

DNSSEC in SURFdomeinen

Final report on the results of the project

Project : GigaPort3
Project Year : 2010
Project Manager : Roland van Rijswijk
Author(s) : Roland van Rijswijk
Date : 2011-01-17
Version : 1.0

Summary

This document contains a final report on the results of the 'DNSSEC in SURFdomeinen' project that was carried out under the GigaPort3 programme in the first three quarters of 2010. In this project, an implementation of DNSSEC based on the OpenDNSSEC open source project was integrated into SURFnet's SURFdomeinen managed DNS environment. The original goal of making this functionality available to end-users of SURFdomeinen could not be realised due to delays in the public availability of secure delegations for the .nl domain. As an alternative, this implementation will be used to sign a number of SURFnet domains in the last quarter of 2010. This both sets and example for SURFnet's constituency and the Internet community in The Netherlands as well as serves as a real-life test case for secure DNSSEC delegations under the .nl top-level domain.

This document contains an overview of the way the implementation was carried out and what the end-user experience will be like.

It then continues with a discussion on the way knowledge has been disseminated during the project by actively maintaining a blog.

The document concludes with a number of recommendations for further work and follow-up projects. One of the follow-up activities already planned for 2011 is the publication of two DNSSEC deployment white-papers; one about deploying DNSSEC on resolver infrastructure and one about deploying DNSSEC on the authoritative side (i.e. signing zones).



Colophon

Programme line : Future IP
Part : FIP 4
Activity : DNSSEC in SURFdomeinen
Deliverable : D1c – DNSSEC in SURFdomeinen final report
Access rights : Public

This project was made possible by the support of SURF, the collaborative organisation for higher education institutes and research institutes aimed at breakthrough innovations in ICT. More information on SURF is available on the website www.surf.nl.



The licence for this publication is the Creative Commons licence "Attribution 3.0 Unported".
More information on this licence can be found on <http://creativecommons.org/licenses/by/3.0/>

Table of contents

- 1 INTRODUCTION 4**
 - 1.1 INTENDED AUDIENCE4
 - 1.2 DOCUMENT OUTLINE4
- 2 PROJECT DESCRIPTION 5**
 - 2.1 INTEGRATION OF DNSSEC INTO SURFDOMEINEN5
 - 2.2 DNSSEC USER SURVEY5
- 3 PROJECT RESULTS 6**
 - 3.1 INFRASTRUCTURE6
 - 3.2 USER EXPERIENCE 10
 - 3.3 USER SURVEY 13
 - 3.4 KNOWLEDGE DISSEMINATION 14
- 4 RECOMMENDATIONS16**
 - 4.1 ROLL-OUT TO END USERS..... 16
 - 4.2 FUTURE WORK 16
- 5 REFERENCES17**



1 Introduction

Since the Kaminsky attack was published in 2008, DNSSEC has been a focus point for SURFnet. There has also been a keen interest in the technology among SURFnet's constituency. This year has seen the introduction of DNSSEC at the root and many Top Level Domain (TLD) registries.

SURFnet has integrated DNSSEC support in the SURFdomeinen portal as a project within the GigaPort3 programme. This document reports on the results of this project.

1.1 Intended audience

This document is intended as a starting point for SURFnet's fellow NRENs as well as the larger Internet community to learn more about SURFnet's DNSSEC deployment.

1.2 Document outline

This document has the following outline:

- Chapter 2 contains a brief description of the original goals of the project, a high-level overview of the work breakdown and some words on deviations from the original plan
- Chapter 3 zooms in on the results of this project; it describes the infrastructure that was realised, the end-user experience and the results of the user survey
- Chapter 4 concludes the document with recommendations for rolling the service out to end users and for future work

2 Project description

2.1 Integration of DNSSEC into SURFdomeinen

The main goal of the project was to integrate DNSSEC functionality into the SURFdomeinen portal.

SURFdomeinen is a web-based portal that allows DNS operators of connected institutions to:

- register or migrate domain names in the following top-level domains (TLDs): .nl, .com, .net, .org, .info and .eu;
- manage contact details for contacts associated with registered domains;
- create secondary DNS configurations on SURFnet name servers for their domains;
- manage complete DNS zones that are then served out by SURFnet name servers.

DNSSEC support has been integrated into the managed DNS functionality.

The original goal of the project was to make this functionality available to end users of SURFdomeinen by the end of Q3 2010 (after a pilot). Unfortunately, secure delegations in the most important top-level domain for SURFnet's constituency, the .nl domain, will not be available earlier than 2011. This makes it impossible to achieve this goal in 2010. It was therefore decided to change the scope of this deliverable and to instead only make the functionality available to SURFnet in 2010 enabling certain SURFnet domains to participate in a limited secure delegation scheme by SIDN (the so-called 'Friends and Fans' programme). Recommendations on how to make the DNSSEC functionality available to end users of SURFdomeinen are given in chapter 4.

2.2 DNSSEC user survey

A secondary goal of the project was to gauge the interest among SURFnet's constituency in 'signing-as-a-service' (a managed environment that implements DNSSEC signing for organisations that operate their own DNS infrastructure).

After an internal discussion within SURFnet we decided that it is not feasible for SURFnet to offer 'signing-as-a-service' because it creates unwanted dependencies between SURFnet and institution DNS infrastructure and because we cannot guarantee the availability of such a service in perpetuity.

We therefore changed this goal during the project to performing a user survey among connected institutions into the interest in and plans for DNSSEC.

3 Project results

3.1 Infrastructure

3.1.1 Overview

The DNSSEC functionality in SURFdomeinen is based on OpenDNSSEC¹, an open source DNSSEC signer solution.

