DPS .paris

Domain signature policy and conditions of implementation

8 December 2023 – Version 1.6

www.afnic.paris | contact@afnic.paris
Twitter: @AFNIC | Facebook: afnic.paris

DOCUMENT IDENTIFICATION	
Title	DPS .paris
Hyperlink	dps-fr.pdf
Reference	DPS-FR-01
Version	1.6
Last updated on	8 december 2023

CLASSIFICATION			
Document manager	Vincent Levigneron		
Classification level (mark with an "X" under the required level)			
Public	Internal	Restricted	Confidential
X			

REVISION HISTORY			
Version	Author	Date	Nature of revision
V. 1	Alain Caristan, David Barou	March 2012	Creation
V. 1.2	Alain Caristan, David Barou	June 2013	Update to RFC 6841, January 2013
V. 1.3	Vincent Levigneron	March 2021	Update
V. 1.4	Vincent Levigneron	July 2021	Change of key algorithm
V. 1.5	Vincent Levigneron	March 2023	Adjustment of ceremony parameters, TTL
V. 1.6	Anthony Hubbard	December 2023	Adding section 7 “compliance audits”

APPROVED BY		
Date	Name	Position
January 2012	Alain Caristan,	CSO
11 June 2013	Philippe Renaut	CTO
11 May 2021	Régis Massé	CTO
27 July 2021	Régis Massé	CTO
27 March 2023	Régis Massé	CTO
December 2023	Anthony Hubbard	CSO

CONTENTS

1. Introduction

- This document is called the “DPS” (DNSSEC Practice Statement) for the .paris zone as it describes all the policies, procedures and tools used to sign the .paris zone thanks to DNS Security Extensions (DNSSEC), in accordance with the draft proposed by the IETF in the RFC-draft DNSSEC Policy & Practice Statement Framework.

- The Domain Name System (DNS) was not originally designed with security mechanisms. Over the years, a number of vulnerabilities have been discovered that threaten the reliability and trustworthiness of the system.

- DNS Security Extensions address these vulnerabilities by using public key cryptography to add data origin authentication, data integrity verification, and authenticated denial-of-existence capabilities to the DNS.

- This document specifies the conditions under which DNSSEC are produced and deployed in the .paris zone, thus enabling all users to assess the level of security of the chain of trust in this zone. 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 authentication of origin and data integrity to the Domain Name System. DNSSEC provides a way for software to validate that Domain Name System (DNS) have not been tampered with or modified during Internet transit. This is done by incorporating public key cryptography into the DNS hierarchy to form, though the set of signatures in the respective parent zones, a chain of trust originating in the root.

Eight main components are described in this document:

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. Document name and identification

Document title: DPS .paris
Version: v1.6
Created: 1 January 2012

1.3. Community and applicability

The following roles and responsibilities have been identified.

1.3.1. Registry

City of Paris is responsible for the management of the .paris zone. The City of Paris delegates the technical management of the TLD to Afnic which manages and upgrades the technical infrastructure ensuring the performance and resilience of the .paris zone at its level.

Similarly, Afnic manages the keys for cryptographically signing registrations in the .paris zone in accordance with the methods and procedures described below.

Afnic undertakes to regularly use its ZSK to sign the cryptographic summary of the KSKs of delegations signed under the .paris 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 a Registrant's domain names. It is responsible for the identification of these Registrant.

It is also responsible for adding, removing and updating Delegation Signer (DS) public keys at the request of the Registrant or the technical contact for the corresponding domain name.

1.3.3. Registrant and contacts

A domain name is created by the Registrant, who designates 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 records and manage their publications through their registrar's interfaces.

1.3.4. Relying parties

Parties involved in the deployment of DNSSEC from one end of the resolution chain to the other, for example the validation of signatures by resolvers and other applications. These parties are involved in the deployment of DNSSEC and the updating of keys. These parties must keep abreast of any updates by Afnic on its zones if the .paris key is used as a trust anchor. Otherwise, they must keep abreast of any updates of the DNS root keys.

1.3.5. Applicability

Each Registrant is responsible for determining the appropriate level of security for the domain names whose TLDs are managed by Afnic. This DPS is exclusively applicable to the .paris TLD and describes the procedures, security controls and practices applicable to the use and management of keys and signatures used for this TLD.

By drawing on this DPS, the various parties concerned can determine the level of trust that they attribute to the .paris domain managed by Afnic and deduce their own level of risk.

