Continuous Data-driven Analysis of Root Server System Stability (CDAR)

Study plan – CDAR

Date: Nov 3, 2015

Responsible: NLnet Labs, SIDN, TNO

Project Leader: Bart Gijsen (TNO)

Dissemination level: Public

Authors

Name	Partner	Email
Bart Gijsen	TNO	bart.gijsen@tno.nl
Benno Overeinder	NLnet Labs	benno@nlnetlabs.nl
Cristian Hesselman	SIDN	cristian.hesselman@sidn.nl
Daniël Worm	TNO	daniel.worm@tno.nl
Giovane Moura	SIDN	giovane.moura@sidn.nl
Jaap Akkerhuis	NLnet Labs	jaap@nlnetlabs.nl

Table of Contents

NLnet Labs SIDN labs TNO

1 Introduction

The security and stability of the Internet, and the DNS (Domain Name System) root server system in particular, is one of the utmost concerns of ICANN. Preserving the security and stability is a challenging task in a dynamic and evolving Internet. One of the recent Internet evolutions coordinated by ICANN was the introduction of new gTLDs (generic Top Level Domains). The resulting expansion of the DNS root zone by the new gTLD program could have an impact on the stability of the DNS root system.
Prior to the launch of the new gTLD program ICANN recognized this potential impact and requested the Root Server System Advisory Committee (RSSAC) and the Security & Stability Advisory Committee (SSAC) to study the technical and operational issues related to expanding the DNS root zone. In the conducted studies that followed a number of risks and recommendations were brought forth. For example, in the Root Scalability Study several potential risks were identified and it was recommended to ICANN that "the focus of root zone management policy should be the establishment of effective mechanisms for detecting and mitigating risks as they become visible." In addition, the ICANN GAC (Government Advisory Committee) expressed 12 concerns in the GAC Scorecard[1]; root zone scaling being one of these. The GAC advised the ICANN board to "defer the launch of a second round of new gTLD applications unless an evaluation shows that there are indications from monitoring the root system that a first round did not jeopardize the security and stability of the root zone system." [RSSAC002, SAC042, SAC046]
In response to these recommendations the ICANN board committed to review the impact of root zone scaling following the delegation of new gTLDs. The RFP for which this proposal is submitted is one of the key contributions to this commitment.
In our vision this Root Stability Study needs to:

a) Provide a **clear view on the current and future impact of the new gTLD program on the security and stability of the DNS** and the root in particular.
b) **Identify next steps** (if any) to safeguard the root system's security and stability à priori to further expansion of the root zone.
c) **Contribute to using commonly accepted, best practice root stability parameters and reference data sets**. Therefor the study needs to build on previous root stability studies and advisories (including those mentioned in the RFP, extended with other global measurement initiatives and the DNS Health symposia[2]) and complement them.
d) **Facilitate constructive discussion in ICANN's multi-stakeholder community** about the impact of the new gTLD program on the stability of the root zone. This requires an open and transparent study approach.
e) **Contribute to broad consensus** of the study results by making the study instrumentation (methodology, source code, and data sets (depending on NDA)) available and providing support to ICANN's community members that are interested to apply the instrumentation themselves.
f) Provide an **extensible proof-of-concept** for continuous future root stability investigation that allows for flexible extension with new analysis modules.

[1] www.icann.org/en/topics/new-gtlds/gac-scorecard-23feb11-en.pdf
[2] See for example the "program globally, measure locally" paradigm in the DNS Health 2011 symposium: www.gcsec.org/sites/default/files/files/DNS_SSR3_REPORT_20120210.pdf

2 Objective

The main objective of this project is to assess the impact of the new gTLD program on the security and stability of the DNS root system, up to the current point in time and beyond. In order to achieve this objective including the other envisioned goals defined in the previous section, we set out a number of activities for data measurements and monitoring, data collection, data analysis, and modeling and simulation. With the information obtained from the data analysis and operational modeling, we can accomplish the outlined goals and assess the impact of the new gTLD program on the security and stability of the DNS root system, up to the current point in time and beyond.

Insights of this study will give an in-depth understanding of the security and stability of the current root system with recently introduced new gTLD domains. Based on the data analysis for the current state, we also model the root system. This model will be used for "what-if" scenarios to extrapolate the measurements and determine the impact on the root stability of future growth of the root zone by the introduction of new gTLDs. With the results of the study, the ICANN community can develop business and operational policies that assure the security and stability of the DNS root system, today and in the future.

