DNSSEC Practice Statement .CORSICA

Registry domain signature policy and conditions of implementation

(Version 02 – 11/06/2013)

Document management

Document identification

Responsible for document
Chief Security Officer

Titre	DNSSEC Practice Statement .CORSICA
Référence document	DPS-CORSICA-01
Version	V02
Dernière modification	June 2013

Security classification		File Name
Public	X	dps-english-CORSICA.pdf
Sensible/Interne	☐	
Réservé/diffusion restreinte	☐	
Stratégique/critique	☐	

Approved by

Date	Nom	Fonction
January 2012	Alain Caristan	Chief Security Officer
11 June 2013	Alain Caristan	Chief Security Officer

Revisions

Version	Author	Date	Revision
V01	Alain Caristan, David Barou	march 2012	Creation
V02	Alain Caristan, David Barou	june 2013	Update to RFC_6841, January 2013

Contents

DPS .CORSICA

Afnic domain signature policy
and conditions of implementation

1. Introduction

This document describes all the policies, procedures and tools used to sign the .CORSICA zone, thanks to DNS Security Extensions (DNSSEC).

DNS Security Extensions respond to these vulnerabilities by implementing cryptographic signature mechanisms to ensure the integrity and authenticity of DNS records.

This DPS is one of several documents relevant to the operation of the .CORSICA zone.

This document provides the items enabling all the users of the .CORSICA zone to assess the security level of the chain of trust in the .CORSICA extension. It also presents the processes and infrastructures implemented for the security of the registry.

1.1. Overview

The Domain Name System Security Extensions (DNSSEC) is a set of IETF specifications for adding origin authentication and data integrity to the Domain Name System. DNSSEC provides a way for software to validate that Domain Name System (DNS) data has not been tampered with or modified during Internet transit. This is done by incorporating public key cryptography into the DNS hierarchy to form a chain of trust originating from the root zone.

The framework outlines the contents of a set of provisions, in terms of eight primary components, as follows:

1. Introduction
2. Publication and Repositories
3. Operational Requirements
4. Facility, Management, and Operational Controls
5. Technical Security Controls
6. Zone Signing
7. Compliance Audit
8. Legal Matters

1.2. Name and identification of document

Document title: DPS .CORSICA
Version: v2

Created: 01/01/2012
Updated: 11/06/2013

1.3. Community and applicability

The following parties to which this document has applicability have been identified. The relation between the Registry and a Registrar is regulated in the Registry-Registrar Agreement.

1.3.1. Registry

Afnic (the French acronym for the French Network Information Centre (Association Française pour le Nommage Internet en Coopération) is in charge of the management of the .CORSICA zone. This means that Afnic manages, adds, changes and deletes the data pointing domain names to authoritative zones for the .CORSICA extension. It also means that Afnic manages and upgrades the technical infrastructure ensuring the performance and resilience of the .CORSICA zone at its proper level.
Similarly, Afnic manages the keys to cryptographically sign registrations in the .CORSICA zone, according to the manner and the procedures described below.
Afnic undertakes to regularly use its ZSK to sign the cryptographic summary of the KSKs of delegations signed under the .CORSICA TLD.

1.3.2. Registrars

The registrar is the third party responsible for the administration and management of domain names on behalf of the Registrant. The registrar handles the registration, maintenance and management of the Registrant's domain names. It is responsible for the identification of these Registrants.
It is also responsible for adding, deleting and updating of borrowed Delegation signer (DS) public keys, at the request of the Registrant or the technical contact of the corresponding domain name.

1.3.3. Registrants and contacts

A domain name is created by its Registrant, who defines a technical contact responsible for the administration of the zone. When they administer their zones themselves, the contacts designated for a domain name can transmit the KSK fingerprints and manage their publications through the interfaces of their registrar, if they administer their zone.

1.3.4. Relying Party

The Relying Party is involved in the deployment of DNSSEC across the resolution chain, such as the validation of signatures by the resolvers and other applications. The Relying Party is involved in the deployment of DNSSEC and in updating the keys. This party must be informed of any updates by Afnic on

its zones if the .CORSICA key is used as a trust anchor. Otherwise it must keep abreast of any updates of the DNS root keys.

1.3.5. Auditor

The auditor is the entity that audits both the DNSSEC service and the way in which Afnic operates it.

