1 - Introduction

1.1 - Overview

This document conforms with the RFC-draft DNSSEC Policy & Practice Statement Framework and defines security practices used by NIC.br for
the .NATURA TLD.

1.2 - Document name and identification

Document title: DNSSEC Practice Statement

Version: 1.2

Created: March 29, 2012
Last Revised: June 12, 2019

1.3 - Community and applicability

The following roles can be defined as participants of the domain registration process:

Registry - Natura Cosméticos S.A. is responsible for managing the .NATURA
zone. Natura Cosméticos S.A. hired Nucleo de Informacao e Coordenacao
do Ponto BR (NIC.br) as its technical back-end.

Back-end - NIC.br is under contract to manage the .NATURA zone, including
key pair generation, signing and publishing, as well as guaranteeing the integrity of private keys.

Registrar - Registrars need to be previously registered and accredited
with the Registry. They'll be responsible for handling registrant's requests and communicating with the Registry for creating and updating
domains.

Registrant - Registrant is the person or organization that represents
the end user for the domain, making that request to one of the available registrars.

Management of the DNSKEYs of a domain, if present, can be done either
by the registrar or the registrant itself, depending on registrar policy.

1.4 - Specification Administration

1.4.1 - Document Management

NIC.br - Nucleo de Informacao e Coordernacao do ponto BR

1.4.2 - Contact Information

NIC.br
Av. das Nacoes Unidas, 11541, 7o. andar
04578-000 - Sao Paulo - SP
BRAZIL

www.nic.br
dnssec@registro.br

Natura Cosméticos S.A
Av. Alexandre Colares 1188 Vila Jaguara
05106-000 - Sao Paulo SP

www.natura.com.br
dominios@natura.net

2 - Publication and repositories

2.1 - Repositories

Current version of .natura DPS is available at http://nic.natura.

2.2 - Publication of Public Keys

The public keys are published in DNSKEY format and DS are published directly in the root zone.

3 - Operational Requirements

3.1 - Identification and authentication of child-zone manager

All authentication and identification mechanisms are provided by EPP protocol. All connections to the EPP server are allowed only from previously registered IP addresses by the registrars.

3.2 - Registration of delegation signer (DS) record

All DS records must be informed through the EPP interface, using the format indicated in RFC4310 (EPP DNS Security Extension Mapping 1.0) or RFC 5910 (EPP DNS Security Extension Mapping 1.1). Whenever this happens a DNS query is performed for the DNSKEY of the zone in order to check if the provided DS is valid.

3.3 - Method to prove possession of private key

Whenever the DS is informed, the system performs a query for the DNSKEY of the zone, as well as its signatures, in order to validate it.

3.4 - Removal of DS record

3.4.1 - Who can request removal

Only the Registrar that owns the child-zone is allowed to request a DS
removal.

3.4.2 - Procedure for removal request

All requests of DS removal are performed using EPP interface.

4 - Facility, management and operational controls

4.1 - Physical controls

4.1.1 - Physical access

- Building and Site Access

NIC.br site shares the building with other organizations. The building
management complies with minimum standards. The building management keeps security guards 24x7 covering all the tower entrances. NIC.br has its own and independent access control system and can grant access
or not to any visitor, not relying on building system. NIC.br has a video surveillance system that keeps track of all points of entry, fire exits and departments entrance. There isn't any historical record
of natural disaster near building's area like flood neither earthquakes.

- Datacenter Access

NIC.br gives datacenter access only to the personnel directly involved
in projects hosted in it. The datacenter access control system is audited monthly by the Operations Manager. Third-party employees and visitors can only enter accompanied by an authorized person. Before enter the datacenter the personnel needs to go into an anteroom first,
where there is always (24x7) a datacenter technician. Both entrances are protected by proximity badge and biometric authentication. The anteroom and datacenter have different access levels. The entrances, anteroom and datacenter aisles are monitored by the video surveillance
system.