The results and recommendations from previous reports [RSSAC002, SAC042, SAC046] will be the basis and starting point, but in the proposed study we will establish a comprehensive set of parameters to measure and monitor, and will validate the results with the DNS community (amongst others ICANN, DNS-OARC and RIR meetings).

In this study analysis modules will be developed that can be applied for future assessments on an ongoing basis. All designed and implemented components of the monitoring and data collection infrastructure, and analyses framework will be available for the ICANN community. Similarly for the simulation model of the root system.

This study will provide objective, technical insight in the influence of the new gTLD expansion on the security and stability of the DNS root system. Moreover, this study aims to make this assessment maximally transparent, by making the instrumentation used to obtain this insight available. In this way ICANN provides its multi-stakeholder community with "effective instrumentation for detecting and mitigating risks as they become visible". By making the instrumentation available the multi-stakeholder community can reflect on the study approach and results, as well as re-assess the obtained insights in the period after completion of this study.

3 Study consortium

Accomplishing this complex exercise requires a team with a very strong track record in DNS security and stability analysis, composed of experts with deep technical knowledge of the DNS, outstanding data analytics and data extrapolation skills and experienced developers of DNS monitoring and analysis tools.
Our consortium comprises NLnet Labs, SIDN, and TNO, which are highly recognized by their expertise and published results in this field. The extensive collaboration between NLnet Labs, SIDN and TNO on DNS security & stability research in the past has made the experts a well-attuned team that has frequently conducted DNS studies together in the past. In addition, the team needs to be, and is, very well connected to the ICANN multi-stakeholder community. TNO will provide the project manager and will act as the coordinator of the consortium.
In the appendix details about the consortium partners are included.

NLnet Labs SIDN labs TNO

4 Approach

To achieve the objectives of this proposal, we define a number of activities for the consortium. An important first step is to define the set of relevant root system security and stability parameters that is adequate for current and future analysis of the root system. This set of relevant parameters will be validated with the DNS community (ICANN, DNS OARC, etc.).

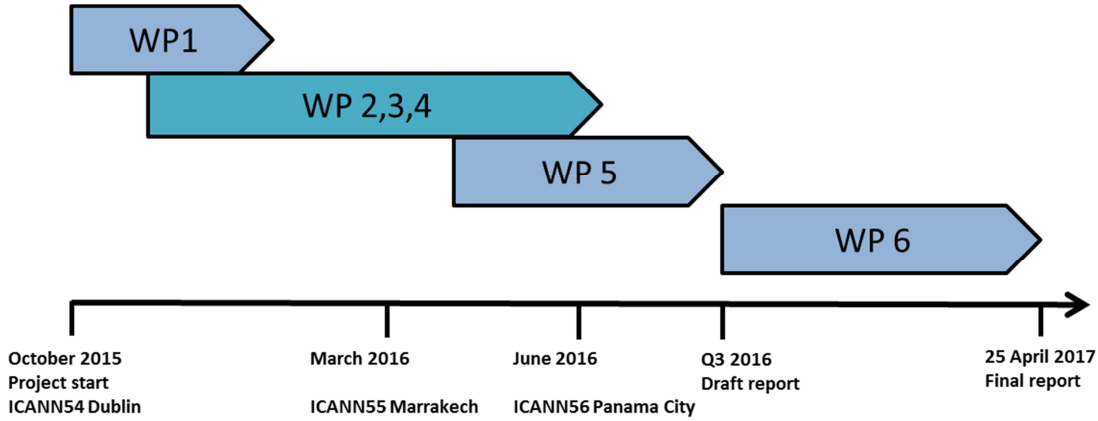
Based on the set of parameters to measure, a monitoring and data collection infrastructure is developed. The measurements are a mix of passive and active measurements that are used in the analysis phase. The monitoring and data collections infrastructure is designed with the idea that future extensions are desirable/possible. The specific questions and concerns for the root stability and scalability define the suite of analyses that can be applied on the collected data. The framework for analysis is similarly designed for extendibility. In the future, new studies can be based on the monitoring and data collection infrastructure and data analysis framework.

