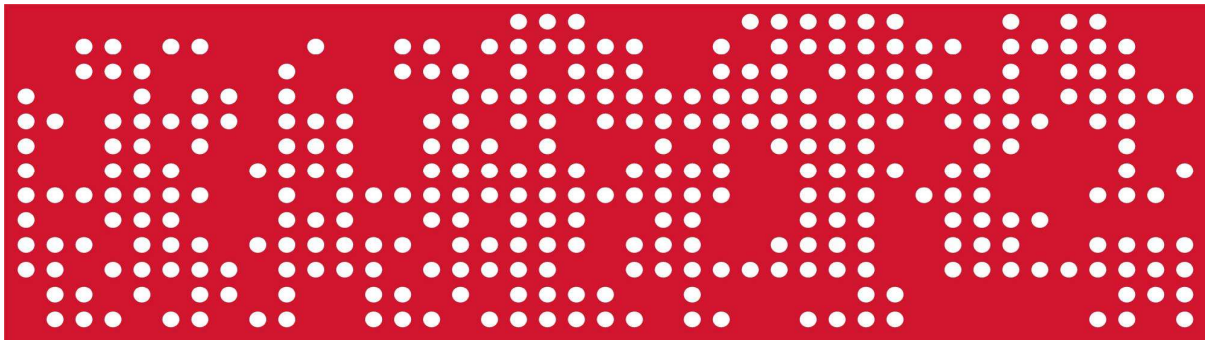
MINISTERIO
DE INDUSTRIA, ENERGÍA
Y TURISMO

red.es

DNSSEC Policy and Practice Statement for the ".ES" zone

Red.es



Version 1.1

MINISTERIO
DE INDUSTRIA, ENERGÍA
Y TURISMO

red.es

Document change control sheet

Created by	Red.es	**Date**	11/06/2014
Reviewed by		**Date**	
Approved by		**Date**	

Version control

Version	Date	Description
1.0	11/06/2014	First version of the document.

CONTENTS

1. INTRODUCTION

This document is the *Declaration of Policy and Procedures* ("*DPS*" -"*Policy and Practice Statement*") relating to *DNSSEC* on Red.es and in accordance with the indications of *RFC 6851* ("*A Framework for DNSSEC Policies and DNSSEC Practice Statements"*) by the *IETF*.

This document includes the policies and practices that *Red.es* uses in the "*.ES*" zone and the distribution services that include generating, managing, changing and publishing *DNS* keys.

1.1. SUMMARY

The Domain Name System (*DNS*) was not originally designed with security measures strong enough to guarantee data authenticity and integrity

Over the years, a series of vulnerabilities have been discovered, which are a security threat to traditional *Domain Name Systems*.

The *DNS* security extensions (*DNSSEC - Domain Name System Security Extensions*) are detailed in the following *RFCs (Requests for Comments) RFC4033, RFC4034, RFC4035,* which can be accessed via the organising body for the same, the *IETF (Internet Engineering Task Force* - http://www.ietf.org/)

These extensions, which resolve the security vulnerabilities using a cryptographic public key that verifies origin authentication of DNS data, authenticated denial of existence and data integrity.

1.2. DOCUMENT NAME AND IDENTIFICATION

- Document title:
  "*DNSSEC Policy and Practice Statement for the .ES zone*"

1.3. USE AND APPLICATION

This document can be used for the subsequently listed purposes. The relationship between the Register and accredited registrars is regulated in the accredited registrar contract, which can be found in full at:
http://www.dominios.es/dominios/sites/default/files/files/es_Contrato%20AR_20130906_con%20marca%20de%20agua%20(espa%C3%B1ol).pdf

1.3.1. Registration

Red.es is the organisation responsible for *ccTLD ".ES"* and managing the *".ES"* register*, and consequently managing the registration of the domain names identified in the .ES zone. This means that Red.es manages, adds, modifies and deletes all the data associated with a domain name. In Furthermore, it implies that Red.es manages and updates the technical infrastructure that ensures the performance and resilience in the .ES zone.*

Red.es is responsible for creating the cryptographic keys*, protecting the confidentiality of private keys, and signing the DNS registers for the .ES zone safely, using DNSSEC and the associated keys.*

In turn, *Red.es is* responsible for creating, exporting and maintaining the "*DS*" registers in a secure manner, so that they may be signed and published in the "*root*" zone. This completes the chain of trust.