- DNSSEC infrastructure protection

The devices that make up the main DNS infrastructure, such as the hidden master server, signer and HSM, are all stored inside a safe that is password protected.

4.1.2 - Fire detection and protection

The facility is equipped with smoke detectors and sprinklers, expect for the datacenter where sprinklers are replaced by FM200 liquified compressed gas system.

4.1.3 - Power and air conditioning

NIC.br's datacenter is protected by two redundant and independent UPS systems, providing two supply lines called QL1 and QL2. Each rack is fitted out independently by lines QL1 and QL2, with its own circuit breaker for each line. Unswitched PDUs are installed in all racks. An exclusive diesel generator is activated automatically in case of mains electricity failure. Its autonomy is around 15 hours. A backup line power is available to fit out the datacenter in case of any issue with main switch. The backup line can be used by the (1) mains, (2) generator, (3) building tower generator or (4) external rented generator.

Three Air Conditioning Variable Refrigerant Flow (VRF) independent systems are installed and dedicated to the datacenter. They work in a 2:3 scheme, where one is kept as a backup system. Automatic rotation between the systems is done in order to avoid uneven wastage. All the systems are protected by the diesel generator and can be fitted out by the backup power line.

4.1.1 - Waste disposal

All printed documents are properly shredded when no longer necessary.
Used hard drives, when damaged, are never returned to the manufacturer, instead they are stored in a safe location before being completely destroyed.

4.1.2 - Off-site backup

There is a complete infrastructure that is capable providing full DNS service located at least 8Km from the main site. All relevant data is kept synchronized using an IPSEC tunnel.

4.2 - Procedural controls

NIC.br trusted roles includes system administrators and datacenter's

operators. Each trusted role has a specific task that is described bellow.

* DNS servers monitoring are done by at least two of seven datacenter's operators 24 hours a day.

* Infrastructure tasks are done by at least one of seven datacenter's operators and one of four system administrators. Where the datacenter's operators are responsible for installing the equipments and the system administrators are responsible for configuring the installed equipment. Datacenter's operators don't have logical access to any equipment.

* Administration tasks are done by at least one of four system administrators.

Datacenter's operators and system administrators have the same access level to the anteroom and datacenter area. The identification of each role is done by proximity badge and biometric authentication, and all attempts to access the restricted area are logged.

4.3 – Personnel controls

All personnel must have at least college degree in the area of information technology and one year of experience. For the purpose of hiring new employees, a specialized company is used in aiding the recruiting process.

Frequently, all personnel is encouraged to take part in training courses in the area of activity.

Occasionally, whenever there's a open job position, it's preferably filled by someone that's already working in the company. Additionally, it is also common that datacenter's operators are promoted to system administrators, as an opportunity arises.

In case of an unauthorized action by any of the employees, a formal warning is given.

4.4 – Audit logging procedures

The entire facility is covered by security cameras. The datacenter videos are stored for 1 year.

All access to the datacenter is logged based on proximity card and biometric authentication.

Any type of physical access to the DNSSEC infrastructure, which includes
the hidden master, signer and HSM, must be properly documented.

Only system administrators have access to these logs.

4.5 - Compromise and disaster recover

In the event of a disaster that complete compromises the main site, the default procedure is to activate the DNSSEC backup infrastructure,
which should be restored less than 24 hours.

5 - Technical Security Controls

5.1 - Key pair generation and installation

The .NATURA zone will have two sets of keys: KSKs and ZSKs, each with a
different handling policy:

5.1.1 - KSK

The Key Signing Key (KSK) is generated and stored in a Hardware Security Module (HSM), which is kept inside a safe. The KSK size is 1280-bit.

The KSK's public key is exported using HSM protocol.

5.1.2 - ZSK

The Zone Signing Key (ZSK) is generated and stored in a remote machine,
called signer, that is connected directly to the server where the zones are generated, kept in a private network. The ZSK size is 1024-bit.