1.4. Specific Technical Administration

1.4.1. Specification technical administration organisation

Afnic

1.4.2. Contact Information

DNSSEC Policy Management Authority:

Immeuble "le Stephenson"

1, rue Stephenson
Hall A2 - 3ème étage
78180 Montigny-le-Bretonneux

Contact information
Afnic
support@afnic.paris

1.4.3. Specification change procedures

Afnic's DPS is reviewed on an annual basis or whenever there is a significant change in the system or in procedures having a significant impact on its content. This review is carried out by the Signing System Administrator (see 4.2.1).

Changes to the DPS are made 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 the following address:

https://bienvenue.paris/en/faq

Only the most recent version of the DPS is applicable.

2. Publication and Repositories

2.1. Publications on the Afnic website

The official electronic version of the DPS is published at:

https://bienvenue.paris/en/faq

2.2. Publication of public keys

Afnic publishes its KSKs in the form of a DNSKEY and DS.

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 email. Applications for registration under the .paris TLD are in accordance with a naming policy that is elaborated with the registry operator, available at this address:

https://bienvenue.paris/en/faq

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 .paris zone, which creates a chain of trust with the child zone. The registrar is responsible for transmitting the DS, while Afnic assumes that the DS record provided is correct.

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 the Registry.

3.4. Registration of delegation signer (DS) resource records

Afnic accepts applications for DS publication via the EPP interface and a web form secured by TLS. For EPP, 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 6 DS records can be published.

3.5. Method to prove possession of private key

The Registry uses the ZoneMaster test to verify correspondence of the key and correct configuration of the zone. The registrar is responsible for conducting such checks as it deems necessary to ensure the proper operation of the domain names it is responsible for registering.

3.6. Removal of DS resource records

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

3.6.1. Who can request removal

Only the registrar may give orders to remove DS records at the request of its client.

3.6.2. Procedure for removal request

The Registrant requests that the Registrar remove the DS record(s) from the .paris zone.

The Registrar executes the removal request in application of the procedures set out by Afnic.

In response to the removal request from the Registrar, Afnic deletes the DS record from the .paris zone.

The time required for the removal of a DS record from the .paris zone after receiving the removal request from the registrar depends on the update of the DNS programmed by Afnic. The maximum update time is 10 minutes.

4. Facility, management and operational controls

4.1. Physical Controls

Afnic has chosen to host its DNS infrastructure in data centres meeting the following requirements:

Double access security to the site with permanent guarding and patrols.

- A double check of the identity and access authorisation of each person working on the site is carried out on arrival and at the security post, manned 24 hours a day.
- An access system using individual badges and a 3-D biometric recognition system complete the procedure by restricting access to authorised 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 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 two metric tons.

Multi-building site interconnected by concrete tunnels.

4.1.1. Site location and construction

Afnic has set up its production infrastructures in two data centres geographically remote from the head office. These sites, operated by separate entities, comply with Tier 3 standards which guarantee a high degree of security and availability of the hosted systems. All the system components are protected in a physical perimeter with access control and an alarm system.

Afnic's business continuity plan conforms to 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 authorised personnel. Each data centre has a list (regularly updated with movements of personnel to Afnic) which contains all the persons authorised to access the facilities. The entrance is continuously monitored.

Afnic has a private room at the data centre sites, access to which is controlled by badge.

4.1.3. Power and air conditioning

Power is supplied to the operational facilities from several separate sources. In the event of outages, power is supplied by the emergency power systems in the data centre (Uptime Institute Tier 3 classification (based on ANSI standard ANSI/TIA-924). These systems can provide power for up to 72 hours.

4.1.4. Water exposures

The sites are in a zone not prone to flooding. The facilities are protected from flooding by:

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

4.1.5. Fire prevention and protection

The sites comply with the following industrial safety standards:

- A category A fire safety system;
- A nitrogen fire suppression system;
- Maintenance of the NFS 940 standard;
- Regular training of teams;
- Facilities for fire-fighter reception and response.

4.1.6. Waste disposal

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

4.1.7. Off-site backup

Afnic's data are automatically replicated at two remote sites.

4.2. Trusted roles

4.2.1. Trusted roles

Trusted roles are assigned to people with the ability to manage the contents of the zone file, i.e. the trust anchors. They are also capable (within the limits of the scope designated by this role) of producing and using cryptographic keys.

The trusted roles are:

Cryptographic Operators (2 out of 9)

- A designated operator performs all actions described in the procedures presented by the "Master of Ceremonies" on the HSMs (hardware security modules). A smart card is needed for authentication purposes on the HSMs.
- The main action of this role is activating/deactivating this equipment.