Most professional DNS setups work with a so-called 'hidden primary' and 'public primary'. DNS management (zone editing) is done on the hidden primary that sits securely in the organisation LAN. Once the zone is complete, it is then transferred to the public primary to be served out to the Internet. Figure 1 below shows this setup:

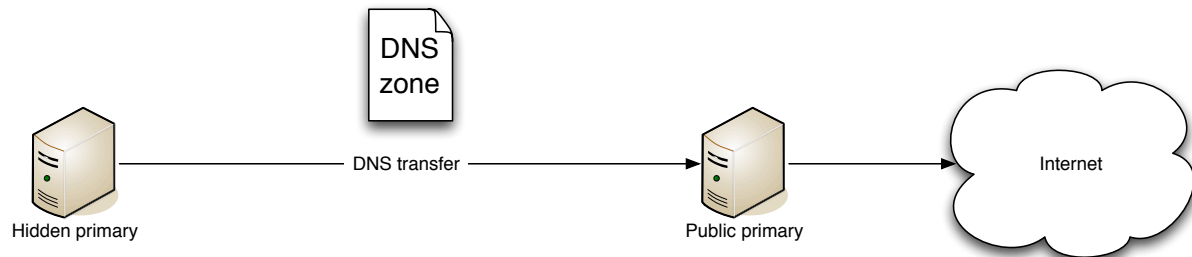


Figure 1 - Hidden/public primary setup

OpenDNSSEC has been designed in such a way that it can be introduced on the path between the hidden primary and the public primary as a 'bump-in-the-wire'. Figure 2 shows this:

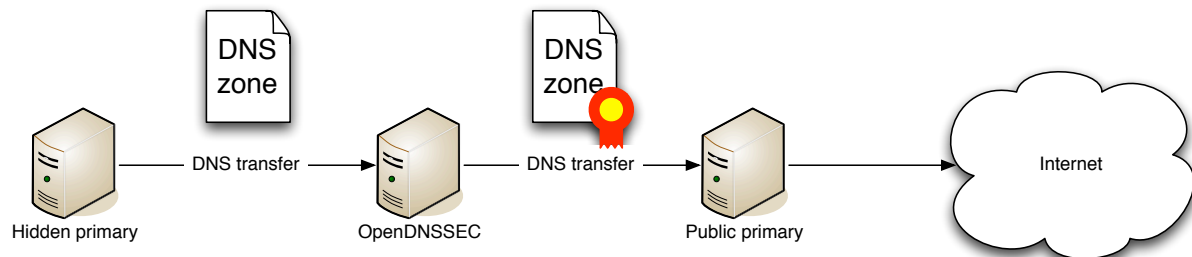


Figure 2 - OpenDNSSEC as bump-in-the-wire

In this configuration, the DNS zone is no longer transferred directly from the hidden primary to the public primary but instead to an OpenDNSSEC instance. OpenDNSSEC processes the zone, makes sure it gets signed and then transfers it to the public primary.

The setup used by SURFnet is similar to the bump-in-the-wire configuration, although certain details are different. Figure 3 shows a schematic overview of the setup for SURFdomeinen.

¹ <http://www.opendnssec.org>

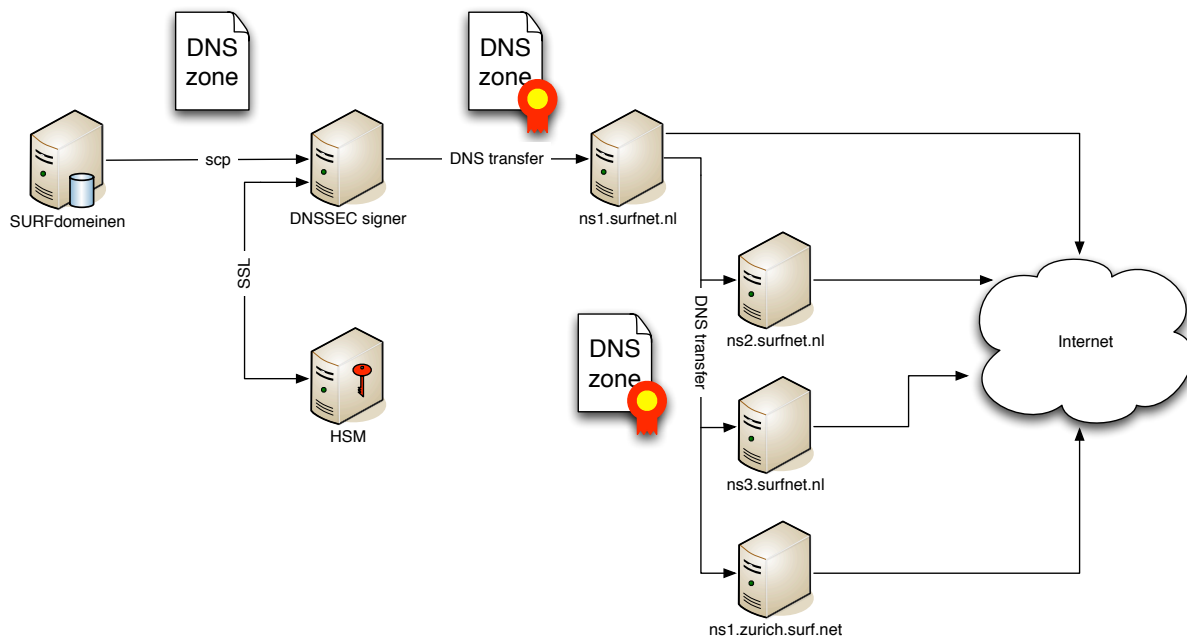


Figure 3 - Schematic overview of the DNSSEC setup for SURFdomeinen

The three entities at the top left-hand side of the diagram are the bump-in-the-wire setup. There are two important differences with the generic setup in Figure 2:

- Data transport from the SURFdomeinen hidden primary to the DNSSEC signer is not done using a standard DNS transfer. Instead, a secure copy method is used. There are two reasons for this:
 - The DNS transfer component of OpenDNSSEC had a critical bug² that caused some trouble while testing with the surfnet.nl zone (this bug has now been fixed, but it was decided that this component should not be used in production). Instead of using a DNS transfer, the zone file is copied using secure copy. A checksum comparison then guarantees the integrity of the file.
 - The secure copy is initiated by the signer instead of SURFdomeinen; this is better from a security perspective as it limits the number of interfaces that the signer has to expose to the outside world.
- The key material used to sign zones is stored in a Hardware Security Module (HSM)³, shown below the signer in the diagram

3.1.2 Redundancy

DNS has had redundancy built-in to it from the start. Everyone operates redundant authoritative name servers and indeed most domain registries mandate registering at least two different name servers for a newly registered domain.