Complementary to the insights gained from the data analysis for security and stability, we develop and implement a simulation of the root system to study future scenarios ("what-if" scenarios). The simulation model will be validated with the current data set and analysis and, once carefully assessed, can be used to study the impact of future changes to the root system and the impact of policies (policy changes).

The results of the study will be presented at various relevant podia, like ICANN, DNS OARC, RIR meetings, IETF/IEPG. Besides presentation of the results at meetings and conferences, we will also actively search for publication of papers in academic and operational-oriented journals.

The activities to be carried out in this project are clustered in the following work packages (WPs):

- WP-1: Involving RSOs and the DNS community
- WP-2: Measurements design and execution
- WP-3: Security and stability analysis of collected DNS data
- WP-4: Future scenario analysis of DNS root security and stability
- WP-5: Dissemination of results and instrumentation
- WP-6: Clarifying and discussing findings with ICANN's multi-stakeholder community
- WP-7: Project management



4.1 WP-1 Involving RSOs and the DNS community

In the end ICANN's commitment to safeguard the security and stability of the Internet can only be realized by the multi-stakeholder Internet community as a whole. Since the objective of this study is to contribute to this commitment, it is important to involve the community and the RSOs and the DNS community in particular. In order to make sure that involving the community will take place continuously during the study, we have especially focused this work package on community interactions. Part of the interactions consists of interviews that will be planned with experts who executed previous studies and/or brought forth recommendations of the impact of the new gTLD program on DNS root stability. These experts will include authors of Root Scaling Study, the GAC scoreboard, SAC042 and SAC046, RSSAC-02, participants of the DNS Health symposia (Kyoto and Rome).

In order to measure the security and stability of the root servers in a data-driven approach, an interpretation of DNS root security and stability plays a central role. In the literature different interpretations can be observed. For example, in David Conrad's ISOC technical report [Conrad2012] the wider concept of DNS stability is described as "the ability of the entire name resolution system and its component parts to be able to respond to DNS queries." One of the outcomes of the interactions with the community will help refine the interpretation of DNS root security and stability.

In our opinion it is important this study is performed by a consortium that is independent from, but well connected to Root Server Operators (RSOs). In fact, apart from receiving experiences and measurement DNS data from ICANN's root L, the study results will be more balanced if such input is received from other RSOs as well. In order to obtain cooperation of as many RSOs as possible a preparatory WP-1 activity will be to clarify the intentions of the study team to the group of RSOs assembled in the RSSAC. One of RSSAC's co-chairs has indicated to endorse the undertaking of the study, and to ask the RSSAC to talk with us concerning information about RSSAC related matters.

In order to incorporate feedback from the wider DNS expert community into the study approach the study team will present the study during the ICANN54 meeting (October

18-22, 2015) in Dublin and at technical meetings in the DNS OARC and IEPG community.

4.2 WP-2 Measurements design and execution

WP-2 focuses on obtaining the necessary measurement data to investigate the stability of the root server. Its activities include identification of the relevant parameters to be measured, the careful design of active measurements as well the preparation and collection of passive measurements from the I, K and L root servers. Additionally this WP concerns the data preparation phase, in which the raw obtained data sets are prepared and delivered in a format that are suitable for analysis in WP-3.

Both in the RFP as well as in previous studies and advisories a large variety of parameters have been proposed for assessing the stability of the DNS root zone. For example, RSSAC has proposed a set of parameters in RSSAC-02 that can be monitored from an RSO perspective. In the Root Scalability Study a broader range (beyond the scope of RSOs) of potential risks were investigated. Not all of these risks were translated into specific parameters that can be measured. And measuring the root security and stability from the new gTLD registry perspective are still an unexplored area.

Based on these previous study reports and interviews with experts (a WP-1 activity) we will define a coherent set of DNS root security and stability parameters. The data needed for these parameters will be gathered via a combination of active and passive measurements, interviewing experts and analysis of historic data sets (including DNS OARC's Zone File Repository and the Day In The Life of the Internet (DITL[3]) data sets).

Figure 1 shows an overview of the actors and processes within the provisioning and the publication subsystem of the Root Server system as well as a set of parameters that will be investigated. This set includes and supersedes the set of parameters specified in RSSAC-02. On the right hand side the publication subsystem is shown, divided into (zone file) distribution and querying. The provisioning subsystem feeds the RSOs with the Root Zone Files, but analyzing this subsystem is out-of-scope for this study.

