adjacent Issues

- Today's panel includes both DS Automation issues, as usual, and some "adjacent" issues:
- HSM replacement
- Debates about going unsigned
- Computational overload

Panel Agenda

2.1	Panel Overview	Steve Crocker, Edgemoor Research Institute
2.2	HSM Evaluation and Preparation for Algorithm Rollover	Kim Davies, ICANN/PTI
2.3	Knot DNS & PowerDNS DNSSEC Bootstrapping Impl'n Status	Peter Thomassen, deSEC/SSE
2.4	Do Not Go Unsigned	Shumon Huque, Salesforce & Eric Osterweil, GMU
2.5	Two Trendy Ways to Hang your DNS Cache	John Levine, Standcore LLC
2.6	Verisign's Transition to Elliptic Curve DNSSEC	Duane Wessels, Verisign

References

DNSSEC Provisioning Automation “Episodes” 2020 through 2022

Episode	Date	Meeting	DNSSEC Provisioning Automation Sessions
1	11 Mar 2020	ICANN 67 “Cancún”	https://tinyurl.com/5dwx fz2v
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	https://tinyurl.com/yn4c45t7
9	21 Sep 2022	ICANN 75 Kula Lumpur	https://tinyurl.com/46fhfkjs

Maps now at George Mason University CARE/MSL: <https://maps.dnssec.gmu.edu/>

DNSSEC Provisioning Automation “Episodes” 2023 - present

Episode	Date	Meeting	DNSSEC Provisioning Automation Sessions
10	15 Mar 2023	ICANN 76 Cancún	https://tinyurl.com/yefd64hw
11	12 Jun 2023	ICANN 77 Washington	https://tinyurl.com/4xxz3uxw
12	25 Oct 2023	ICANN 78 Hamburg	https://tinyurl.com/8ffyc4c
13	6 Mar 2024	ICANN 79 San Juan	

Maps now at George Mason University CARE/MSL: <https://maps.dnssec.gmu.edu/>

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, Afiliias; 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 Wissner, 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., Afiliis, 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/4cwendrr
4.4	Multisigner Protocols	Ulrich Wissner, SIF*	https://tinyurl.com/v4y727sj
4.5	Multisigner Testbed	Ulrich Wissner, 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 Wissner, 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/3cvusnpn
3.8	DNS(SEC) Views	P.F. Tehrani, et al, Weizenbaum Institute / Fraunhofer FOKUS	https://tinyurl.com/566t57s2

*SIF = The Swedish Internet Foundation

5 March 2024

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

Episode 9: 21 September 2022 Kuala Lumpur

#	Title	Speaker	TinyURL
3.1	Overview: DNSSEC Provisioning Automation	Steve Crocker, Shinkuro, Inc.	https://tinyurl.com/mry27pd2
DS Automation			
3.2	GoDaddy DNSSEC DS	Brian Dickson, GoDaddy	https://tinyurl.com/4yu9934p
3.3	Automation of DS Management	Peter Thomassen, deSEC/SSE	https://tinyurl.com/2p9h8wxx
Multi-Signer Project			
3.4	MUSIC : Multi-Signer Controller - Status Update	Johan Stenstam & Roger Murray , Swedish Internet Foundation	https://tinyurl.com/5h4wr8zj
3.5	Multi-signer DNSSEC with NS1 Managed DNS	Jan Včelák, NS1	https://tinyurl.com/3amn7ekd
3.6	Multi-Signer Testing: Testbeds and Scenarios	Steve Crocker, Shinkuro, Inc.	https://tinyurl.com/ya7kfw3j

Episode 10: 15 March 2023 Cancún

#	Title	Speaker	TinyURL
4.1	Overview: DNSSEC Provisioning Automation	Steve Crocker, Edgemoor Research Institute	https://tinyurl.com/y439v4uu
4.2	DNS child updates in the gTLD space	Francisco Arias, Sr. Director, GDS Technical Services, ICANN org	https://tinyurl.com/4ytwajs2
4.3	GoDaddy DNSSEC CDS to DS Polling Status	Brian Dickson, GoDaddy	https://tinyurl.com/ym3avrmc
4.4	CDS Scanning rollout at CentralNic	Gavin Brown, Technical Fellow, CentralNic Group PLC	https://tinyurl.com/3d7kdzce
4.5	CDNSKEY Support in TANGO Registry Services	Michael Bauland, Knipp Medien und Kommunikation GmbH	https://tinyurl.com/mr37vut9
4.6	The State of DS Automation: Deployments and Current Work	Peter Thomassen, deSEC/SSE	https://tinyurl.com/3dxzjz3k
4.7	The New DNSSEC Deployment Maps and DNSSEC Views	Koushik Sura Bhaskar, George Mason University	https://tinyurl.com/y8zcdp59

Episode 11 (Part 1): 12 June 2023 Washington

#	Title	Speaker	TinyURL
1.1	Workshop Overview	Jacques Latour, Steve Crocker	https://tinyurl.com/2xs9atva
1.2	The DNSSEC Vision	Rod Rasmussen, Jacques Latour, Danny McPherson, Russ Mundy, Eric Osterweil	https://tinyurl.com/25rte5ra
1.3*	ICANN Org's view of DNSSEC	Rod Rasmussen, Matthew Shears, Adiel Akplogan	
1.4	Automation of DS updates in gTLD space	Matt Larson, Francisco Arias, Mary Wong	https://tinyurl.com/bdfbbb6m
1.5*	Review of key organizational issues	Peter Thomassen, Steve Crocker	

* = Panel without slides

Episode 11 (Part 2): 12 June 2023 Washington

#	Title	Speaker	TinyURL
2.1	DS Automation: Current work	Shumon Huque, Matthijs Mekking, Ondrej Filip	https://tinyurl.com/bdeh6jp5 https://tinyurl.com/49enj4jr https://tinyurl.com/3rwrpf68
2.2	Bootstrapping DNSSEC: Methods, Implementations, Open Issues	Peter Thomassen	https://tinyurl.com/5essnja7
2.3	Scalability of Scanning	Peter Thomassen	https://tinyurl.com/bkw4msfz
2.4	Generalized Notifications	Peter Thomassen & Johan Stenstam	https://tinyurl.com/29h7u2j9
2.5	DS Automation Work Party Draft Recommendations	Russ Mundy, Shumon Huque, Peter Thomassen, Steve Crocker	https://tinyurl.com/5n7acvvp
2.6*	Review of key system issues		

* = Panel without slides

Episode 12: 6 May 2023 Hamburg

#	Title	Speaker	TinyURL
2.1	Panel Overview	Steve Crocker, Edgemoor Research Institute	
2.2	Generalised Notifications: Infrastructure for Robust Multi-Signer Operations	Johan Stenstam, Swedish Internet Foundation	
2.3	DS Automation Report	Peter Thomassen, deSEC/SSE	
2.4	Documenting and Managing Algorithm Lifecycles	Steve Crocker, Russ Housley, Peter Thomassen	
2.5	DNS Provider Coordination of Multi-Signer and DNSSEC Automation	Steve DeJong, UltraDNS-Vercara	
2.6	Monitoring and Evaluating ENS through the INSO	Eric Osterweil, George Mason University	
2.7	DNSSEC - is the juice still worth the squeeze?	Warren Kumari	

Thanks!