1.3.6. Applicability

Each Registrant is responsible for determining the appropriate level of security needed for the domain names whose TLDs are managed by Afnic. The DPS is only applicable at the level of Afnic extensions and describes the procedures, security controls and practices applicable to the use and management of the keys and signatures used for the .CORSICA.

With the support of this DPS, the relying party can determine the level of confidence they attribute to the extensions managed by Afnic and deduce their own level of risk.

1.4. Specification Administration

This DPS is updated as appropriate, such as in the event of significant modifications in systems or procedures that have significant effect on the content of this document.

1.4.1. Specification Administration Organisation

[NOM DU REGISTRE], .CORSICA registry

1.4.2. Contacts

DNSSEC PMA (Policy Management Authority):

Afnic
Immeuble International
13 avenue de la gare
Hall A2 - 7ème étage
Montigny le Bretonneux
France
http://www.afnic.fr

Contact information
Afnic
support@afnic.fr

1.4.3. Specification change Procedures

The .CORSICA DPS is reviewed on an annual basis or in case of force majeure. This revision is made by the .CORSICA DPS Manager (see 4.2.1).

Changes are made to DPS either in the form of amendments to the existing document or by publishing a new version of the document.

The DPS and its amendments are published at:
https://www.afnic.fr/fr/ressources/documents-de-reference/politiques-de-registre/dps-4.html
Only the latest version of the DPS is applicable.

2. Publication and repository

2.1. Publications on the Afnic website

Afnic publishes important information on DNSSEC for each of its extensions at
http://www.afnic.fr/en/certificates/
The official electronic version of the DPS is published at:
https://www.afnic.fr/fr/ressources/documents-de-reference/politiques-de-registre/dps-4.html

Notifications on DNSSEC are pushed on:
https://www.afnic.fr/en/about-afnic/news/operations-news/
and
https://twitter.com/AFNIC_Op

2.2. Publications of publics keys

Afnic publishes its KSK as a DNSKEY and DS
The DNSKEY to be used as the trust anchor is published on the Afnic website at
http://www.afnic.fr/en/certificates/
The DS is published with IANA in the root of the DNS.

3. Operational Requirements

3.1. Meaning of domain names

The domain is a unique identifier that is associated with services such as web access, domain name hosting or e-mail. Applications for registration under the .CORSICA TLD are in accordance with a Naming policy that is elaborated with the Registry Operator.

The procedures manual for the registration of domain names is available here:
https://www.afnic.fr/en/resources/reference/technical-guidebooks/gtld-6.html

3.2. Activation of DNSSEC for child zones

DNSSEC is enabled for a domain name by at least the publication of a DS record in the .CORSICA zone, which creates a chain of trust with the child zone. The registrar is responsible for transmitting the DS, Afnic supposes that the DS record provided is correct and cannot carry out any specific checks other than those used by Zonemaster tool. (**http://www.zonemaster.fr/**).

3.3. Identification and authentication of child zone manager

The Registrar is responsible for properly identifying and authenticating the Registrant with a mechanism that is both appropriate and compliant with the contracts that bind the Registrar with its client and Afnic.

3.4. Registration of delegation signer (DS) resource records

Afnic accepts DS publication applications of via the EPP interface and a web form secured by TLS. For EPP, the registrations must be validated and submitted in the format specified in RFC 5910 (Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)).
A maximum of 5 DS records can be published.

3.5. Method to prove possession of private key

The Registry does not conduct any checks with the aim for validating the Registrant as the holder of e certain privat key. The registrar is responsible for conducting the checks that are deemed necessary to ensure the proper operation of the domain names it is responsible for registering.

3.6. Removal of DS record

A DS record can be deleted by request from the registrar via EPP or a web form secured by TLS. The removal of all the DS records is used to deactivate the DNSSEC security mechanism for the zone in question.

3.6.1. Who can request removal

Only the registrar, or the Registrant's representative as the Technical contact or the Administrative contact formally designated by the Registrant, can place orders to remove DS records at the request of its client.

3.6.2. Procedure for removal request

The Registrant, or the Registrant's representative as the Technical contact or the Administrative contact formally designated by the Registrant, is assigned to perform the task of carrying out the removal.
The registrar performs the removal request using the procedures defined by Afnic.
In response to the removal request from the Registrar, Afnic deletes the DS record from the .CORSICA zone.
The time required for the removal of a DS record from the .CORSICA zone after receiving the removal request from the registrar depends on the update of the DNS programmed by Afnic. The maximum update delay is therefore 10 minutes.