[3] www.dns-oarc.net/oarc/data/ditl

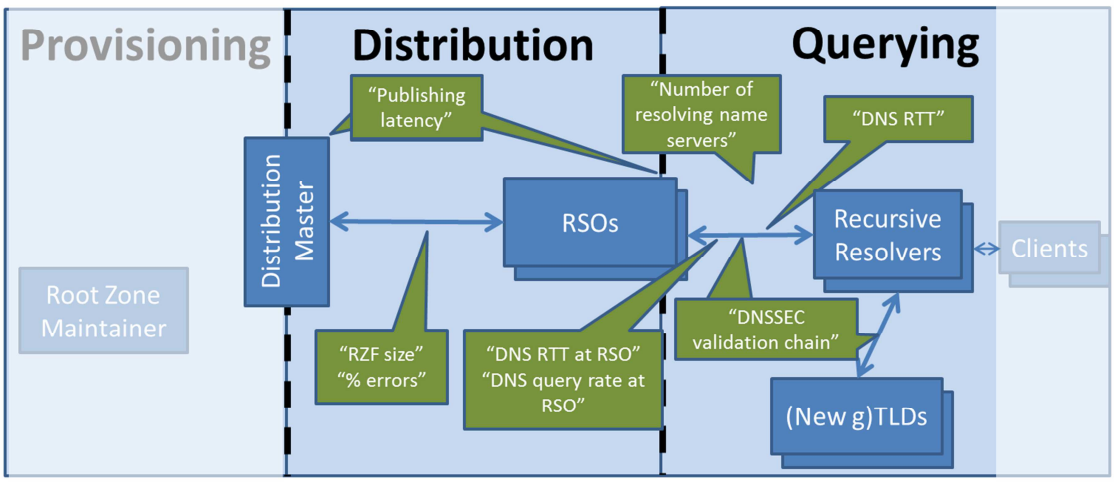


Figure 1 - Overview of the actors and parameters within the provisioning and publication subsystem of the Root Server system

Brief explanation of the root stability parameters in Figure 1:

1. *"RZF size":* Size of the root zone file in terms of bytes, number of TLDs. Including differences in size of the subsequent Root Zone Files.
2. *"% errors":* % errors in the root zone file (basic checks: empty root zone file, missing data, syntax errors, etc.). For this parameter the distribution of measurements per RSO (or if needed per individual RSO site) will be determined.
3. *"Publishing latency":* Latency in publishing the root zone file by RSOs after receiving a NOTIFY from the DM. Similar to the previous parameter, the distribution of measurements will be split out per RSO.
4. *"DNS query rate at RSO":* The number of queries received by the RSO per time interval (hourly, daily, monthly,...). In the reverse direction the number of responses per time interval are measured. These are split out for:
5. Distribution per RCODE
6. Distribution per (new g)TLD
7. Distribution per protocol type (IPv4/IPv6, TCP/UDP)
8. *"DNS RTT at RSO":* Round Trip Time of DNS queries to the root as can be determined from log files recorded by the RSO. Also for this parameter, distributions over RCODES, etc. will be investigated.
9. *"Number of resolving name servers":* The number of unique IP source addresses accumulated across all instances of a root server cluster during a time interval (hourly, daily, monthly,...), divided into IPv4 and IPv6.
10. *"DNSSEC validation chain":* Verification of related DNSSEC crypto-keys from the root and their delegation to the (new g)TLDs.
11. *"DNS RTT":* DNS Round Trip Time. The same parameter as *"DNS RTT at RSO"* but this parameter is measured by active monitoring probes.

For the determination of the parameter values, we envision at least the following measurements and data sources:

- **Active measurements**: We will employ the RIPE Atlas probes in order to measure the stability of the root servers. Therefore, we need to carefully plan what to measure, where to measure, and for how long to measure. First and foremost, these measurements must be continuously carried out, so we have

longitudinal data that allow us to measure these metrics as new TLDs are added to the root zone. The same properties will be measured whenever IPv6 and DNSSEC are active. The consortium has a software framework to support ease-of-development for measurements and to support repeated measurements on the ATLAS monitoring infrastructure.