1.3.2. Accredited Registrars

Accredited registrars are responsible for managing and administering the domain names and representing the register, according to the agreements established with the "*Register*" (*Red.es*).

They are responsible for the registration, maintenance and management process for the domains of "*Domain Name Holders*" who acquire their domain names through "*Accredited registrars*" who are accredited as *Red.es* collaborators.

Accredited registrars are responsible for establishing the mechanisms necessary to identify and authenticate the "*Domain Name Holders*", as well as for adding, deleting and updating specific DS registers for every domain name at the request of the holder.

1.3.3. Domain Name Holders

Natural or legal persons who acquire a domain name.

Domain name holders are responsible for creating and protecting their *DNSSEC* keys to sign off data in the zone, as well as for registering and maintaining the corresponding DS registers either directly or through an accredited registrar.

The holder is also responsible for changing the keys when there is any indication that they have been compromised or that the keys have been lost.

1.3.4. Application

Every Domain Name Holder is responsible for establishing a security level for their domain. This DPS only applies to first level .ES domains, and it describes the procedures, security controls and practices used to manage DNSSEC in the .ES zone.

1.4. ADMINISTRATIVE DATA

1.4.1. Organisation

Red.es is a public company reporting to the *Ministry of Industry, Energy and Tourism (MINETUR)*, responsible for managing domain names with the ".ES" country code.

1.4.2. Contact information

Public Corporate Entity Red.es – ".es" Domain Names

Edificio Bronce

Plaza Manuel Gomez Moreno, s/n

Madrid 28020

Email: info@dominios.es

Tel.: 902 010 755 (only for national calls)

Fax: (+34) 91 212 79 16

1.4.3. Procedure Changes

Any modification to this document will be notified via the official media channels of *Red.es*, and the latest official version will be saved in the Repository section.

The changes made to the *DPS* will be applied immediately following publication.

The latest version of the *DPS* published by the official media channels of *Red.es* is the only applicable version.

2. PUBLICATION AND REPOSITORY

2.1. Repository

Red.es will publish communications related to the *DNSSEC* on its official website. More specifically, the publications relating to the present *DPS* document will be published on the .es domain name website:

http://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/valores-anadidos/dnssec

2.2. Publishing the public signing keys

Red.es will publish the *Key Signing Keys* via the following mechanisms:

- The "*DS*" register will be published through the *root* zone.
- Via the official website *dominios.es*:

http://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/valores-anadidos/dnssec

2.3. Confidentiality

The following information shall remain confidential:

- Private components of the *Key signing* and *Zone Signing* keys.
- Public components of the *Key signing* and *Zone Signing* keys before the publication date (future keys).
- Identifying the people who will take part in the procedures for creating and signing the keys generated.

3. OPERATIONAL REQUIREMENTS

3.1. WHAT ARE DOMAIN NAMES?

A domain name is a unique identifier, normally associated with services such as web hosting and email addresses. For the purposes of this document, a domain name is a name registered with the .ES domain name, and it corresponds to the .ES zone, the server name operated by the domain name owner or the representative of the same.

3.2. DNSSEC ACTIVATION PROCESS FOR ".ES" DESIGNATED ZONES

DNSSEC for a delegated zone is activated by publishing a DS register signed for the zone. The inclusion of the same on the .ES register for the corresponding domain name establishes a chain of trust between the .ES zone and the delegated zone.

Red.es assumes that the "*DS*" registers provided are correct, and will not carry out checks or specific validations on said registers, except basic syntax tests. This means that Red.es will not verify whether a DNSSEC delegated zone has been validated by the corresponding DS register.

3.3. IDENTIFYING AND AUTHENTICATING THE DS REGISTER ISSUER IN THE ZONE TO BE SIGNED

"*Accredited registrars*" are responsible for guaranteeing that the data associated with the "*Domain Name Holders*" are true and correct, in accordance with the contract between Red.es and the Registry Operator.

Domain Name Holders who acquire a domain name directly via *Red.es* will be identified and authenticated directly by said organism, using the methods established by Red.es to manage the domains.