Security Officers (2 out of 4)

The Security Officers have access to the system configuration menus of the HSM (IP addressing, time setting, etc.). They set up the initial configuration of the HSM and should not have to intervene again once these have been put into service. As with the Cryptographic Operators, they need a smart card to validate access to these dedicated menus. The Security Officers are also Cryptographic Operators.

Cryptographic Officers (2 out of 4)

Cryptographic Officers have access to the various HSM menus for key operations (choice of algorithms, back-up/restoring of SMKs, deletion of application keys, etc.). They too need a smart card to access a number of specific menus. Cryptographic Officers intervene above all in procedures ("ceremonies") involving keys, performing various actions with the HSM under the control of the "Master of Ceremonies".

Key Holders (1 out of 5)

The application keys are stored on encrypted USB drives accessible by means of a specific access code. The Key Holders provide this access when the Cryptographic Officers need to make a transfer of application keys from the HSM to the USB drives (and vice versa). The Cryptographic Officers authorise the connection of these USB drives to the HSM.

Console Operators

They do not have access to the HSM, but manage the functioning of the applications and scripts needed for the smooth performance of the “ceremony”. They can connect to the various servers on which the key ceremonies are carried out and make any modifications that may be needed to the programs used (for example when changing algorithm, in accordance with the instructions given by the Signing System Administrator). They execute the commands depending on the scenario put in place by the “Master of Ceremonies”.

Signing System Administrator

Responsible for the configuration files and the various scripts of the signing solution. Also for keeping this document updated.

“Master of Ceremonies” (1 out of 3)

Prepares all the ceremonies by constructing a scenario based on Afnic procedures. Enables access to the safe and distributes all the cards and USB drives containing the application keys to the personnel involved in the ceremony. The safe also contains the physical key needed to activate the HSM used for key ceremonies. Responsible for stopping or continuing the ceremony in case of problems or unforeseen events. At the end of the ceremony, recovers all the elements and returns them to the safe.

4.2.2. Identification and authentication for each role

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

4.2.3. Tasks requiring separation of duties

A single person cannot simultaneously have more than one trusted role (Security Officer, Cryptographic Operator, Cryptographic Officer).

A Console Operator can be a Key Holder but may not occupy a role giving access to the HSM (Cryptographic Operator, Security Officer or Cryptographic Officer).

A Security Officer may be a Cryptographic Operator at the same time.

4.3. Personnel Controls

4.3.1. Qualifications, experience, and clearance requirements

Applicants wishing to perform 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 Afnic's HR department, which checks the background and qualifications of candidates, taking into account:

- Candidates' résumés
- Previous employment
- References
- Degrees/diplomas

To be eligible for one of the trusted roles, these controls must not reveal any unsuitability.

4.3.3. Training requirements

Afnic provides the necessary and relevant training on its procedures, administration and technical systems associated with each trusted role.

These training courses involve:

- Training on Afnic operations

- Training on 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

Personnel performing trusted roles must take these training courses and additional tests in the event 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 assigned, as far as possible, in turn to all the personnel with a trusted role.

4.3.6. Sanctions for unauthorised actions

The sanctions resulting from unauthorised actions are specified in the accountability agreement corresponding to the trusted role. Gross negligence may lead to dismissal and incur the liability of the person for any damage caused.

4.3.7. Contracting personnel requirements

In certain circumstances, Afnic 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.

Only qualified third parties may perform one of the trusted roles described in 4.2.1.

4.3.8. Documentation supplied to personnel

Afnic and its technical teams supply 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 continuous collection of information on the life of the Registry, forming an activity log.

This log is used to monitor operations for statistical purposes and for investigations in the event of suspected or confirmed breaches of Afnic policies and regulations.

The information in the log also includes reviews, lists and other paper documents vital for security and audit purposes.

The purpose of storing information in the log is to be able to reconstruct the sequence of events and analyse them to determine which people, applications or systems did what and when.

The log and the identification of users can be used to establish the traceability and monitoring of unauthorised uses.

4.4.1. Types of events recorded

The following events are included in the log:

- All activities involving the use of an HSM, such as key generation, key activation, as well as the signing and exporting of keys.
- Remote access attempts, both successful and unsuccessful
- Privileged operations
- Access to a facility.

4.4.2. Frequency of processing log

The log(s) is/are analysed continuously through automated and manual controls. Specific checks are conducted for the management of cryptographic keys, system reboots and detection of anomalies.

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

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

4.4.5. Audit log backup procedures

All electronic log information is securely backed up and stored separately of the system.

4.4.6. Audit collection system

All paper-based log information is scanned and stored electronically at at least two distinct sites remote from one another.