Introducing DNSSEC as a bump-in-the-wire runs the risk of creating a single point of failure. DNSSEC requires continuous resigning of zones since signatures have a limited validity. This issue was recognised at the start of the project and has been addressed with several measures.

Conceptually, as shown in Figure 3, key material is stored and processed in a HSM. In actual fact, two HSMs are used in a high-availability setup. This means that all newly generated key material is automatically replicated instantaneously between the two HSMs. Furthermore, when cryptographic operations are required (when a zone is being signed), the signer talks to a virtual HSM interface that delegates the operation to the real HSMs. This works in such a way that if one HSM is offline, this does not affect the signer. To further improve redundancy and reliability, the HSMs are in physically separate locations (one is in Amsterdam, the other in Tilburg).

² See the ticket, see <http://trac.opendnssec.org/ticket/183>; it is recommended to use at least version 1.6.7 of LDNS in conjunction with OpenDNSSEC

³ A HSM is a high-end security device for storing and using cryptographic key material

In addition to this, regular backups of key material are performed onto a secure backup token. This backup is then stored in a physically separate location by the security officer. OpenDNSSEC has been configured in such a way that key material can only be used if it has been backed up.

Redundancy has also been realised for the signer by installing a second signer system. The slave system is kept up-to-date by synchronising the database and configuration files. If a problem occurs with the active signer, a manual procedure can be performed to fail over to the backup signer.

3.1.3 Resilience

Even though every effort has been made to prevent critical errors from occurring it is not possible to exclude all eventualities. To make sure that errors have as little impact as possible and that a solution can be made sufficiently quickly a number of measures have been taken:

- Negative caching times for signed zones never exceed 1 hour and are often set lower
- The time-to-live of the DNSKEY RRset is set to 1 hour for signed zones
- Signatures are valid for 7 days with automatic resigning 3 days before they expire (thus, a signature is always valid for at least 3 days giving enough recovery time if a signer or HSM fails)

3.1.4 Monitoring

DNS is critical infrastructure; if DNS has problems then this can affect all services. To make sure that any problems are caught in an early stage it is important to implement monitoring checks. The following checks have been implemented:

- Continuous monitoring of correct validation of zones on a dedicated caching resolver
- Continuous monitoring of signature expiration (sends a warning if the expiration time drops below 3 days, see §3.1.3); a Nagios plug-in was specifically designed for this purpose⁴
- Monitoring of signer components
- Monitoring of HSM availability

3.1.5 Security

The aim of DNSSEC is to add authenticity to the DNS. This can only be achieved if the infrastructure around a DNSSEC signer is secure and trustworthy. The SURFnet DNSSEC deployment has been designed with security in mind; this section discusses the security measures that were taken.

Firstly, it is important to make sure that the source data from which the signed zone is generated is protected sufficiently, both during creation as well as in transit to the signer. This has two consequences:

- Access to the SURFdomeinen web portal needs to be restricted sufficiently; only zone owners should be able to alter zone data. This is achieved by using a federated access mechanism to the SURFdomeinen portal that restricts editing of the zones belonging to a connected institution to specific users of that institution that have been assigned an attribute that indicates that they are authorised to edit zones for that institution.
- Transport of zone data from the SURFdomeinen portal to the DNSSEC signer needs to be secured; it should not be possible to alter data in transit. This goal is achieved by using secure copy to transfer the data and by comparing a checksum generated on the SURFdomeinen server to a checksum on the signer to guarantee the integrity of the data.

Secondly, access to critical components in the infrastructure such as the DNSSEC signer should be restricted as much as possible. This is achieved by having a compartmentalised and restrictive network design.

⁴ The source code and a description of this plug-in can be found here: <https://dnssec.surfnet.nl/?p=562>

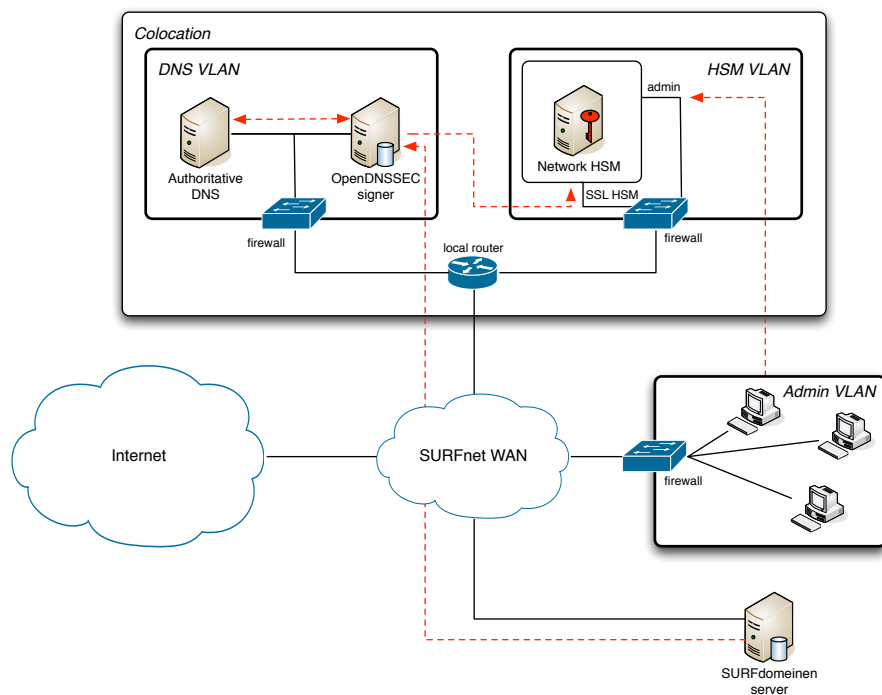


Figure 4 - Network setup

Figure 4 shows a schematic overview of this network design. The top half of the diagram shows the setup for a single co-location; for redundancy reasons the same setup is replicated in another co-location (see §3.1.2). The layout of the network setup is as follows:

- The DNS VLAN (which was an existing VLAN in both locations) contains both the authoritative servers as well as the DNSSEC signer. Only the SURFdomeinen server has direct access to the signer.
- The HSM VLAN, this VLAN contains the HSM with its two interfaces. One interface is only accessible from both DNSSEC signers, this is the interface used for cryptographic operations (communication between the signer and the HSM is secured using SSL). The other interface is used for administrative purposes (such as activating the backup procedure) and is only accessible from administrative VLANs in Tilburg (for the security officer) and in SURFnet's office.

Finally, access to the HSM needs to be restricted. Strict role separation is required to maximise protection of key material. The following roles have been defined in the setup used by SURFnet:

- User – this is the signer application; the user role can use and generate cryptographic keys and is authenticated by a user PIN (more on storing PIN codes below).
- Security Officer (SO) – the SO role is fulfilled by two people (authenticated using the SO PIN); the security officer can perform administrative tasks on the HSM such as resetting (clearing) the HSM, resetting the user PIN and restoring key material from a backup.
- Backup Officer (BO) – the BO role is fulfilled by two people; the backup officer is authorised to create backups of key material onto a secure backup token.

The PIN codes are of key importance since they are used to authenticate users with certain roles. To ensure that they are sufficiently strong, all PIN codes have been generated automatically using a secure password generator and all PIN codes are 16 bytes long.

The user PIN needs to be accessible online to the signer in order for it to be able to operate automatically. This makes the user PIN particularly vulnerable. Network access control rules and strictly limiting which users can access the signer ensures online security. The signer, however, is operated as a virtual machine, which makes data stored on disk (such as the PIN) vulnerable to outside access. In order to prevent unauthorised access, the configuration file containing the PIN code is stored on an encrypted file system (which thus cannot be read outside of the virtual machine). Furthermore, the swap space of the system is encrypted. The only downside of this is that the signer cannot recover automatically from a reboot; an administrator has to log in to mount the encrypted file system (which is also protected using a 16-byte PIN code).

For emergency purposes all PIN codes have also been printed on paper and stored in sealed envelopes that are stored in a safe that is only accessible to authorised personnel.

3.2 User experience

As was already mentioned in §2.1, SURFdomeinen offers a fully managed DNS environment to SURFnet and its connected institutions. The DNSSEC functionality has been integrated into the zone management view as shown in Figure 5 below:

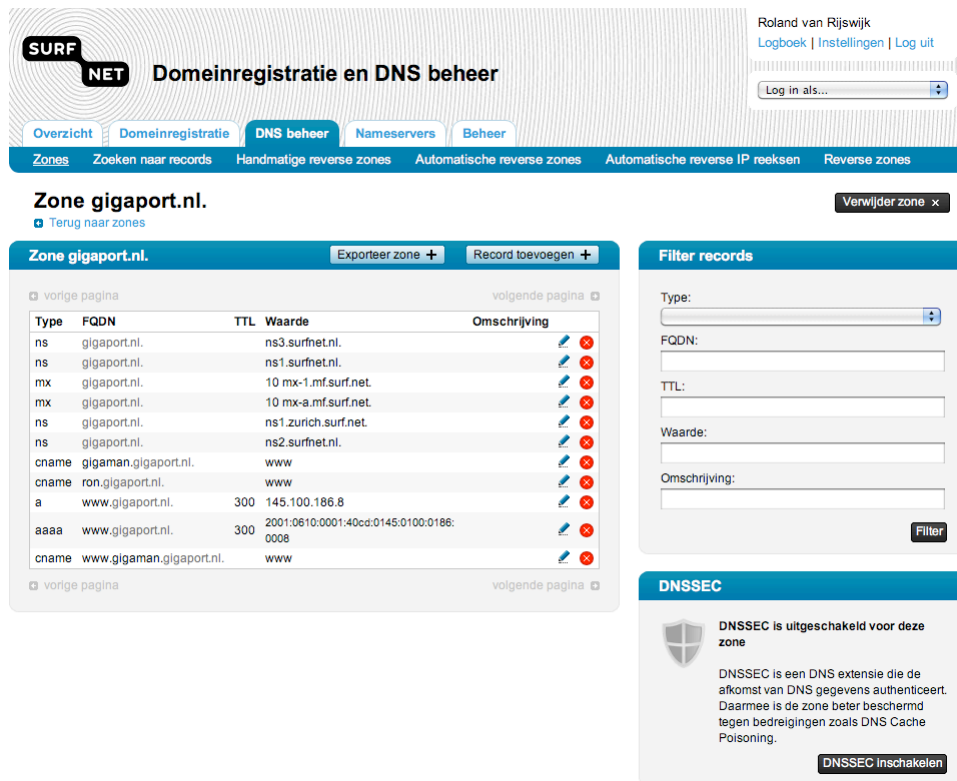


Figure 5 - Integration of DNSSEC in SURFdomeinen zone view

The figure shows the “edit zone” view for the **gigaport.nl** zone. Users are able to turn DNSSEC on and off on a per zone basis. The view above shows a zone for which DNSSEC has not yet been enabled. By pushing the button labelled “DNSSEC inschakelen”⁵ users can initiate enabling of DNSSEC for a zone. They are then shown a confirmation dialog (Figure 6) explaining the implications of enabling DNSSEC, which they have to conform explicitly⁶.