- **Passive measurements**: This task will involve passively collecting data available from the root servers (I, K and L) as well as using SIDN's .NL data. That will involve a careful planning of what will be measured (e.g., metadata (NetFlow) or full packets, SNMP, etc.), and for how long. In the preparation of this proposal a representative of the RSO operating root I has committed to provide this consortium access to the historic logged data. The details will be discussed with the RSO administrators of root I, K and L. In addition we will investigate how other data sets such as the Day In The Life of the Internet (DITL[4]) could provide additional insights.

- **Public data sources:** DNS OARC has stored all root zone files in their repository[5] that is accessible for their members. From the root zone files we can extract parameters such as the Root Zone File size and possible errors in the Root Zone File size. For new gTLD zone files similar data can be retrieved from ICANN's centralized zone data service[6].

We will combine both active and passive measurements in assessing the stability of the root servers. From these measurements we will collect a large variety of parameters as specified in the RFP proposal complemented with other parameters which have been proposed in previous studies and advisories to measure the status of security and stability of DNS root zone.

4.3 WP-3 Security and stability analysis of collected DNS data

WP-3 will focus on analyzing the data collected from the measurements designed in WP-2 in order to measure the security and stability of the DNS. For example, what is the RTT in the DNS requests when you probe all TLDs from IP addresses from 2,200+ Autonomous Systems (RIPE Atlas probes)? Or is there any correlation in the latency and number of TLDs?
A large variety of techniques and approaches can be applied here, ranging from simple statistics to machine learning (e.g., clustering) and others. Based on the obtained data, we will be able to compare the performance of the root servers across each other for different vantage points, and employ the .NL (SIDN) as a case study base.

[4] www.dns-oarc.net/oarc/data/ditl
[5] www.dns-oarc.net/oarc/data/zfr
[6] czdap.icann.org

4.4 WP-4: Future scenario analysis of DNS root security and stability

Complementary to the DNS stability & security analysis we will develop a quantitative model of DNS query/response flows towards the DNS root. The purpose of the model will be (a) to find correlations in the DNS data and (b) to execute "what-if" scenarios and sensitivity analysis for future growth of, for example, the root zone. This enables us to extrapolate the DNS stability data to an impact analysis of future growth scenarios of the root zone. This is a necessary complement to the data analysis of the current DNS stability, in order to deal with the uncertainty that is caused by the rapid, current and near-future developments of the new gTLD program.

The model input parameters will consist of a subset of the DNS stability parameters that result from the data analyses performed in WP-3, namely a selection of parameters that are relatively easy to measure or predict such as the DNS query rate at an RSO, the root zone file size, etc. We then investigate the relations between these parameters and the parameters that correspond more closely to DNS root stability as defined in WP-2, such as the DNS Round Trip Time (RTT) of a query to / response from an RSO (server). For this we will use correlation analysis combined with other stochastic modelling techniques. This allows us to (approximately) express relevant output parameters in terms of one or more input parameters, which enables us to execute what-if scenarios.

One type of relations will be related to the measured values from active monitoring to the values in RSO data sets. For example, we will design our data collection such that we can correlate DNS query / response from the active measurement and the RSO data set. This enables investigation of, for example, the relations between the RSO query rate (load) and the end-to-end RTT from the measurement data.

The identified relations between the parameters may also be used for reducing the dimensions of the parameter distribution. For example, as mentioned for the data analysis most DNS security and stability parameters will be analyzed for their distribution according to DNS response codes (RCODE), etc. The presentation of distributions for these multiple dimensions does not create a clear overview. Fortunately, some dimensions may be 'collapsed' to strongly reduce this complexity. For example, we will investigate whether the DNS stability of new gTLDs is comparable for those that are served by the same registry provider[7]. If so, then the distribution of parameters values for new gTLDs can be reduced from a distribution over thousands of new gTLDs, to a distribution over tens of registry providers. Similar reductions may holds for other dimensions.

For each of these types of relations between parameters it will be validated whether these are 'invariant' (i.e. whether they remain constant under varying circumstances). Using the invariant relations we will develop a quantitative model that can be used for analyzing what-if scenarios where input parameter values may vary from current measurements.

The algorithms that will be used for the evaluation of what-if scenarios will be implemented in commonly used programming software, such as Java or a variant of C.