The communication between DNS server and signer is done over a proprietary protocol that is protected by a shared secret authentication.

5.2 - Private key protection

5.2.1 - KSK

The HSM access is protected by smartcards in a 4:12 scheme, meaning that 4 cards out of possible 12 are required to grant access to the device. The communication to HSM is done over a text protocol via TLS
connection.

The KSK is stored in a HSM that is also directly connected to the DNS
server. This architecture provides better security for private keys

and more entropy for key generation as well.

5.2.2 - ZSK

The ZSKs are kept in the disk of the signer, each encrypted with a symmetric key, which is then split in 2:8 scheme using the Shamir Secret Sharing Scheme (SSSS). These parts are protected by smartcards. This way, it is necessary to have at least 2, out of possible 8 smartcards to decrypt the ZSKs, which are then stored only
in memory ready to be used for signing purposes. If by any chance the
signer machine goes down, the activation process needs to be repeated
in order to restore its functionality.

The ZSK's private key are replicated on a backup site which is kept synchronized with the main site.

5.3 - Other aspects of key pair management

The operational period of the ZSKs is 3 months. For the KSK it varies
from 2 to 5 years. A more detailed description can be found on Rollover section.

5.4 - Activation data

In order to make both types of keys (ZSK and KSK) available for usage,
a set of smartcards is necessary to grant access to the keys. Each smartcard is protected by a PIN.

5.5 - Computer security controls

The entire infrastructure that handles zone generation and signing are
safely stored inside NIC.br's facilities, as described in section 4.1. Access is limited to system administrators and crypto officers -
authorized people that possess the required smartcards.

The system is designed to operate mostly automatically, with a minimum
of human intervention, which should happen only twice a year, when new
keys are generated. These events, called ceremonies, are properly logged and audited.

5.6 - Network security controls

The main DNS infrastructure, where the zones are generated and signed,

is properly protected by a dedicated firewall hardware that only allows traffic from designated slaves to perform DNS queries and transfer zones.

There is also an IPSEC tunnel connecting the main site to the backup site, that is used for keeping the data synchronized.

Each slave is protected at the border router, where only DNS traffic is allowed to pass.

5.7 - Time stamping

All servers are kept with their clocks synchronized using the NTP protocol.

6 - Zone signing

6.1 - Key length and algorithms

Key lengths and algorithms are defined in order to be sufficient to prevent crypto-analysis attacks during its operational period.

The RSA algorithm with a modulus size of 1280-bit is used for KSK. For
ZSK uses a RSA algorithm with modulus size of 1024-bit.

Supported DS digest algorithm types are SHA-1 and SHA-256, defined in
RFC4509.

6.2 - Authenticated denial of existence

The NSEC3 denial of existence method is supported.

6.3 - Signature format

Signatures are generated using RSA signing algorithm in conjunction with a hash algorithm that must use SHA256 function.

6.4 - Key roll-over

To minimize the risk of compromising DNSKEYs, periodic rollovers are programmed. There are rollovers for both the ZSKs and KSKs, and these
events happen in previously defined moments.

For the ZSKs, the rollover happens every 3 months in a pre-publish strategy, when the new key is inserted 1 day before it becomes effectively active. Two days later, the old key is removed, to ensure
that no invalid data is cached in recursive name servers.

KSKs are replaced after 2 to 5 years of use, in a pre-publish procedure, where the new key is inserted 3 weeks before it becomes

effectively active. In this interval, it is expected that the new DS is inserted in the parent zone.

Either way, all the new keys involved in the rollover process, are generated in a ceremony, as well as the KSK signatures and a schedule
of events when keys will be added and removed.

6.4.1 - Ceremonies

There are two sites with the same infrastructure. A ceremony happens each time in a different site and at the end of a ceremony, all data (ZSKs and signatures) is synchronized with the other site. The connection between the sites uses IPsec with SSL. All private ZSK are
encrypted with the smartcards.

