

ICANN DNSSEC and Security Workshop Single Focus on DS Updates Automation Episode 11

ICANN 77, Washington, DC

Steve Crocker, Shumon Huque, Jacques Latour, Peter Thomassen

steve@shinkuro.com, shuque@gmail.com,
jacques.latour@cira.ca, peter@desec.io

A Departure from our usual program

Usually, we address multiple topics.

- DNSSEC Provisioning Automation (for the past 3+ years)

- DS Automation

- Multi-Signer protocol

A Departure from our usual program

Usually, we address multiple topics.

DNSSEC Provisioning Automation

DS Automation

Multi-Signer protocol



Today:
Our entire
program

NZ websites down - Security update causes widespread internet outages

29 May 2023

30 May 2023

Widespread website, app outages: InternetNZ apologises for 'change of house keys' gone haywire

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)**

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 key (RFC 8901 Model 2)
- Each DNS provider has its own keys for the other DNS providers
- No one has access to the keys of the other DNS providers
- New DNS providers can be added at any time
 - Capacity and performance
 - Glitch-free transfer of a signed zone from one DNS Provider to another (Disruptions can be worse than expected)

Wait until ICANN 78
October 2023
Hamburg, DE

Some key points

- Tools, technology and services should be available prevent the operator or a system from breaking a secure delegation
- Increase the focus on the VALIDATION of DNSSEC automation
- SSAC is working on a DNSSEC Automation report; your feedback is important
- There are policies and contractual impediments 'real or perceived' that prevents us from doing our best to automate DNSSEC
- We want to hear from you, your feedback is important, this is a policy meeting.

Part 1: Larger context, organizational matters

	1.1	Workshop Overview	Jacques Latour, Steve Crocker
	1.2	The DNSSEC Vision	Rod Rasmussen, Jacques Latour, Danny McPherson, Russ Mundy, Eric Osterweil
*	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
*	1.5	Review of key organizational issues	Peter Thomassen, Steve Crocker

* = Panel without slides

Novice

Intermediate

Expert

Part 2: Technical Stuff

	2.1	DS Automation: Current work	Shumon Huque, Matthijs Mekking, Ondrej Filip
	2.2	Bootstrapping DNSSEC: Methods, Implementations, Open Issues	Peter Thomassen
	2.3	Scalability of Scanning	Peter Thomassen
	2.4	Generalized Notifications	Peter Thomassen & Johan Stenstam
	2.5	DS Automation Work Party Draft Recommendations	Russ Mundy, Shumon Huque, Peter Thomassen, Steve Crocker
*	2.6	Review of key system issues	

* = Panel without slides

Novice

Intermediate

Expert

Feedback, please

- Audience response at the end of each part of this workshop
- SSAC is working on a DNSSEC DS automation report
 - Draft recommendations at the end of this workshop
- The workshop addresses both policy and technical aspects of DS automation. Community input is very important to achieve effective results for both.
 - What are the policy issues for deployment of DS automation solutions?
 - Contract modification(s), modified policies, etc.
 - What technical capabilities are needed for deployment of DS automation?
 - New protocols, modifications/extensions to existing protocols, capabilities needed to validate automated DS updates, etc.
- We want to hear from YOU!!!

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/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
10	15 Mar 2023	ICANN 76 Cancún	https://tinyurl.com/yefd64hw

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/44dtx7p
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, Waehlich	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/3cvusnpn
3.8	DNS(SEC) Views	P.F. Tehrani, et al, Weizenbaum Institute / Fraunhofer FOKUS	https://tinyurl.com/566t57s2

*SIF = The Swedish Internet Foundation

12 June 2023

19

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

Thanks!