3.6.3. Emergency removal request

A Registrant of a domain name under an extension managed by Afnic who is unable to contact the registrar for the name, may use a special procedure for removing DS records, similar to the auth_info emergency request procedure.

4. Facility, management and operational controls

4.1. Physical Controls

Afnic has set up the physical security controls to meet the requirements specified in this DPS.

- Double access security to the site with permanent guarding and guard tours.

  A double-check of the identity and access authorization of each person working on the site is carried out at the walk-in service, and then at the guard house, with presence of staff guaranteed 24/24.
  An access system by individual badge and a 3-D biometric recognition system complete the procedure by restricting access to authorized zones and enabling the "traceability" of people on the site. Three checkpoints are installed between the site entrance and the customer area.

  In addition, security of the premises is further ensured by a CCTV system plus infrared cameras placed outside. A large number of cameras digitally film and record movements inside the premises and outside the buildings.
  A battery of control monitors record and retain filmed data over periods of up to 6 months.

- Resilient Infrastructure offering large spaces and a ground load of up to 2 tons.

- Multi-building site interconnected by concrete tunnels.

4.1.1. Site location and construction

Afnic has set up a data center geographically remote from the head office. The site complies with Tier3 standards that guarantee the high security and high availability of hosted systems. All the system components are protected in a physical perimeter with access control and an alarm system.
The Afnic business continuity plan meets best practices in terms of physical security, power supply, environmental, fire and water protection.

4.1.2. Physical access

Physical access to the secure environment is limited to authorized personnel. The entrance is continuously monitored.
On the Datacenter site, Afnic has a private room, access to which is controlled by badge.

4.1.3. Power and air conditioning

Power is supplied to the operational facilities through several separate sources. In the case of outages, power is supplied by the emergency power systems in the data center (applying Tier 3 level from Uptime Institute (based on ANSI standard: ANSI/TIA-942). They can provide power for up to 72 hours.

Nota:

- tier 1
  - Single non-redundant distribution path serving the IT equipment
  - Non-redundant capacity components
  - Basic site infrastructure guaranteeing 99.671% availability
- Tier 2
  - Meets or exceeds all Tier 1 requirements
  - Redundant site infrastructure capacity components guaranteeing 99.741% availability
- Tier 3
  - Meets or exceeds all Tier 1 and Tier 2 requirements
  - Multiple independent distribution paths serving the IT equipment
  - All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture
  - Concurrently maintainable site infrastructure guaranteeing 99.982% availability

4.1.4. Water exposures

The site is in a zone not liable to flooding. The facilities are protected from flooding by:

- A water detection system under the raised floor and on all the hardware.
- A drainage architecture (drainage and lifting pumps in the galleries in the basement)

4.1.5. Fire prevention and protection

The site meets the following industrial safety standards:

- A Class A fire safety system
- A nitrogen sprinkler system
- Application of Rules R7/R13/R4
- Maintenance of the NFS 940 standard
- Regular training of teams
- Facilities for fire-fighter reception and response

4.1.6. Media storage

Storage is performed in accordance with the Afnic storage policy. The classification of information defines mandatory storage conditions, especially for sensitive data.

4.1.7. Waste disposal

All the storage media or those that have contained sensitive information must be withdrawn from service or destroyed in a secure manner by Afnic or a contractor.

4.1.8. Off-site backup

Afnic data is automatically replicated to two remote sites. Domain data is entrusted to a third-party escrow agent conforming with the ICANN DataEscrow procedure.

4.2.Procedural Controls

4.2.1. Trusted roles

Trusted roles are given to people with the ability to manage the contents of the zone file, i.e. the trust anchors. They are also capable of producing and using cryptographic keys.

The trusted roles are:

- Cryptographic operators (2 out of 9)

  A designated operator enters all the instructions described in the procedures presented by the master of ceremonies on cryptographic boxes.
  The HSM in auto-online mode performs some of the operator functions.

- Security Officers (2 out of 9)

  The security officers enable access to the different menus of the boxes with their cards and ensure that all of the ceremony takes place according to Afnic procedures. Afnic security officers are also cryptographic operators.