Figure 6 - Example confirmation dialog

Once a user has confirmed that they wish to enable DNSSEC for a zone, approval by a SURFnet administrator is required. This extra confirmation step was introduced for two reasons:

⁵ Dutch for: Enable DNSSEC

⁶ The dialog explains (in Dutch) the implications of enabling DNSSEC; the most important implication is that once DNSSEC is turned on, it takes a while to turn it back off again and that it makes moving a zone to another registrar harder

- It gives SURFnet a chance to review DNSSEC requests before they are processed; if, for instance, an institution that has never shown an interest in DNSSEC before sends in a request, the administrator may wish to contact them to confirm that they actually wish to proceed and to check if they are aware of the implications.
- The first time an institution enables DNSSEC for a zone, an OpenDNSSEC policy and corresponding key material are generated for that institution. Key material can only be used when it has been backed up; this process is normally only performed once every 4 weeks, which may be unacceptably long for an institution. Thus, when a request like this comes in, the administrator can decide to schedule an extra backup cycle.

Once the DNSSEC enabling process for a zone has started, the UI will communicate this to the user as shown in Figure 7.



Figure 7 - Notification that DNSSEC is being enabled for a zone

The notification tells the user (in Dutch) that DNSSEC is being enabled and that the user will receive an e-mail when the process has completed and the zone is signed.

The system will now start processing everything that is necessary to enable DNSSEC for a zone in the background. In outline this process consists of:

- The SURFdomeinen system configuring the signer to accept the zone as input
- The signer transferring an initial copy of the zone to be signed to the signer
- The signer signing the zone for the first time
- The SURFdomeinen system noticing that the zone has been signed
- The SURFdomeinen system reconfiguring the authoritative name servers such that they now retrieve the zone from the signer
- The SURFdomeinen system waiting for a secure delegation (DS) to appear in the parent zone
- The SURFdomeinen system waiting until the secure delegation has propagated to all DNS caches
- The SURFdomeinen system signalling to the user that the zone is now signed

Administrators are able to view more status information about the current state of a zone that is in the process of being signed, an example of this is shown in Figure 8:

Zone	Gewenste wijziging	Status	Datum
checkdnssec.org.	Aanvraag voor inschakeling loopt	DS is gezien	2010-09-20 15:29:36
gigaport.nl.	Aanvraag voor inschakeling loopt	Zone is gesigned (nameserver)	2010-09-21 13:18:53

[Alle zones met DNSSEC bekijken ->](#)

Figure 8 - Current states of zones being signed

The dialog in the figure shows that the secure delegation (DS) has been seen by the system for **checkdnssec.org** and that the zone **gigaport.nl** is being served out as a signed zone (no secure delegation has been seen yet).

When the zone is fully signed, this is shown to users in the zone view using the notification show in Figure 9:



Figure 9 - Notification showing that DNSSEC is enabled

The notification tells the user (in Dutch) that DNSSEC is enabled for the zone. It also contains a button that allows the user to disable DNSSEC. Pushing this button will lead to another confirmation dialog and a request being submitted to SURFnet administrators.

The DNSSEC status of a zone is also shown in the zone list. Figure 10, below, shows this for the zone **dnshealth.org**. The blue shield icon that is used in the zone view is re-used in a smaller version in the zone list.


Zone	Type	Gebruiker	Reseller
dnshealth.info	Managed	SURFnet B.V.	SURFnet B.V.
dnshealth.org	 Managed	SURFnet B.V.	SURFnet B.V.

Figure 10 - Zone list showing DNSSEC status using the blue shield icon

Figure 11 below shows the complete life-cycle a zone can go through from unsigned (top of the diagram) to signed (bottom of the diagram) and back:

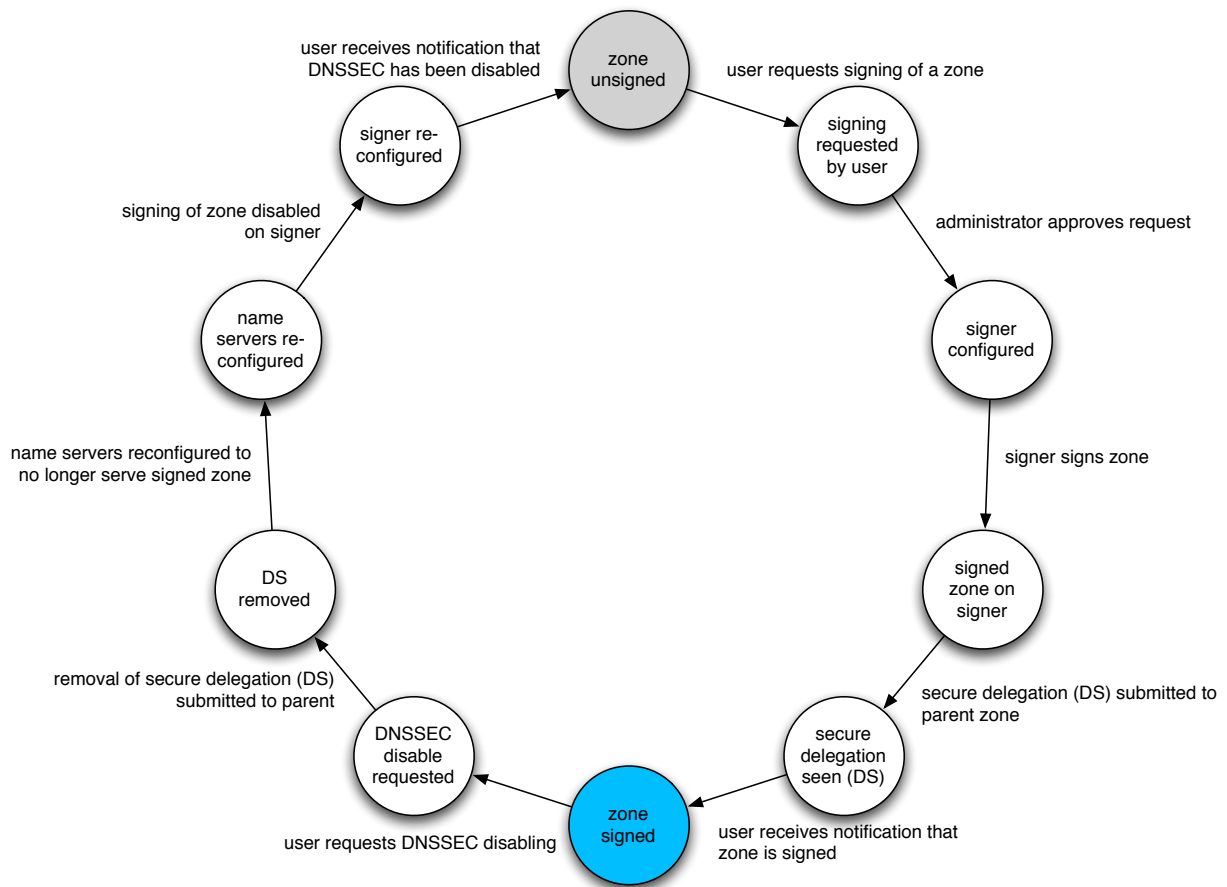


Figure 11 - Zone life-cycle

3.3 User survey

3.3.1 About the survey

As part of the project, SURFnet performed a user survey among its constituency into the interest in and plans for DNSSEC. The survey was carried out using an online questionnaire. This questionnaire was circulated among 169 people responsible for DNS management at connected institutions; out of this group, 38 people completed the survey (23%). The participants were a relatively homogeneous representation of the various parts of SURFnet's constituency (i.e. equally distributed over universities, teaching hospitals, research institutions, etc.).

This section contains a brief summary of the results of the survey, the full report can be found in [2].

3.3.2 Interest in DNSSEC

A large number of participants indicated that they have an interest in DNSSEC and are already familiar with it. Only a minority claims to have no interest whatsoever in DNSSEC. The graph below (Figure 12) shows how participants responded:

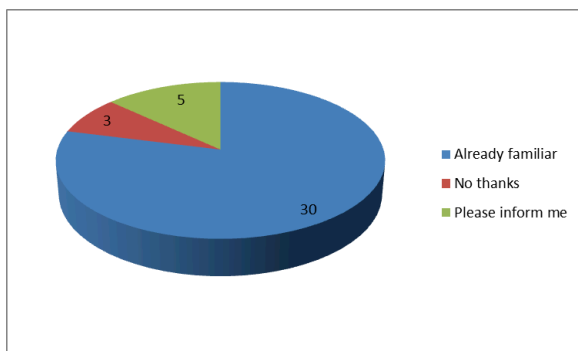


Figure 12 - Familiarity with DNSSEC among survey participants

One can assume that there is a bias among participants towards knowledge of and interest in DNSSEC; even so, the number of participants that think that DNSSEC is important is higher than initially expected. Figure 13 shows how participants responded to the following question: "On a scale of 1 to 10, how important do you think DNSSEC is?".

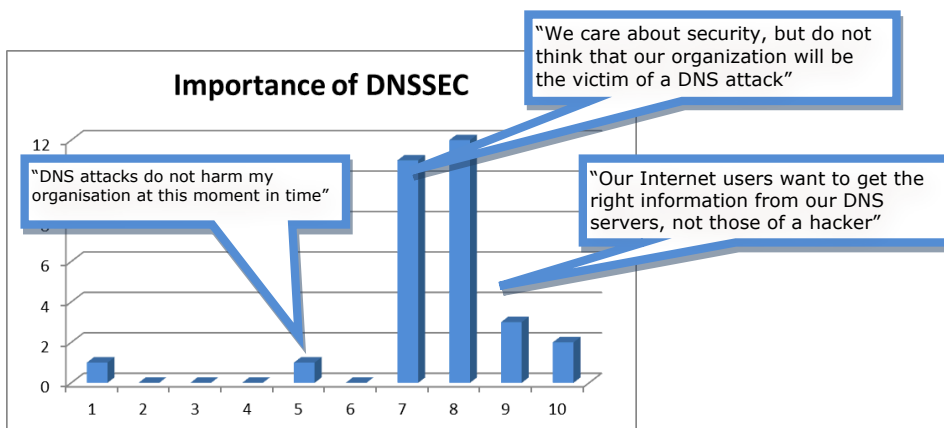


Figure 13 - Importance survey participants attribute to DNSSEC

3.3.3 Plans for DNSSEC

A majority of participants indicate that they are planning to sign some or all of their domains using DNSSEC. Figure 14 shows how participant view this issue.

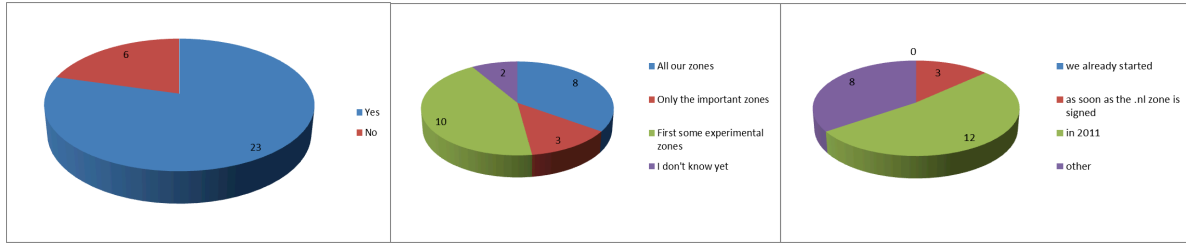


Figure 14 - Participants view on signing their domains

The graphs show – from left to right – if participants are planning to sign their .nl domains, which domains they’re planning on signing and when they want to start doing this.