[7] Using public information, such as icannwiki.com/All_New_gTLD_Applications.

The program code will be available for others in ICANN's multi-stakeholder community to enable execution of what-if scenarios.

4.5 WP-5: Dissemination of results and instrumentation

Based on the results from WP-3 and WP-4 conclusions will be drawn regarding the impact of the new gTLD program on the security and stability of the DNS root system, up to the current point in time and beyond.

The presentation of these conclusions to the ICANN and DNS community at large will be an important part of our activities. From the presentations we obtain input and comments from the community. As a result from the collected feedback, we can run more measurements and do complementary analysis to answer additional questions.

In our planning, we deliver a draft study report in the summer of 2016, around the ICANN56 meeting. Possible sessions are the DNS Tech Day, ccNSO, and the RSSAC WG. With the DNS Tech Day meeting, we reach out to the technical DNS community for feedback. The ccNSO are important stakeholders of (relying on) the root zone. And in the RSSAC WG the root operators and advisory members are present for consult and comments.

Besides the ICANN community, we will present our results on the DNS OARC meetings, where technical and operational issues are discussed. With the DNS OARC members there is a unique mix of expertise that can be reached. Other potential platforms to present our results are RIR meetings like RIPE meetings, APNIC/APRICOT meetings, or ARIN/NANOG meetings. The IETF meetings are not about operational issues, but the IETF meeting is accompanied by the IEPG meeting on Sunday.

Additionally, we will seek to publish our results in scientific journals or conference proceedings (e.g. Internet protocol journal) – in our own time. This allows for dissemination of Internet measurements and analysis methodology, but will also increase visibility and discussion of the results.

The tools for measurements and analysis will be made available. The developed code will be open source under the GPL or BSD license and will be accompanied by basic documentation. The collected (and possibly processed/anonymized) data will also be available to the community within the constraints imposed by the providers of the data. Interested researchers and network engineers can rerun the measurements, do the analysis and validate the results themselves.

4.6 WP-6: Clarifying and discussing findings with ICANN's multi-stakeholder community

Throughout the project a number of interactions with ICANN's multi-stakeholder community are foreseen, as indicated in the description of WP-1. This work package focuses on the period after publication of the draft study report.

Shortly after the publication, ICANN will start a period for receiving public comments. The study team will be available for clarifications in this period. In the summer of 2016 the draft study report will also be presented to ICANN's multi-stakeholder community. The exact setting and date will be discussed with the commissioner, but it is likely to be scheduled during the ICANN-56 meeting. After the public comments period has closed,

the study team will formulate a response to the feedback obtained. In parallel, the received feedback will be analyzed and the necessary adjustments will be incorporated in a new version of the study report.
In October 2016 and February 2017 study team members will attend the meetings ICANN-57 and ICANN-58. For each meeting the study team will compose a renewed status updated of the DNS stability parameters, for example based on the continuous active monitoring probes. In April 2017 a final evaluation with the study commissioner, including the active monitoring results up till that point in time, will conclude the study.

4.7 WP-7: Project management

TNO will provide the project manager for the study and TNO will be the main contractor for ICANN. The consortium partners NLnet Labs and SIDN will be sub-contractors of TNO for this study. TNO has wide experience with managing international (e.g., for ICANN and the European Commission) and national projects. TNO has incorporated project management in their ISO 9001 certified Quality Management System ISO 9001. See the individual partner descriptions for references to previous projects and expertise.
The study team will be directed by a board with one representative of each of the three partners. The main duties of the project board are the overall supervision of the project, including technical coordination, progress review, quality control, risk management, dissemination and possible resource reallocations due to unanticipated events. Project board meetings will be held monthly as telephone conferences or as face-to-face meetings.
For matters of daily study progress and project management Bart Gijsen (TNO) will be the primary consortium contact person for ICANN. For more general questions and feedback between the ICANN community and the study team Cristian Hesselman (SIDN) will act as primary liaison.

Each work package will have one work package leader, but other partners will contribute to the work package. The individual contribution of the partners to the work packages and tasks are described in the work package descriptions and in appendix B. The lead for each of the work packages is assigned to the following partners:

WP-1 is led by TNO.
WP-2 and WP-3 are led by SIDN.
WP-4 is led by TNO.
WP-5 is led by NLnet Labs.
WP-6 is led by SIDN.
WP-7 is led by TNO.