- Key Holders (1 out of 4)

  Keep the backup smart cards (SMK / ISMK) that define the user rights for HSM keys, Key applications, and backed-up signing keys. Each key is required to perform the backup or import the signing key (application keys) on different smart cards. On the other hand, the SMKs are backed-up in the box and only two out of the 4 keys are needed to restore the SMK. The security officers must authorize the operations involving these personnel.

- Signing system administrators

  They are responsible for the configuration files of the signing solution and the supply of the backups to be placed in a safe.

- Auditors
  They periodically check the machine logs and ensure that the processes automated via the API work as scheduled.

- The Master of Ceremonies (1 out of 3)

  S/he prepares all the ceremonies by constructing a scenario based on Afnic procedures. S/he enables access to the safe and distributes all the cards to the personnel involved in the ceremony. S/he is responsible for stopping or continuing the ceremony in case of problems or unforeseen events.

4.2.2. Identification and authentication for each role

Only persons who have signed a confidentiality agreement and have been cleared by Afnic can assume one of the trusted roles. Anyone wishing to access the system must present a valid ID.

4.2.3. Tasks requiring separation of duties

A single person cannot simultaneously hold two cards of the same trusted roles (security officer or operator) which means that two persons at least are needed to perform ceremonies.

An administrator of the signing system cannot also be an operator;

No separation of duty has been required between the two roles of operator and security officer which means that a security officer can also be an operator.

4.3.Personnel Controls

4.3.1. Qualifications, experience, and clearance requirements

Applicants wishing to operate a trusted role must provide proof of their qualifications and past experience.

4.3.2. Background check procedures

Internal or external recruitment is conducted by the HR function of Afnic, which checks the background and qualifications of candidates, taking into account:

- Their curriculum vitae
- Previous employment
- References
- Diplomas obtained

To be eligible for one of the trusted roles, these controls must not result in a criterion of unsuitability.

4.3.3. Training requirements

The Registry provides the necessary and relevant training on its procedures, administration and technical systems that are associated with each trusted role. Tests are performed after each training course has been completed in order to improve the recognized skills of the person.

These training courses involve:

- Training on Afnic operations
- Training in the management of domain names
- Training in DNS and DNSSEC theory
- Information on the security policy
- Training on quality procedures

4.3.4. Retraining frequency and requirements

Staff assuming trusted roles must take these training courses and additional tests in case of major changes to operations, or once every three years.

4.3.5. Job rotation frequency and sequence

The responsibility for conducting the operations will be given, as much as possible, in turn to all the personnel with a trusted role.

4.3.6. Sanctions for unauthorized actions

The sanctions arising from unauthorized actions are specified in the accountability agreement corresponding to the trusted role. Gross negligence can lead to dismissal and the liability of the person for any damage caused.

4.3.7. Contracting personnel requirements

Under certain circumstances, The Registry may need to use third parties to supplement full-time internal resources. These third parties sign the same type of accountability agreement as full-time employees.
Third parties who are not qualified for trusted roles may not take part in the activities described in 4.2.2.

4.3.8. Documentation supplied to personnel

The Registry and its technical teams provide the necessary documentation so that the employee or contractor can carry out their work satisfactorily and safely.

4.4.Audit Logging Procedures

Automated procedures involve the collection of information on the fly of activity in the registry, forming an activity logbook.

This logbook is used to monitor operations for statistical purposes and for investigations in the event of suspected or confirmed violations of Afnic policies and regulations.
The information in the logbook also includes reviews, lists and other paper documents vital for security and audit purposes.
The purpose of storing information in the logbook is to be able to reconstruct the sequence of events and analyze them to determine which people or applications / systems did what and when.
The logbook and identification of users can be used to establish the tracing and monitoring of unauthorized uses.

4.4.1. Types of events recorded

The following events are included in automatic logging:

- All activities that involve the use of an HSM, such as key generation, key activation, as well as the signing and exporting of keys.
- Attempts for remote access, successful and unsuccessful
- Priviledged operations
- Entrance into a facility

4.4.2. Frequency of processing log(s)

The logs is/are analyzed continuously through automated and manual controls. Specific checks are conducted for the management of cryptographic keys, system reboots and anomaly detection.