4.4.7. Notification to event-causing subject

Personnel causing an event to be logged are notified that such logging is taking place. Personnel are not authorised to review the log data.

4.4.8. Vulnerability assessments

All anomalies in the log information are investigated to analyse potential vulnerabilities.

4.5. Compromise and Disaster Recovery

4.5.1. Incident and compromise handling procedures

An incident is defined as:

- any real and perceived events of a security-critical nature that caused or could have caused an outage or damage to the information system,
- disruptions and/or defects due to incorrect information,
- any breach of security.

All incidents are handled in accordance with Afnic's procedures. The incident management procedure requires:

- investigating the causes of the incident,
- identifying the effects the incident has had or may have had,
- measures to prevent the incident from happening again, and
- documenting the information relating to incident management

An incident that involves suspicion that a private key has been compromised leads to the immediate rollover of keys pursuant to the procedures indicated 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 incident management procedures must be initiated and appropriate measures taken.

4.5.3. Entity private key compromise procedures

Upon the suspected or known compromise of a key, a new key will be generated in the following manner (in accordance with the procedures described in RFC 6781):

For the ZSK

If a zone signing key (ZSK) of having been compromised, it will immediately be removed from production and stopped being used. If necessary, a new ZSK will be generated and the zone immediately re-signed. The old key will be removed from the key set as soon as its signatures have expired.

Notification of this compromise will be sent through the channels indicated in section 2.1.

For the KSK

If a KSK is suspected of having been 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 to

sign key sets until such time as required for the new key to be taken into account by all the validating resolvers and for a rollover to be performed without any risk of resolution error.

The rollover of the KSK is notified through the channels indicated in section 2.1.

In the event of loss of a KSK, which is unlikely given the various safeguard mechanisms put in place, the KSK will be changed with no overlap between the lost key and the new key.

At this time, the information will be notified through the channels indicated in section 2.1.

Third parties using an Afnic KSK as a trust anchor must add the new KSK as a trust anchor. During this time, the key set will be fixed, no rollover of the ZSK will occur until the KSK has been replaced.

4.5.4. Business continuity and IT disaster recovery capabilities

Afnic has a BCP (Business Continuity Plan) designed to ensures the continuation of critical services.

To this end, the back-up facilities are equivalent in terms of physical protection and logistics. The data are replicated in real time between the facilities.

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

The BCP defines:

- who decides on the activation of an emergency recovery procedure,
- how and where crisis management shall convene,
- activation of backup operations,
- appointment of a Task Manager,
- criteria for restoring normal operations.

4.6. Entity termination

If, for any reason, Afnic must discontinue DNSSEC for one of its zones and return to an unsigned position, this will take place in an orderly manner in which the general public will be informed.

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) that is operated by trained and specifically appointed personnel in trusted roles.

Key generation takes place via open-DNSSEC commands. Their replication on the various HSM takes place in the presence of two Cryptographic Officers, two Cryptographic Operators, a Key Holder, a Console Operator and a Master of Ceremonies. These people must be present during the entire operation.

The entire key-generation procedure is logged, part of which is recorded electronically and part of which is recorded manually on paper by the Master of Ceremonies.

5.1.2. Public key delivery

The public component of each generated KSK is exported from the signing system and verified by the Cryptographic Officers and the Cryptographic Operators.

The Cryptographic Officer is responsible for publishing the public component of the KSK in a secure manner as per 2.1.

The Console Operator is responsible for ensuring that the keys that are published are the same as those that were generated.

5.1.3. Public key parameters generation and quality checking

Key parameters are regularly reviewed by Afnic's Key and Signature Management Policy and quality control includes checks of the key length.

5.1.4. Key usage purposes

Keys generated for DNSSEC are never used for any other purpose or outside the signing system.

Whether for the ZSK or the KSK, a signature produced with a DNSSEC key cannot have a service life longer than two months.

5.2. Private Key Protection and Cryptographic Module Engineering Controls

All cryptographic operations are performed by the hardware security module and it is not possible to use private keys outside this 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 under (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 activate the security module, but physical access is operated by the Systems Administrator who is the sole person authorised to do so.

5.2.3. Private key escrow

Afnic does not apply a key escrow.

5.2.4. Private key backup

The keys created are copied in encrypted format onto USB drives which are themselves encrypted (hardware encryption XTS-AES 256 bits, military class) before being stored in a safe.

5.2.5. Private key storage on cryptographic module

Each module ensures the signing and automatic management of 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 USB drive can be used on each of the security modules.

5.2.6. Private key archival

Private keys that are no longer used are archived solely in the form of backup copies.