References

[RSSAC002] RSSAC 002 RSSAC Advisory on Measurements of the Root Server System, November 2014. Online: https://www.icann.org/en/system/files/files/rssac-002-measurements-root-20nov14-en.pdf

[SAC042] SAC 042 SSAC Comment on the Root Scaling Study Team Report and the TNO Report, December 2009. Online: https://www.icann.org/en/system/files/files/sac-042-en.pdf

[SAC046] SAC 046 Report of the Security and Stability Advisory Committee on Root Scaling, December 2010. Online: https://www.icann.org/en/system/files/files/sac-046-en.pdf

[Conrad2012] Conrad, David: Towards Improving DNS Security, Stability, and Resiliency. Technical Report. 2012. Online: http://www.internetsociety.org/sites/default/files/bp-dnsresiliency-201201-en_0.pdf

A Consortium Partners

NLnet Labs (www.nlnetlabs.nl)

NLnet Labs is a non-profit research and development company that focuses on developments in Internet technology bridging the gap between theoretical insights and practical deployments; engineering and standardization, where public interest is often more pressing than commercial interest. It is NLnet Labs' goal to play an active and important role in the development of open source software, participation in development of open standards, and dissemination of knowledge through training, consultancy, and evangineering. NLnet Lab's software is an important component of the Internet infrastructure. NLnet Lab plays a significant role in standards development. Dissemination of knowledge is realized through education and collaboration. NLnet Labs has a staff of nine software developers and experts.

NLnet Labs is recognized for her expertise in Internet system technology, security and architecture, in particular in DNS, DNSSEC, inter-domain routing and addressing. With the development of authoritative name servers and recursive resolvers, NLnet Labs has deep knowledge of the DNS system and its protocols. Complementary to this, NLnet Labs has a strong track record in providing expertise to security and stability analysis of critical infrastructures like scaling the root study, SSAC, ENISA study of the routing infrastructure and is member of the ENISA Internet Infrastructure Security and Resilience Reverence Group. With this, NLnet Labs is strongly involved in the ICANN, DNS and Internet infrastructure community.

NLnet Labs team member: Benno Overeinder

Benno Overeinder is managing director of NLnet Labs in the Netherlands. He is active in the RIPE and IETF community, focusing on Internet infrastructure security and stability, both DNS and routing related. He is the chair of the RIPE Programme Committee and co-chair of the RIPE Best Current Operational Practices Taskforce. Overeinder has contributed to ENISA commissioned studies on Internet routing infrastructure security and stability, and is member of the ENISA Internet Infrastructure Security and Resilience Reverence Group.

NLnet Labs team member: Jaap Akkerhuis

Jaap Akkerhuis is a senior research engineer at NLnet Labs. He has been instrumental in the development of the Internet in the Netherlands and in Europe in the early 1980s. After some year in the US, he returned to the Netherlands where he joined the first independent ISP. Later he worked as a Technical Advisor for SIDN, the registry of the .NL TLD. Jaap Akkerhuis has served in the SSAC since its inception and is co-chair of the RIPE DNS working group and served as a co-chair for the IETF ProvReg WG. He is a regular consultant to ICANN and their member of the ISO 3166 Maintenance Agency.

SIDN (www.sidn.nl)

SIDN manages the Internet extension of the Netherlands, .nl. As the Dutch national domain name registry, we enable Internet users to safely use and register .nl domain names anytime and anywhere. We operate the .nl zone of the Domain Name System (DNS) and handle over a billion DNS queries every day for more than 5.5 million registered .nl domain names. Over 2.4 million of those are secured with DNSSEC, making .nl the largest secured Internet extension in the world. We also provide the backend services for the new gTLDs .amsterdam and .politie ("Police" in Dutch) as well as for the country code .aw (Aruba).

SIDN is actively involved in the ICANN community since its inception. We currently contribute to the cross-community working groups on the IANA Stewardship Transition and ICANN Accountability and we are leading the working group "Secure Email Communication for ccTLD Incident Response" (SECIR). In the past, we had staff on the ccNSO Council and led the ccNSO working group "Strategic and Operational Planning" (SOP). In addition, SIDN is a long-time member of DNS-OARC and had one of our staff on the DNS-OARC board from 2012 until 2014.