4.4.3. Retention period for audit log information

Log information is stored in the system, and then archived for a minimum of 10 years

4.4.4. Protection of audit log(s)

All electronic log information is stored at the same time in at least two distinct sites remote from one another. The recording system is protected against manipulation and unauthorized viewing of the information.

4.4.5. Audit log backup procedures

All electronic log information are backed up and stored in secure premises independent of the system.

4.4.6. Audit collection system

All the information on paper is scanned and stored electronically at the same time in at least two distinct sites remote from one another.

4.4.7. Notification to event-causing subject

The staff concerned is informed of the use of the logbook(s). The staff is not authorized to view the data in the logbook(s).

4.4.8. Vulnerability assessments

All the anomalies in the information of the logbook(s) are studied to analyze potential vulnerabilities.

4.5. Compromise and Disaster Recovery

4.5.1. Incident and compromise handling procedures

An incident is defined as:

- any actual event of a critical nature to security or perceived as such that has caused or could have caused an outage or damage to the information system,
- any disturbance and / or default due to incorrect information,
- any breach of security.

All the incidents are treated in accordance with the Registry procedures. The incident management procedure requires:

- investigating the causes of the incident,
- identifying the effects it has had or could have had,
- taking appropriate measures to prevent it from happening again and reporting this information.

In the event that an incident could lead to the suspicion of key compromise, an immediate roll-over of the key is carried out in accordance with the procedures specified in Chapter 4.5.3.

4.5.2. Corrupted computing resources, software, and/or data

In the event of corrupted computing resources, software, and/or data, the procedures for incident management must be applied and appropriate measures must be taken.

4.5.3. Entity private key compromise procedures

The suspicion that a private key has been compromised or misused leads to the roll-over of the key as described below:

For the ZSK
If a zone signing key (ZSK) is suspected of being compromised, it is immediately taken out of production and is no longer used. If necessary, a new ZSK will be generated and the old key will be removed from the set of keys when the signature has expired.

The compromise will be notified through the channels indicated in section 2.1.

For the KSK
If a KSK is suspected of being compromised, a new key will be immediately generated and used in parallel with the old key. The old KSK will remain in place and will be used for the signature of all the keys all the time required to take into account the new key by all the validating resolvers and for a roll-over to be performed without any risk of resolution error.
The roll-over of the KSK will always be notified through the channels indicated in section 2.1.

In the case of loss of a KSK, the KSK will be changed with no overlap between the lost key and pre-published emergency key.
In this case, the information will be notified through the channels indicated in section 2.1.

The third parties using one of the Afnic KSK as trust anchors must add the emergency KSK provided for this purpose as a trust anchor. During this time, the set of keys will be fixed, no roll-over of the ZSK will occur as long as the KSK has not been replaced.

4.5.4. Business Continuity and IT Disaster Recovery Capabilities

Afnic has a BCP (Business Continuity Plan) that ensures the continuation of the critical services.
For this purpose, the back-up facilities are equivalent in terms of physical protection and logistics. The data is replicated in real time between the facilities.

The BCP and the recovery procedures are regularly tested and if necessary improved.

The BCP defines:

- the responsibilities for the activation of emergency recovery procedures,
- The operation of crisis management,
- The launch of backup operations.
- The appointment of a task manager.
- The requirements for a return to normal.

4.6.Entity termination

If for any reason, Afnic should disable DNSSEC for one of its zones and no longer signs the zone, this will be done in an orderly manner that includes providing information to the public.
If the operation of a zone must be transferred to a third party, Afnic will participate in this transition in order to make it as smooth as possible.

5.Technical security controls

5.1. Key Pair Generation and Installation

5.1.1. Key pair generation

Key generation is performed by a hardware security module (HSM) which is operated by skilled personnel, properly appointed for these trusted roles.
Key generation is done via open-DNSSEC commands. Their replication on pair boxes is done in the presence of two security officers, two operators, a key holder and a master of ceremonies. These people must be present throughout the operation.
The whole of the key generation process is traced by logs, some of which are recorded electronically and some are recorded on paper by the security officers.

5.1.2. Public key delivery

The public part of each KSK generated is recovered in the signature system and verified by the security officers and the operators.
The Security Officer is responsible for the publication of the public part of the KSK in a secure manner as defined in 2.1.
The system administrator verifies that the keys published are those that were generated.

