

# Report of Public Comments

<b>Title:</b>	<b>Consultation on Root Zone KSK Rollover</b>																				
<b>Publication Date:</b>																					
<b>Prepared By:</b>	Terry Manderson																				
<table border="1"> <tr> <td colspan="2"><b>Comment Period:</b></td> </tr> <tr> <td>Comment Open Date:</td> <td>8 March 2013</td> </tr> <tr> <td>Comment Close Date:</td> <td>12 April 2013</td> </tr> <tr> <td>Reply Close Date:</td> <td>31 May 2013</td> </tr> <tr> <td>Time (UTC):</td> <td>23:59</td> </tr> </table>		<b>Comment Period:</b>		Comment Open Date:	8 March 2013	Comment Close Date:	12 April 2013	Reply Close Date:	31 May 2013	Time (UTC):	23:59	<table border="1"> <tr> <td colspan="2" style="text-align: center;"><b>Important Information Links</b></td> </tr> <tr> <td colspan="2" style="text-align: center;"><a href="#">Announcement</a></td> </tr> <tr> <td colspan="2" style="text-align: center;"><a href="#">Public Comment Box</a></td> </tr> <tr> <td colspan="2" style="text-align: center;"><a href="#">View Comments Submitted</a></td> </tr> </table>		<b>Important Information Links</b>		<a href="#">Announcement</a>		<a href="#">Public Comment Box</a>		<a href="#">View Comments Submitted</a>	
<b>Comment Period:</b>																					
Comment Open Date:	8 March 2013																				
Comment Close Date:	12 April 2013																				
Reply Close Date:	31 May 2013																				
Time (UTC):	23:59																				
<b>Important Information Links</b>																					
<a href="#">Announcement</a>																					
<a href="#">Public Comment Box</a>																					
<a href="#">View Comments Submitted</a>																					
<b>Staff Contact:</b>	Terry Manderson	<b>Email:</b>	terry.manderson@icann.org																		
<b>Section I: General Overview and Next Steps</b>																					
<p>The Internet Assigned Numbers Authority (IANA) Functions contract (SA1301-12-CN-0035) between ICANN and the United States Department of Commerce, National Telecommunications Information Administration (NTIA) to perform services related to certain interdependent Internet technical management functions calls for a public consultation from all interested and affected parties to help satisfy the following objective:</p> <p>C.2.9.2.f Root Domain Name System Security Extensions (DNSSEC) Key Management –The Contractor shall be responsible for the management of the root zone Key Signing Key (KSK), including generation, publication, and use for signing the Root Keyset. As delineated in the Requirements at Appendix 2 entitled Baseline Requirements for DNSSEC in the Authoritative Root Zone that is incorporated by reference herein as if fully set forth. The Contractor shall work collaboratively with NTIA and the Root Zone Maintainer, in the performance of this function.</p> <p>More specifically, this consultation involves "Appendix 2: Baseline Requirements for DNSSEC in the Authoritative Root Zone," that articulates the contract requirement to perform a scheduled root zone KSK rollover.</p>																					
<b>Section II: Contributors</b>																					
<p><i>At the time this report was prepared, a total of twenty-three (23) community submissions had been posted to the Forum. The contributors, both individuals and organizations/groups, are listed below in chronological order by posting date with initials noted. To the extent that quotations are used in the foregoing narrative (Section III), such citations will reference the contributor's initials.</i></p>																					
<u>Organizations and Groups:</u>																					

Name	Submitted by	Initials
APNIC	George Michaelson & Geoff Huston	APNIC
Internet Society	Dan York & Andrei Robachevsky	ISOC
NLnet Labs	Olaf Kolkman & Jaap Akkerhuis	NLNET
Internet Infrastructure Foundation (.SE)	Anne-Marie Eklund Löwinder & Patrik Wallström	SE
Netnod	Patrik Fältström	NETNOD
Internet Architecture Board	Russ Housley	IAB

#### Individuals:

Name	Affiliation (if provided)	Initials
David Burns		DB
Chris Thompson	University of Cambridge	CT
Steve Crocker	Shinkuro Inc	SC
Mike StJohns		MSJ
Michael Graff		MG
Timothe Litt		TL
Thierry Moreau		TM
Ralf Weber	Nominum Inc	RW
Edward Lewis	NeuStar	EL
Tony Finch		TF
Jaap Akkerhuis		JA
Florian Weimer		FW
Matthäus Wander		MW
Ron Aitchison	ZYTRAX	RA
Doug Barton		DB1

#### Section III: Summary of Comments

*General Disclaimer: This section is intended to broadly and comprehensively summarize the comments submitted to this Forum, but not to address every specific position stated by each contributor. Staff recommends that readers interested in specific aspects of any of the summarized comments, or the full context of others, refer directly to the specific contributions at the link referenced above (View Comments Submitted).*

#### The KSK rollover consultation highlighted seven (7) questions. They were:

1. What prerequisites need to be considered prior to a first scheduled KSK rollover?
2. When should the first scheduled KSK rollover take place?
3. What should the IANA Functions Operator (ICANN) and the other Root Zone Management Partners do to gauge the technical and end-user impact of a KSK rollover following the first scheduled KSK rollover?
4. How often should a scheduled KSK rollover take place, following the first one?