Participants were also asked how they plan to sign their domains. Interestingly, the vast majority indicated that they do not yet know this.

3.4 Knowledge dissemination

Knowledge dissemination forms an integral part of all projects carried out under the GigaPort3 programme. Knowledge gained in this particular project was shared in two ways: by giving presentations at national and international events and by maintaining a web log about the activities in the project.

3.4.1 Blog goals

The web log was created with a particular goal: to share any insights gained during the design and implementation of DNSSEC in SURFdomeinen. The rationale behind this is simple: many of the design decisions and implementations choices that need to be made to implement DNSSEC are not particular to SURFnet. Indeed they are much more universally applicable.

As an NREN and non-profit organisation SURFnet can freely share any such information and thus contribute to the build-up of knowledge; commercial organisations, on the other hand, dealing with DNSSEC will or can be much less forthcoming in sharing such information either because it concerns trade secrets or because – for instance – admitting mistakes can be problematic for them giving shareholder stakes.

The web log was used during the project to share information in several categories: architecture, cryptography, policies, procedures, resilience, security, technical issues, timing issues and user stories. Although the project is finished, the blog is still kept up-to-date with fresh insights and information about SURFnet’s DNSSEC deployment and DNSSEC on the wider Internet. Figure 15 shows a screenshot of the blog. The blog can be found at <https://dnssec.surfnet.nl>.

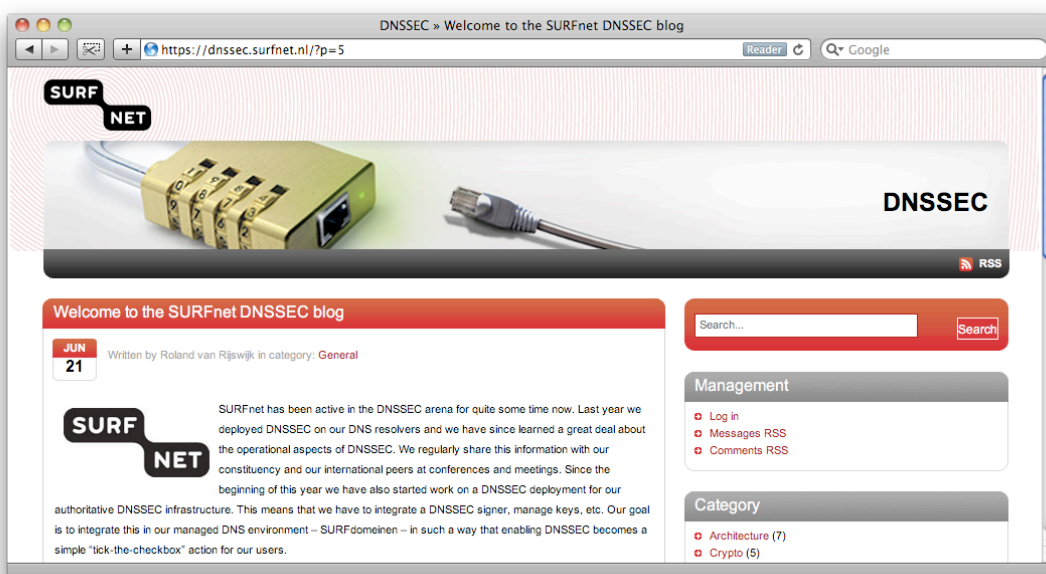


Figure 15 - Screenshot of the SURFnet DNSSEC blog

3.4.2 Interest in the blog

To gauge the interest in the blog, Google Analytics was used to track the number of visitors and their country of origin. Figure 16 below shows the general statistics of the blog.

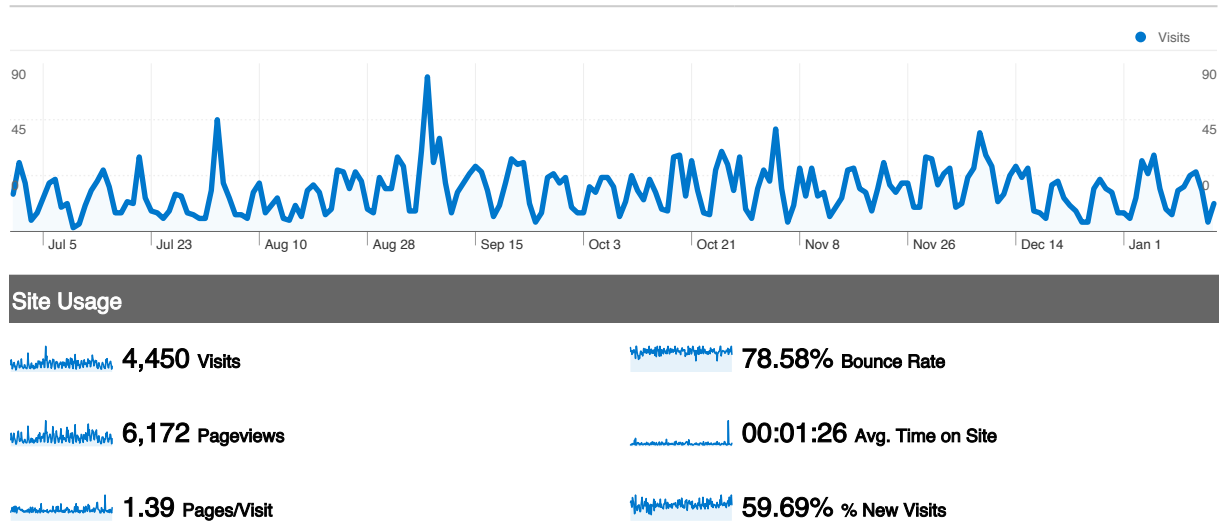
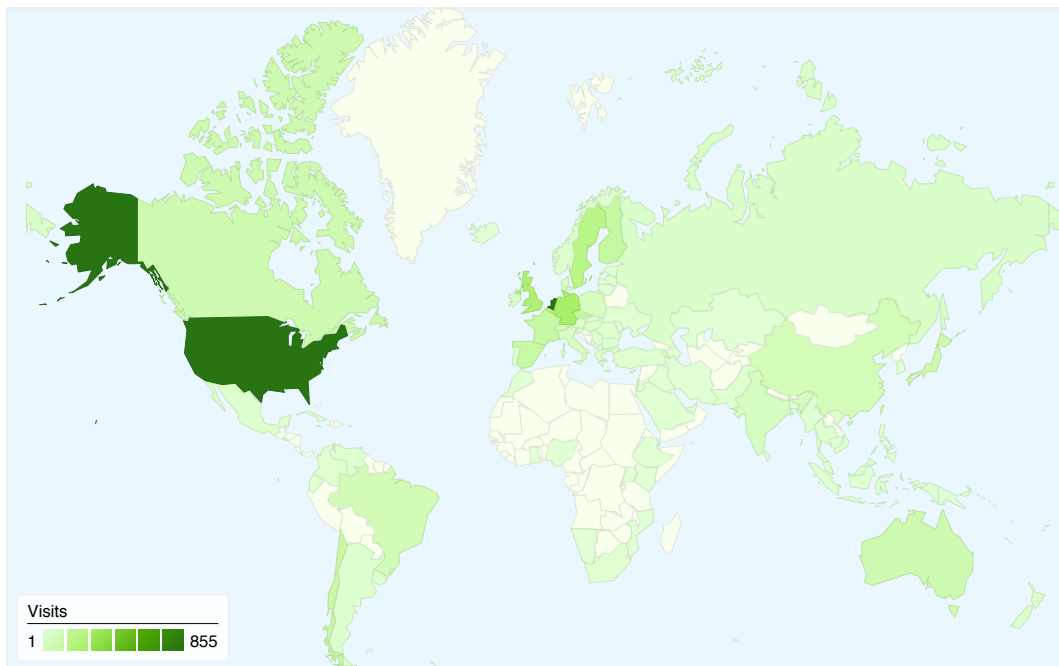