5.1.3. Public key parameters generation and quality checking

The key parameters are defined by the Afnic key management and signing policy and the control includes checking the key length.

5.1.4. Key usage purposes

The keys generated for DNSSEC are never used for anything other than DNSSEC purposes nor are they used outside of the signature system.
Whether for the ZSK or the KSK, a signature produced with a DNSSEC key cannot have a service life longer than 2 months.

5.2.Private key protection and Cryptographic Module Engineering Controls

All the cryptographic operations are performed by the hardware security module and it is not possible to have private keys outside the module.

5.2.1. Cryptographic module standards and controls

The system uses a hardware security module (HSM) compliant with the requirements of FIPS 140-2 Level 4 (Federal Information Processing Standards: *Security Requirements for Cryptographic Modules*).

5.2.2. Private key (M -of-N) multi-person control

The Registry does not apply multi-person control to activate the module. The presence of the Security Officer is required to enable the security module, but physical access is operated by Systems Administrator who has sole authority.

5.2.3. Private key escrow

The Registry does not ecrow private keys.

5.2.4. Private key backup

The keys created are:

- Copied in encrypted format on the backup cards (SMK) specific to the HSM operated by Afnic.

  The following options are then possible:

  - the keys are copied in the BCP HSM from the backup cards which are then deleted,
  - the keys are copied in the BCP HSM from the backup cards which are then stored in a location that is accessible only to a Security Officer,

The keys are backed-up securely and synchronized after each key generation.

5.2.5. Private key storage on cryptographic module

Each module ensures the signature and automatic management of the keys.
As a result, the production keys are continuously present in each of the security modules, which contain the same information for redundancy purposes.
Each backup card can be used on each of the security modules.

5.2.6. Private key archival

The private keys that are no longer used are only archived as backup copies.

5.2.7. Private key transfer into or from a cryptographic module

Private keys are exchanged between the various modules using the backup and restore mechanism by the backup cards (SMK).

The backup cards are managed in accordance with the rules laid down in 5.2.4.

5.2.8. Method of activating private key

The private keys are automatically activated by the key management system.
Activation is performed according to the configuration set up by the Administrator of the signature system (see 4.2.1).

5.2.9. Method of deactivating private key

The HSM is automatically locked if the signature device is switched off or restarted.

5.2.10. Method of destroying private key

After their effective use, the private keys are deleted from the signature device.

5.3. Other Aspects of Key Pair Management

5.3.1. Public key archival

Public keys are archived in accordance with the archival of other information relating to the traceability of the system, such as log data.

5.3.2. Key usage period

A key pair becomes invalid when it is revoked and / or withdrawn from production.

5.4. Activation data

Activation data is the authentication code used by each security officer to activate the HSM.

5.4.1. Activation data generation and installation

Each Security Officer is responsible for creating his/her own authentication codes respecting the rule of a list of characters of a different nature.

5.4.2. Activation data protection

Each Security Officer is responsible for the protection of his/her activation data in the best practival way. If the activation data is suspected of having been compromising or lost, it is the responsibility of Security Officer to take immediate action to have it revoked and replaced.

5.4.3. Other aspects of activation data

A stamped, sealed envelope containing the activation data will be held in a safe place. It may only be used in an emergency according to a protocol applied by a security officer officiating as part of the Registry DNSSEC contingency plan.

5.5. Computer Security Controls

All the critical components of the Registry's systems are located in secure locations in accordance with Article 4.1. Access to the operating system for the servers is strictly limited to authorized personnel, i.e. the System Administrators.

All accesses are logged and traceable on an individual basis.

5.6. Network Security Controls

The registry has logically segmented its network into several secure zones securely interconnected. All access is through firewalls. All communications containing sensitive information are robustly encrypted.

5.7. Timestamping

The clocks of Registry's NTP servers are synchronized.

Timestamping is based on UTC time. It is recorded in the same format for all the log information as well for defining the signature validity periods.

5.8. Life Cycle Technical Controls

5.8.1. System development controls

All of the source code is retained in a version control system. The source code is regularly checked and copies are stored separately in a secure, fireproof location.

The developments made by Afnic are based on industry standards and include:

- Complete, documented functional specifications on security requirements,
- An ongoing commitment to reduce complexity,
- Systematic automated testing and regression tests,
- Provision of separate software versions,
- Ongoing monitoring of quality and correcting of any defects.