5. How far should the published calendar for scheduled KSK rollovers extend into the future?
6. What public notification should take place in advance of a scheduled KSK rollover?
7. What other considerations are necessary for the Root Zone Management Partners to take into consideration prior, during, and after a planned key roll over?

### ***Posting Summary***

Total Number of Responses submitted: 23

Number of Responses from Individuals: 15 (with two (2) supplemental posts)

Number of Responses from Organisations: 6

Number of Responses opposed to a KSK roll: 3

Number of Responses specifically in favor of multiple KSK rolls: 10

Number of Responses specifically mentioning the use of RFC5011: 9

Number of Responses off topic: 1

### ***Summary of the critical Responses:***

#### **1. What prerequisites need to be considered prior to a first scheduled KSK rollover?**

Respondents, in the majority, called for ICANN to establish a set of tests and measurements, with a test-bed, before embarking on a RFC5011 KSK roll. Lines of communication need to be established during testing phases and methods for success evaluation constructed.

#### **2. When should the first scheduled KSK rollover take place?**

Respondents, in the majority, highlighted that the KSK rollover should be performed as soon as practical with an emphasis on preparedness.

#### **3. What should the IANA Functions Operator (ICANN) and the other Root Zone Management Partners do to gauge the technical and end-user impact of a KSK rollover following the first scheduled KSK rollover?**

Respondents, in the majority, proposed that measurements and monitoring where the key modes to gauge the impacts.

**4. How often should a scheduled KSK rollover take place, following the first one?**

There appeared to be no specific trends in responses, suffice to highlight that performing multiple regular KSK rolls was operationally responsible. Responses highlighted schedules between six(6) months and two(2) years.

**5. How far should the published calendar for scheduled KSK rollovers extend into the future?**

A token number of respondents suggested that an indefinite calendar was needed however no trend in definitive timelines from respondents was observed.

**6. What public notification should take place in advance of a scheduled KSK rollover?**

Respondents, in the majority, called for public notifications via many different stakeholder groups with significant advance notice prior to a KSK rollover event.

**7. What other considerations are necessary for the Root Zone Management Partners to take into consideration prior, during, and after a planned key roll over?**

There were no observable trends in the responses. Respondents suggested more investigation is needed, operational stability is key, repeated KSK rollovers gives added resiliency, and raised concerns regarding non-compliance of RFC5011.

**Section IV: Analysis of Comments**

*General Disclaimer: This section is intended to provide an analysis and evaluation of the comments received along with explanations regarding the basis for any recommendations provided within the analysis.*

**ICANN Recommendations**

The NTIA and the Root Zone Maintainer shall be apprised of the outcome of this consultation by ICANN. Specifically ICANN will present the following input to the NTIA and the Root Zone Maintainer to address during their collaborative discussions with ICANN.

**1. What prerequisites need to be considered prior to a first scheduled KSK rollover?**

A set of tests and measurements, with a test-bed, should be established before embarking on a RFC5011 KSK roll. Lines of communication need to be established during testing phases and methods for success evaluation constructed.

**2. When should the first scheduled KSK rollover take place?**

The KSK rollover should be performed as soon as practical with an emphasis on preparedness.

**3. What should the IANA Functions Operator (ICANN) and the other Root Zone Management Partners do to gauge the technical and end-user impact of a KSK rollover following the first scheduled KSK rollover?**

Measurements and monitoring are the key modes highlighted to gauge the impacts and should be implemented.

**4. How often should a scheduled KSK rollover take place, following the first one?**

It is deemed that performing regular KSK rolls is operationally responsible.

**5. How far should the published calendar for scheduled KSK rollovers extend into the future?**

A review of this item will be undertaken, as the consultation did not yield a clear direction.

**6. What public notification should take place in advance of a scheduled KSK rollover?**

An effort of public notifications via multiple diverse stakeholder groups with significant advance notice, prior to a KSK rollover event, should be undertaken.

**7. What other considerations are necessary for the Root Zone Management Partners to take into consideration prior, during, and after a planned key roll over?**

Further investigation is needed on operational stability, repeated KSK rollovers, and non-compliance of RFC5011.

**Additional Reference Material**

While not a direct outcome of this consultation, the ICANN Security and Stability Advisory Committee (SSAC) published document SAC063 "[SSAC Advisory on DNSSEC Key Rollover in the Root Zone \(07 November 2013\)](#)". ICANN will promote this document to the NTIA and the Root Zone Maintainer to review and consider its recommendations on their own merits, as intended by the SSAC.