SIDN Labs (www.sidnlabs.nl) is SIDN's research and development team, which would carry out the project if commissioned. SIDN Labs develops and evaluates new Internet technologies and systems to further enhance the security and stability of the DNS and the Internet at large., as for example our ENTRADA (ENhanced Top-level domain Resilience through Advanced Data Analysis) project[8], an experimental platform that we use to capture, store, and analyze the DNS traffic we handle on our production systems. The goal of the platform is to develop new services and applications to discover anomalies and threats in the DNS traffic and use that information to enable us and others to further increase the security and stability of the Internet, which also comes along with a Privacy framework[9].

SIDN team member: Cristian Hesselman

Cristian is the head of SIDN Labs, the R&D team of SIDN. SIDN Labs develops and evaluates new technologies and systems to further enhance the security and stability of the DNS and the Internet at large, for instance based on as anomaly detection, self-organization, and reputation metrics. Cristian was previously with Telematica Instituut, a research facility in the Netherlands, where he led and developed large national and international R&D projects. He also worked as a senior researcher on topics such as sensor systems, adaptive multimodal user interfaces, and service platforms. Before that, he was a software engineer at Lucent Technologies. Cristian holds a Ph.D. (2005) and an M.Sc. (1996) in computer science, both from the University of Twente, the Netherlands.

[8] https://www.sidnlabs.nl/uploads/tx_sidnpublications/NCSC-presentatie-BIG-data-pub.pdf

[9] https://www.sidn.nl/downloads/whitepapers/SIDN_Labs_Privacy_Framework_Position_Paper_V1.3_EN.pdf

SIDN team member: Giovane Moura

Giovane is a Data Scientist at SIDN working on the analysis of the DNS traffic on .nl, using the ENTRADA Hadoop-based platform. Giovane has a record of publications in large-scale Internet measurements and Internet security, and has worked at Delft University of Technology, in the Netherlands, as a Post-doctoral researcher running a Work Package at 28-partners EU anti-botnet project (EU ACDC). He obtained his PhD degree from the University of Twente (NL).

TNO (www.tno.nl)

TNO[10] is one of the major internationally oriented contract research and technology organizations (RTO) in Europe. With a staff of approximately 3000 and an annual turnover of 586 million Dollars, TNO is carrying out technological and life science research aimed at boosting innovation and achieving societal impact. By translating scientific knowledge into practical applications, TNO contributes to strengthening the innovation capacity of businesses and government. TNO is involved in many international projects (about 30% of the market turnover), including the Scaling the Root study commissioned by the ICANN board in 2009.

In TNO's innovation area of Information Society applied research is carried out along three lines:

- Technical Robust Infrastructures (Security, Stability & Quality)
- Information Creation (Media & Content Delivery; Big Data Evolution)
- Information Influence (Privacy & e-Identity; Strategic Use of Information)

TNO's Performance of Networks and Systems expertise (contributing to the Robust Infrastructures research line) was recognized as 'internationally leading' by an external knowledge auditing committee led by prof. W. Jonker. In the proposed study team TNO contributes quantitative modelling & analysis experts, who were involved in the Scaling the Root study team. Moreover, their research on the Global DNS reference model[11] was awarded the best paper award at the international DNS Easy conference in 2011.

TNO team member: Bart Gijsen

One of the team members for this proposal is Bart Gijsen. In 2009 Bart led TNO's contribution to the Scaling the Root study team and has been an active contributor to numerous DNS stability research initiatives. He presented his work at, amongst others, ICANN and DNS OARC meetings and DNS Health symposia. Bart has also led a study investigating the plans of Dutch multinationals regarding brand name TLDs, in cooperation with SIDN.

10 TNO is a not-for-profit organisation, whose acronym is an abbreviation of "Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek"

11 www.gc-sec.org/sites/default/files/files/dnseasy2011.pdf#page=6

TNO team member: Daniël Worm

Daniël Worm works at TNO since 2011 as mathematical researcher and consultant. He has extensive experience with mathematical modelling and analysis, with a primary focus on stochastic modelling including statistics. He has participated in a variety of projects in the domains of ICT and energy. His work includes development of new models and performing stochastic analysis for telecom operators in order to estimate performance KPIs in their networks, applying optimization techniques and performing resilience and anomaly detection techniques.