3.4. VALIDATING THE DS REGISTER IN THE ZONE TO BE SIGNED

Accredited registrars will provide the DS registers using the tools provided by Red.es.
Domain name holders operating directly through Red.es can include their DS register directly via the user interface, using the domain name management tool SGND.

3.5. METHODS FOR VALIDATING PROOF OF POSSESSION OF THE PRIVATE KEY

Red.es, will not carry out any checks on whether the owner has the private key. Accredited registrars are responsible for carrying out the necessary checks to ensure the domain names have been correctly loaded on the registry.

3.6. DELETING DS REGISTERS

A DS register can be deleted via the EPP interface, SOA or extranet by an accredited registrar or via the user interface by the Domain Name Holder. If all the DS registers in a specific zone are deleted, the DNSSEC validation for this zone will be disabled.

3.6.1. Who can ask for DS registers to be deleted in the ".ES" zone?

Only Domain Name Holders have the authority to ask for a DS register to be deleted via an accredited registrar or directly through the user interface.

Accredited registrars can only delete a DS register when acting on behalf of the holder.

3.6.2. How can I delete the DS registers for a domain?

The holder will order the accredited registrar to delete the registers, or will delete them directly from the user interface.

Changes to data associated with a domain will be reflected on the next generation of files for the zone, from the moment the request to delete the registers is received by Red.es.

3.6.3. Emergency procedure to delete DS registers

There is no emergency delete procedure.

4. INFRASTRUCTURE, ADMINISTRATION AND OPERATIONAL CONTROLS

4.1. PHYSICAL CHECKS

4.1.1. Physical Location and Checks

The *DNSSEC* services offered by *Red.es* are distributed across several data processing centres. This includes server centres, racks and a backup centre.

4.1.2. Physical Access

All of the locations have restricted access, limited to authorised staff only.

4.1.3. Power supply and air conditioning

The data processing centres owned by *Red.es* have unlimited power supplies (UPS) and a cooling system. All of the locations have backup systems in case of a power failure.

4.1.4. Flood protection

The data centres are reasonably protected against flooding and the facilities have flood detection systems.

4.1.5. Fire prevention and protection

All of our facilities have fire alarms and extinguishers.

4.1.6. Data storage

Data is stored in accordance with the Red.es quality management policy. Storage conditions depend on how the data is classified, particularly for sensitive data.

4.1.7. Offsite backup

All data is automatically backed up in a remote location.

4.2. AUDIT PROCEDURES

4.2.1. Types of Event Recorded

The following events are automatically recorded by the devices that are part of *DNSSEC*:

- All of the operations related to *HSM* such as creating, deleting, activating, signing and accessing keys.
- Remote Access that has been authorised or denied.
- Operations that require administrative privileges.
- Access to physical storage locations.

4.2.2. Log processing frequency

Logs are continuously analysed, both manually and automatically. Random inspections are carried out for actions such as key management, operations that require a higher level of clearance.

4.2.3. Retention period for audit events

The logged events are stored online for a period of at least 90 days. After this period of time they are stored on file for at least a year.

4.2.4. Security copy procedures for audit events

Data concerning audit information should be backed up with a security copy every month.

4.2.5. Compiling audit events

All of the information contained in the audit events should be compiled and processed in real time.

4.3. DATA COMPROMISE AND DISASTER RECOVERY

If the *Key signing* and *Zone Signing* keys are compromised, or in the case of a disaster, the emergency procedure will start to generate new keys.

All of the incidents will be managed based on the procedures defined by *Red.es.*

Red.es has set procedures for generating keys, publishing, zone signatures, rollovers, zone maintenance and for the physical equipment used for *DNSSEC* and *HSM*.

Red.es reserves the right to deactivate DNSSEC whenever there is a stability risk in the ".ES" zone.

The Spanish version of the present document will prevail, without prejudice to translations into other languages.

4.4. TERMINATION

If Red.es has to discontinue DNSSEC for the .es zone for any reason and return to an unsigned zone, this will be carried out in an orderly way following public notification.

If the operation of the .es register is transferred to a third party, Red.es will take part in the transition to make sure it runs as smoothly as possible.

5. TECHNICAL SECURITY MANAGEMENT

5.1. GENERATING AND INSTALLING KEY PAIRS

5.1.1. Generating Key Pairs

The key pairs used by the *DNSSEC* system are generated using the cryptographic *HSM* module from the *DNSSEC* settings using secure network protocols (*TLS*).