5.2.7. Private key transfer into and from a cryptographic module

Private keys are distributed among the various HSMs during the key ceremony using an appropriate application (AEP load balancer), thus ensuring redundancy and continuity of service in the event that a HSM should break down or become temporarily unavailable (power or network outage, etc.).

5.2.8. Method of activating private key

Private keys are activated automatically by the key management tool (OpenDNSSEC in this case).

Activation is carried out in accordance with the configuration put in place by the Signing System Administrator (see 4.2.1).

5.2.9. Method of deactivating private key

The HSM is automatically locked if the signing system is turned off or rebooted.

5.2.10. Method of destroying private key

After their effective use, private keys are deleted from the signing system during the next key ceremony.

5.3. Other Aspects of Key Pair Management

5.3.1. Public key archival

Public keys are archived in accordance with the archiving of other information relating to traceability in 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 means 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 maximum differentiation of character sequences.

5.4.2. Activation data protection

Each Security Officer is responsible for the protection of his/her activation data in the best possible way. On suspicion of compromised activation data, the Security Officer must immediately change it.

5.4.3. Other aspects of activation data

A stamped, sealed envelope containing the activation data will be held in a secure location. It may only be used in an emergency according to a protocol applied by a Security Officer officiating in the context of Afnic's BCP on DNSSEC.

5.5. Computer security controls

The computers and servers involved in the delivery of the Registry services and their administration are protected by the following security measures:

- application of the least privilege
- remote access protected by dual authentication
- encryption of network flows
- logging and centralisation of security events generated on these components
- application of best practices in secured configuration
- regular security audits

5.6. Network security controls

The registry has logically segmented its network into several secure zones securely interconnected. Access is through firewalls. All sensitive information transferred is protected by strong encryption.

5.7. Timestamping

Synchronisation of server clocks is obtained on Afnic's NTP servers.

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

5.8. Life Cycle Technical Controls

All source code is stored in a source management system. Source code is regularly archived and copies are stored separately in a secure, fireproof location.

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

- functional specifications documenting security requirements in particular,
- an ongoing commitment to minimising complexity,
- automated systematic testing and regression tests,
- issuing of separate software versions,
- ongoing monitoring of quality and correction of detected defects.

6. Zone Signing

6.1. Key lengths, key types, and algorithms

Key lengths and algorithms must be of sufficient length for their designated purpose during each key's useful life (2 years for the KSK, 3 months for the ZSK).

Algorithms shall be standardised by the IETF, available to the public and resource efficient for all parties involved.

The algorithms currently in force at Afnic are ECDSA with a single key length of 512 bits for ZSK and KSK.

6.2. Authenticated denial of existence

The Registry uses NSEC3 records + Opt-outs as specified in RFC 5155, in accordance with the best practices described in RFC 9276.

6.3. Key rollover

The ZSK is automatically rolled every 60 days.

The KSK is automatically rolled every two years.

Other rollovers can be programmed in the case of specific maintenance operations such as a change of algorithm.

6.4. Signature life-time and re-signing frequency

The zone is incrementally signed with each publication (see the publication frequency announced by Afnic).

A complete re-signing takes place whenever a new key is introduced or the tag modified. During this operation, the life of the signatures is distributed uniformly so as to avoid them expiring on the same day.

The signatures have a maximum life of two months.

6.5. Verification of zone signing key set

To ensure the validity of the keys and signatures, security controls are conducted against the DNSKEY prior to publishing zone information on the Internet.

6.6. Verification of resource records

The Registry checks that all Resource Records (RR) are valid in accordance with the currently applicable standards prior to distribution.

6.7. Resource records time-to-live (TTL)

The time-to-live (TTL) for each RR (RFC 4034) is as follows, in seconds:

RRtype	TTL
DNSKEY	3600
DS	3600
NSEC3	Like minimum SOA (600)
RRSIG	as RR (variable)

7. Compliance Audits

The entity responsible for the technical management of the registry can conduct internal security audits at regular intervals.
These audits will be carried out by those responsible for the security of the registry and will focus more particularly on the main elements indicated in §1.1 of this document.
Corrective action taken further the audit will be recorded for follow-up purposes.

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 provisions of the Naming Charter, all personal data processed and for which Afnic is the data controller fall within the framework of the French Data Protection Act, or Act No. 78-17 of 6 January 1978.

8.3. Duration and Termination

8.3.1. Period of validity

This DPS will expire upon publication of the next version.

8.4. Dispute resolution

8.4.1. Governing Law

This document is governed by French law.