



Technical Description:

## **DNSSEC Functionality in Nixu NameSurfer Suite**

Nixu Software Oy Ltd

Nixu Group

## Table of Contents

<b>1. ENABLING DNSSEC IN NAMESURFER SUITE</b> .....	<b>3</b>
<b>2. ADDING DNSSEC KEYS</b> .....	<b>3</b>
<b>3. EDIT NSEC3PARAM RECORD DATA</b> .....	<b>3</b>
<b>4. AUTOMATED ROLLOVER OF ZONE SIGNING KEYS (ZSK)</b> .....	<b>4</b>
USING THE PRE-PUBLISH METHOD.....	4
USING DOUBLE SIGNATURE METHOD.....	4
<b>5. ACCESS RIGHTS</b> .....	<b>5</b>
<b>6. ENABLING DYNAMIC DNS UPDATES IN NIXU NAMESURFER USING TSIG KEYS</b> .....	<b>6</b>

## 1. Enabling DNSSEC in NameSurfer Suite

Navigate to the zone's page and click "*Settings*" on the left-hand side menu. There, one can see "*Enable DNSSEC*" option. Switching this setting on allows the zone to be secured using DNSSEC. When this setting is not on, adding/manipulating DNSSEC keys on the zone is impossible, and any DNSSEC functionality on the hidden primary server is also unavailable.

To allow DNSSEC secured data to be returned by the server, the zone will need to be equipped with one or more signing keys in addition to selecting this option. Switching this option off does NOT delete existing signatures from the zone; rather, it only turns off signing of subsequent updates. To remove existing signatures, disable all zone signing keys first before turning the option off.

## 2. Adding DNSSEC Keys

After enabling DNSSEC functionality in Nixu NameSurfer as described above, under the zone "*Settings*" page appears a new menu entry – "*Add DNSSEC key*". This page allows creation or upload of keys to use for DNSSEC signing of the zone. The uploaded key file must be in "*private key format*" version 1.2, as generated by the `dnssec-keygen` utility provided with the BIND DNS server software. The `dnssec-keygen` binary is also installed together with the local BIND secondary in the 'named' subdirectory of the Nixu NameSurfer installation.

Nixu NameSurfer currently supports key type RSA-SHA1. The key parser included in the product also recognizes and accepts RSA-MD5 (type 1), RSA-SHA1 (type 5) and DSA (type 3) key types as specified in the DNSSEC specification; however, these three key types will not be functional even though they can be uploaded on the server.

In addition to DSA-SHA1 (type 5) Nixu NameSurfer also supports RSA/SHA-256 (type 8) and RSA/SHA-512 (type 10) keys (RFC5702), as well as the NSEC3-compatibility workaround RSASHA1-NSEC3-SHA1 (type 7) keys. For types 7, 8, and 10 supporting them means also NSEC3 support is mandatory on the server but doesn't need to be enabled on the zone - with type 5 and other older key types it is NOT possible to use NSEC3 at all.

A DNSSEC key can be either a zone signing key, used to sign all resource record sets in a zone, or a key signing key, used only to sign the set of keys that is used to sign the zone. Every DNSSEC signed zone should have at least one of both with the mandatory key type 5.

## 3. Edit NSEC3PARAM record data

This part of the page is hidden unless use of NSEC3 authenticated denial of existence is enabled for the zone (*Zone -> Settings -> General settings*, check-box "*Use NSEC3 denial of existence authentication (DNSSEC only)*"). This form can be used to add, remove and change the NSEC3PARAM record data on the zone, and thus define the parameters used to generate NSEC3 hash nodes on it.

If the NSEC3 records should be generated on the zone, a NSEC3PARAM record must be defined. Otherwise, the zone signing process will revert to using traditional NSEC records instead. The NSEC3PARAM record is defined by entering a Salt length value between 0-255, and then

adding the new Salt string in hexadecimal (numbers 0-9 and letters a-f, two characters for each salt byte) manually, or generating it by pressing the "Generate new salt" action button. Additionally, Hashing iterations contains a numeric value between 0 and 65535, telling how many times the hashing function is repeated on each original value and salt before storing it into a resource record. The length of salt, randomness of the salt value and the number of iterations work together to reduce the possibility of dictionary-based decomposition of the original domain name from the hashed value.

To enable use of NSEC3 records, the NSEC3PARAM record must be inserted into the zone either by entering the Salt length, Salt string and Hashing iterations and then pressing the "OK" action button on the page, or by entering just the Salt length and Hashing iterations values and pressing the "Generate new salt" action button. To disable use of NSEC3, press the "Remove" action button to remove the NSEC3PARAM record from the zone and the database.

#### 4. Automated Rollover of Zone Signing Keys (ZSK)

Two methods are available for automatic zone signing key rollover: the pre-publish method and the double signature method, as proposed in RFC4641. When a key is set up to use automatic rollover, a new key is automatically created in the key chain, with its key inception time set at one zone expiry period before the expiry time of the previous key in the chain, and key expiry automatically set with validity period equal to the previous key.

##### Using the pre-publish method.

Pre-publish rollover means publishing the upcoming new key before it is used for signing; the signatures are generated when the signatures made by the outgoing key are removed. This reduced the zone data / transfer size as there is only one RRSIG per RRSET at any given time.