5.1.2. Distributing public keys

The public Key Signing Key is exported from the signature system as part of the key generation procedure. Once exported it is verified by RS and AD. The RS is in charge of publishing the key securely, as indicated in section 2.2. The AD is in charge of checking whether the published key is the same as the one that has been exported and programmed for use, and whether it is functioning as it should.

5.1.3. Parameters for generating and managing the quality of the public key.

The parameters for generating the keys are defined in the zone signature policy (see below) and as part of the quality controls included in key length verification.

5.1.4. Proposals for key use

A key generated for DNSSEC should only be used for DNSSEC activities and should never be used outside the signature system. A key should be used for a specific zone and should not be reused.

5.2. PROTECTING AND MANAGING PRIVATE KEYS

All the cryptographic operations are carried out within the HSM.

5.2.1. Checks and Standards for cryptographic modules

The HSM hardware has FIPS 140-2 level 2 certification.

5.2.2. Multi-staff use of Private Keys

A minimum of 2 to 5 people are required to activate an HSM module.

5.2.3. Storing Private keys

Private keys cannot be exported from the HSM.

5.2.4. Backup for Private Keys

Private keys are stored on two synchronised cryptographic devices and on the devices there is a security copy for this purpose.

The data on the cryptographic *HSM* module cannot be exported and therefore is only stored on the *HSM* modules for this purpose. However, there are additional cryptographic modules which are used exclusively for storing backup copies of the *HSM* data with security measures for access and data similar to those on the *HSM*.

5.2.5. Method for Activating Private Keys

The new private keys will be activated by the AD once they have been expressly authorised by the RS.

5.2.6. Method for Deactivating Private Keys

Private keys will not be destroyed at the end of their useful life. At the end of their useful life they will be deleted from the signature system.

5.3. OTHER ASPECTS RELATED TO KEY MANAGEMENT.

5.3.1. Public Key Archive

The public keys are backed up and archived as part of the Red.es backup system.

5.3.2. Duration of Key Use

Red.es will change the Key Signing Key when it deems it necessary. The Zone Signing Key will be changed every 90 days.

5.4. COMPUTER SECURITY CONTROLS.

Access to the computers and systems is registered on a log. Staff accessing these computers have to use individual user identification.

5.5. NETWORK SECURITY CONTROLS

The *DNSSEC* system used for the "*.ES*" environment is the only system that has access over the network to the *HSM* cryptographic modules.

5.6. SYNCHRONISATION OF TIME/HOUR

The computers/systems used for *DNSSEC* are synchronised periodically via *NTP services*.

5.7. TECHNICAL CONTROLS IN THE LIFE CYCLE

Red.es maintains a constant monitoring system and will run verification procedures on the data prior to the publication of the data for the ".*ES*" zone in order to validate the data published.

6. SIGNATURE FOR THE ".ES" ZONE

The signature for the ".*ES*" zone will be used with the specific parameters mentioned below.

Any change to the same should be reflected in the present document and will be published in accordance with section 2.1. Repository.

6.1. VALIDITY PERIOD FOR KEYS AND ALGORITHMS

- Key Signing Key: 2048 bits, RSASHA256 (algorithm number 8).
- Zone Signing Key: 1024 bits, RSASHA256 (algorithm number 8).

6.2. DENIAL OF AUTHENTICATED EXISTENCE.

The register will use NSEC3 with an opt-out (RFC 5155)

6.3. SIGNATURE FORMAT

The signatures will use RSASHA256 (algorithm number 8).

6.4. ROLLOVER OF THE ZONE SIGNING KEY.

Every Zone Signing Key will be active for 3 months.

6.5. ROLLOVER OF THE KEY SIGNING KEY.

If there is a normal rollover, the key will be published 3 months before it is activated, and will be maintained for 3 months after it has been deactivated. Key duration will be determined by the criteria Red.es considers necessary.

An automatic rollover process will be used, in accordance with RFC 5011.

6.6. SIGNATURE LIFE CYCLE AND RE-SIGNING FREQUENCY.

Zone Signing Key signatures are valid for 14 days and are resigned in every new zone.

6.7. TIME-TO-LIVE OF RRS.

The TTL of the DNSKEY is around 3,600 seconds.