Figure 16 - Blog visitors by date⁷

Figure 17 shows the origin of visitors. Interestingly, the majority of overseas visitors came from the U.S.:



4,450 visits came from 99 countries/territories

Figure 17 - Blog visitors country of origin⁷

Although it is hard to compare these visitor numbers with other sites, we believe that the blog is a success. DNSSEC is a highly technical subject with only a limited number of people having an interest in the subject. Given these constraints, we are quite satisfied with the visitor statistics. Although the number of direct comments on the blog is relatively low, e-mail exchanges with blog visitors have led to some interesting insights and discussions.

⁷ Source: Google Analytics, period: June 30th 2010 – January 16th 2011

4 Recommendations

4.1 Roll-out to end users

4.1.1 To-do for SURFnet

During the project, the decision was made not to deliver a full end-user service due to restrictions imposed by the fact that SIDN does not yet have a process for automated submission of secure delegations (DS) for the .nl zone. Once such a process becomes available, however, SURFnet should endeavour to make the full service available to end-users. This would entail the following:

- Implementing DS submission in SURFdomeinen
- Implementing automated DNSSEC disablement (this is currently a manual process)
- Testing the full process (both enablement as well as disablement)
- Operating a pilot with connected institutions
- Standardising the service according to SURFnet Operational Excellence guidelines

4.1.2 Planning

It is very hard to plan for specific dates because it is currently unknown when SIDN will be ready with the automated process for DS submission. Our current estimate is that this will be in the first half of 2011. Nevertheless it is already possible to start with some of the required development work by using stubs were necessary to substitute unknown processes.

Development can start in the last quarter of 2010 and continue into 2011. It should be possible (depending on the complexity of the process specified by SIDN) to have a full implementation available within weeks of SIDN enabling the automated process.

4.2 Future work

4.2.1 Support team

With the implementation of DNSSEC in SURFdomeinen SURFnet is facilitating those connected institutions that use SURFdomeinen to manage their zones. The majority of connected institutions, however, operate their own DNS infrastructure.

In order to support these institutions in their DNSSEC deployments we are thinking about setting up a so-called support team. Such a team would consist of one or more consultants that can assist connected institutions with planning and executing a DNSSEC deployment.

4.2.2 White-papers on DNSSEC deployment

DNSSEC has two sides: signing a zone on the authoritative side and validating queries on the resolving side. To aid connected institutions with the implementation on both sides we aim to publish white papers. These white papers will address the following generic issues:

- How to plan a deployment
- Which services and/or users will be affected
- How to set up policies and procedures
- Which technical decisions need to be made

4.2.3 Investing in OpenDNSSEC

SURFnet has already made contributions to the OpenDNSSEC project. The current stable version of OpenDNSSEC (at the time of writing version 1.1) works well (and is used in our own deployment) but is not as easy to use as we would like it to be for our connected institutions. Therefore, SURFnet is investing in additional development work for OpenDNSSEC together with IIS (the Swedish top-level registry).

We have specifically chosen to invest in new development work only; maintenance and support of the code base will be taken care of by NLnet Labs, which – as an organisation – is much better suited for the continued maintenance of the project.

5 References

- [1] Project Initiation Document DNSSEC in SURFdomeinen
Roland van Rijswijk, SURFnet, January 2010
- [2] Results DNSSEC user survey
Migiel de Vos, Eefje van der Harst and Roland van Rijswijk, SURFnet, August 2010
[http://www.surfnet.nl/nl/innovatie/gigaport3/Documents/FIP4%20D2%20DNSSEC%20user%20survey%20results%20\(v1.0\).pdf](http://www.surfnet.nl/nl/innovatie/gigaport3/Documents/FIP4%20D2%20DNSSEC%20user%20survey%20results%20(v1.0).pdf)