There are 4 HSMs (two on each site), where one is used at ceremonies while the other remains turned off as a backup. The contents of HSMs only needs to be synchronized when there is a KSK rollover (every 2 to
5 years). This procedure needs to be done manually, where a public key
is exported from the device receiving the new data, and it is used to
encrypt the data that will be synchronized.

Twice a year, a ceremony will happen to prepare the software for the next 6 months. This involves generating the future keys, using the HSM
to sign the DNSKEYs with the KSK and schedule the next rollovers.

The usual ceremony will create 2 new ZSKs, generate all the necessary
KSK signatures for the appropriate period and schedule the next 2 ZSK
rollovers. If needed, a new KSK can also be created, as well as its rollover scheduled in a double-signing way.

It's important to note that, since the ceremony is the only event where the HSM is used, and therefore it is necessary to have at least
4 of the 12 smartcards to activate it.

6.5 - Signature life-time and re-signing frequency

The signature validity period of the zones signatures is one week, and
automatic resigning guarantees that every record is resigned in 3 days
at most. Considering that TTL of the records is one day, this policy ensures that an expired signature is never cached by a recursive name

server.

The signatures generated by KSK have a validity period of 21 days. The
signatures are replaced every 14 days, this results in two valid
signatures overlapped by one week. This policy gives us time to
recover in case something goes wrong.

Since the KSK resides in the HSM, which remains turned off most of the
time, we seek to generate all the signatures necessary for a period of
6 months at once, in an event that is called a ceremony.

6.6 - Verification of resource records

At every publication all resource record signatures are validated
before the zone is published.

6.7 - Resource record time-to-live

DNSSEC related resource records are defined with the following TTL:

- DNSKEYs is 6 hours.
- NSEC3 is the same as SOA minimum (900 seconds).
- DS is 1 hour.
- RRSIG is the same as the covered RRSET (may vary).

7. Compliance Audit

7.1. Frequency of entity compliance audit

Audits are performed at least once a year.

7.2. Identity/qualifications of auditor

NIC.br-managed TLD (Top-Level Domains) DNSSEC Policy and Practice
Statements audits are performed by the crypto officers. Each crypto
officer is a NIC.br employee or trusted community
representatives. Trusted community representatives have proficiency in
IT security, DNS and DNSSEC.

7.3. Auditor's relationship to audited party

Some of the auditors are NIC.br employees; the others are trusted
community representatives.

7.4. Topics covered by audit

Each audit includes DNSSEC key management procedures, keys and
signature life cycle management and infrastructure controls.

7.5. Actions taken as a result of deficiency

Deficiencies are corrected at the "A" phase of the PDCA (Plan, Do, Check, Act) cycle, starting as soon as the deficiency is discovered. The next audit then checks whether the deficiency has been cleared out.

7.6. Communication of results

Deficiencies are communicated to NIC.br through a private mailing list where all crypto officers are subscribed.

8. Legal Matters

8.1 Fees

No fees are charged for any function related to DNSSEC. We reserve, though, the right to provide financial incentives for DNSSEC-signed domains in an equal fashion among registrants and registrars.

8.2 Financial responsibility

Both NIC.br and Natura Cosméticos S.A. accepts no financial responsibility for improper use of Trust Anchors or signatures, or any other improper use under this DPS.

8.3 Limitations of liability

Both NIC.br and Natura Cosméticos S.A. shall not be liable for any financial loss, or loss arising from incidental damage or impairment, resulting from its performance of its obligations hereunder. No other liability, implicit or explicit, is accepted.

8.4 Term and Termination

The DPS is amendeded from time to time. This version of the DPS is valid until it is replaced by a new version.

8.5 Dispute resolution provisions

Disputes among DNSSEC participants shall be resolved pursuant to provisions in the applicable agreements among the parties.

8.6 Governing law

This DPS shall be governed by the laws of Brazil. The many treaties where Brazil is a signatory can provide stakeholders from other

countries with ample support to uphold their lawful rights.