5.8.2. Security management controls

Records are kept of authorized personnel and monitored regularly.
Afnic carries out regular audits on the security of the signature device.
Afnic develops and maintains a "signature device security plan" based on a recurring risk analysis.

6. Zone Signing

6.1. Key lengths, keys types and algorithms

The Registry uses a split-key signing scheme in signing of the zone .CORSICA Key lengths and algorithms must be of sufficient length for use during their lifetime (2 years for the KSK, 3 months for the ZSK).
The algorithms must respond to the IETF standard, be public, and be efficient for all the parties concerned.
The RSA algorithm is currently used with a length of 2048 bits for the KSK and 1024 bits for the ZSK.

6.2. Authenticated denial of existence

The Registry uses NSEC3 records + Opt-out as specified in RFC 5155.

6.3. Signature Format

The signatures are generated by an RSA operation using a cryptographic hash function based on SHA2 (RSA/SHA-256, RFC 5702).

6.4. Key roll-over

A roll-over of the ZSK is performed every 60 days

The roll-over of the KSK is performed as needed (approximately once every two years).

6.5. Signature life-time and re-signing frequency

The zone is incrementally signed with each publication (see the frequency of publication announced by the Registry).
A complete "resignature" occurs at least once a week.

The signatures have a life span of 3 months.

6.6. Verification of zone signing key set

To ensure the validity of the keys and signatures, security checks are carried out with the DNSKEY before each publication of the zone information on the Internet.

6.7. Verification of resource records

Before any distribution, the Registry checks the Resource Records are valid in accordance with the currently applicable standards.

6.8. Resource records time-to-live

The time-to-live (TTL) for each DNSSEC Resource Record (RFC 4034) is specified as follows, in seconds :

RRtype	TTL
DNSKEY	172800
DS	172800
NSEC3	as SOA minimum (5400)
RRSIG	as RR (varies)

7.Compliance audit

To verify process integrity and to assess the security posture of the Registry System, .CORSICA conducts both internal and external audits.

The Compliance Audit is based on:

- documents (policies, procedures, requirements),
- information about the facts observed,
- any verifiable information that can be used to meet the criteria for the audit.

7.1. Frequency of entity compliance audit

Afnic may decide to launch an audit:

- in the case of recurrent anomalies,
- in the case of substantial changes to the organization, or in the management of the process.
- For any other reason related to the competence of the personnel involved, to changes in equipment or any other major change.

7.2.Identity/qualifications of auditor

The auditor must be an expert in computer security, the DNS and DNSSEC.

7.3.Auditor's relationship to audited party

Management of the audit is entrusted to an external manager. If necessary, the Manager hires an expert for the requirements of the audit. The Audit Manager is fully responsible for the conduct of the audit.

7.4. Topics covered by audit

The Audit Manager ensures that:

- s/he has contact with the competent Registry's authorities,
- The auditee is informed and is preparing for the audit,
- The auditee is notified in advance of the audit and informed of its scope,
- Procedures for monitoring the results of the audit have been set up.

7.5. Actions taken as a result of deficiency

The Audit Manager must immediately inform the Afnic management of any anomalies.

7.6. Communication of results

The Audit Manager must provide a written report containing all the results within 30 days after the end of the audit.

8. Legal matters

8.1. Costs of use

Afnic will not require its registrars to pay for the management of its DS publications.

8.2. Privacy of personal data

In accordance with the Naming Policy, all Personally Identifiable information treated under Afnic's responsibility are treated in accordance with Law No. 78-17 of 6 January 1978 on Data Processing, Files and Individual Liberties, known as the "Data Protection Act".

8.3. Limitation of Liability

In accordance with a Naming policy that is elaborated with the Registry Operator.

The procedures manual for the registration of domain names is available here: **https://www.afnic.fr/en/resources/reference/technical-guidebooks/gtld-6.html**

8.4. Duration and Termination

8.4.1. Period of validity

This DPS applies until further notice.

8.4.2. Period of validity

This DPS expires on publication of the next one (document revision).

8.5.Dispute resolution

Any conflict or dispute relating to this approval will be heard before the relevant Court for the .CORSICA.

8.5.1. Governing Law

This document is governed by French law.