- The new key is added to the zone  $2 * \text{zone expiry}$  prior to the expiry of the outgoing key.
- The new signatures are added to the zone  $1 * \text{zone expiry}$  prior to the expiry of the outgoing key. The signatures generated by the outgoing key are removed from the zone at the same time (they are still valid, and may exist on secondaries but are no longer server by the master server).
- The outgoing key is removed from the zone root when it expires.
- In the master zone, there is only one set of RRSIGs (per key chain) in any given RR set. Up to 3 versions of a key can exist in the zone root (outgoing key, current key and upcoming key), only one of them being used.
- For correct operation of rollover, key validity period (key expiry - key inception) must be at least  $2 * \text{zone expiry}$ , this is also automatically corrected in rollover on future releases if the user has specified a too short validity period, or the zone expiry period has been adjusted so that this rule isn't fulfilled for a key any more.

##### Using double signature method.

Double signature rollover means publishing the upcoming key and the signatures generated by it at the same time. This happens before removing the signatures generated by the outgoing key, thus increasing the zone data / transfer size at the time of rollover because 2 RRSIGs exist per RRSET.

- The new key is added to the zone  $2 * \text{zone expiry}$  prior to the expiry of the outgoing key. It will immediately generate signatures that are valid from that moment until the expiry of the new key.

- The signatures generated by the outgoing key are removed 1 \* zone expiry prior to the expiry of the outgoing key. They are no longer served by the master but may exist on secondaries and are still valid.
- The outgoing key is removed from the zone root when it expires.
- In the master zone, there must exist at least one set of RRSIGs (per key chain) in any given RR set. During the double signature period (from 2 \* zone expiry to 1 \* zone expiry prior the expiry of the outgoing key) there will exist two RRSIGs in one set (per key chain).
- For correct operation of rollover, key validity period (key expiry - key inception) must be at least 3 \* zone expiry, this is also automatically corrected in rollover on future releases - on existing release, however, specifying a bad key validity period can produce really weird results like multiple signatures, multiple upcoming keys, or no signing at all at times.

Automatic rollover is done only on keys that are currently in use and that are not yet expired. Thus, keys that are not in use, or are taken into use after their marked expiry time, will not be automatically rolled over even if the rollover is enabled on them.

When choosing the proper validity period for a key with rollover, it should be noted that the key validity should never be shorter than the maximum TTL (expiry time) of the zone data, and preferably the key should be valid for at least two times the zone expiry period to avoid having multiple pre-published future keys or multiple (more than two) simultaneous signatures in double signature mode.

If a key is configured with its automatic rollover function set on, Nixu NameSurfer will delete the outgoing (old) signatures created with the previous key at one zone expiry period prior to the key expiry. If a key without automatic rollover is used, the signatures will remain in the zone until the key expires.

Starting from the next release (6.8.2/6.9.1), the automatic rollover will force the minimum key validity period (for a new automatically generated key) to be longer if it was set too short - the minimum is 2 \* current zone expiry for prepublish key and 3 \* current zone expiry for a double signature key. For current release, setting the key validity within those borderlines is also highly recommended so the rollover will work without significant problems.

## 5. Access rights

Since NameSurfer UI quite explicitly requires that any RRs modifiable by a user must be allowed for that user, the DNSSEC RR types (DNSKEY, RRSIG, NSEC, NSEC3, NSEC3PARAM) are and must be specified in the group rights. However, none of these RRs can be manipulated directly from the node data page even if the user has the rights, because that would not be safe (all except DNSKEY and NSEC3PARAM are automatically generated, and even those are generated with acceptable values by the zone settings page). However, if a user doesn't have rights set for those RR types, removing a node that contains any of those RR types will not be possible for that user.

Apart from the ones mentioned above the DS (Delegation Signer) record can be directly manipulated by the user that has the rights to it. This is because it is used in a parent zone to refer to the keys of a child zone. If both the parent and child zone exist in the same instance of NameSurfer, and automatic delegation update is used when manipulating the root node of the child zone or the delegation in the parent, NameSurfer attempts to automatically synchronize the DS records in the parent with the KSKs of the child zone.

To define appropriate access rights for the group, please navigate to *Configuration -> Groups* and click the link with group name (or create a new one). Each group has the following accessibility settings available for the Nixu NameSurfer Suite modules listed below:

Modify - the group members can create, modify and/or remove module contents.

View - the group members can only view the module contents, but cannot change them.  
No access - the group members do not have any kind of access to the modules or to their contents.

The DNS access limitations have an additional access level:

Full access - the group members can create, modify and/or remove zones and views in addition to DNS data.

Modify rights on zones only give rights to manipulate zone data and settings.

Access to Keys: TSIG and NSAPI keys. Access levels are: Modify, View and No access.

Access Restrictions -> Access to specific record type(s): When a new group is created, all its members have rights to modify all record types by default. This is indicated by marked checkboxes. In order to restrict group's access to specific record types (DNSSEC, RRSIG, NSEC), please unmark the appropriate checkboxes.

## 6. Enabling Dynamic DNS Updates in Nixu NameSurfer using TSIG Keys

TSIG keys can be used to configure Secure DynDNS in Nixu NameSurfer. To create a new key, navigate in UI to the "DNS" -> "Keys" -> "New TSIG key". With the checkbox "*Can be used for Dynamic DNS updates:*" (available for TSIG keys only) one can specify whether the key may be used for dynamic DNS updates. If no zone restrictions have been specified for the TSIG-key on the key configuration page, any master zone managed in Nixu NameSurfer can be dynamically updated using the key.