DNSSEC Practice Statement (DPS)

for .LAT TLD

NIC Mexico Ave Eugenio Garza Sada 427 Loc. 4, 5 y 6 - C. P. 64840 – Monterrey, NL, Mexico

Table of Contents

1. Introduction

NIC Mexico has been selected by eCOM-LAC as the backend registry services provider for the .LAT new gTLD. This document is NIC Mexico's DNSSEC Practice Statement (DPS) for the LAT zone. It describes the practices and provisions that NIC Mexico applies in the LAT Top Level Domain DNSSEC operations.

1.1. Overview

DNSSEC is a protocol modification to the original DNS specification that enable origin authentication of DNS data and allow DNS software to verity that the data have not been modified during transit. DNS data is verified using what is called chain of trust that originates in the root. DNSSEC uses public key cryptography to secure DNS data and to validate the chain of trust.

1.2. Community and applicability

1.2.1. Registry Operator

eCOM-LAC is the Registry Operator for .LAT TLD. eCOM-LAC is the Latin America and Caribbean Federation of Internet and Electronic Commerce. It's a non-profit regional entity, which congregates non-profit industry associations, chambers of commerce and corporations, interested in contributing to the development of the Internet and Electronic Commerce in Latin America.

1.2.2. Registry Services Provider

NIC Mexico is the Registry Services Provider (RSP) for LAT TLD.
The RSP is responsible for:

Generation of ZSK and KSK used in .LAT zone and the protection of the private component of the keys.

Signing all authoritative DNS Resource Records in the .LAT zone.

Transmitting the necessary DS Resource Record to the root zone operator.

1.2.3. Registrars

Registrars make Registry Services available to the public. As they maintain direct contact with the registrants, they are responsible for most of the DNSSEC functions
Registrars are responsible of:

Implementing DNSSEC-compliant name servers

Creating private/public key pairs for the domain names
Creating and signing the zone,

Key management

- Handle key rollovers (scheduled and emergency) for ZSKs and KSKs
- Perform scheduled resigning of security-related resource records
- Update the parent zone with delegation signer (DS) records based on the KSKs

1.3. Specification administration

This DPS will be reviewed each six months following NIC Mexico's standard process management procedures. It will be updated as appropriate, such as in the event of significant modifications in system or procedures that affect it.

1.3.1. Specification administration organization

NIC Mexico
Av. Eugenio Garza Sada #427 L456 Col. Altavista
Monterrey, NL. C.P. 64840
MX

1.3.2. Contact information

NIC Mexico DNSSEC Policy Management Authority
Av. Eugenio Garza Sada #427 L456 Col. Altavista
Monterrey, NL. C.P. 64840
MX
Telephone: +52 81 83875346
Fax: +52 81 83875346 x 8111
dnssec@nic.mx

1.3.3. Specification change procedures

Only the most recent version of this DPS is applicable.
The most recent version is published at
http://nic.lat/politicas/DNSSEC-Practice-Statement-LAT.pdf.
NIC Mexico reserves the right to modify this DPS as appropriate.
This DPS and newer versions are effective upon publication.

2. Publication and repositories

The following section specifies the relevant repositories for LAT DNSSEC related information.

2.1. Repositories

NIC Mexico publishes the most recent version of this DPS at:
http://nic.lat/politicas/DNSSEC-Practice-Statement-LAT.pdf.

2.2. Publication of key signing keys

NIC Mexico publishes the public portion of the KSK in the root zone.

2.3. Access controls on repositories

Information published at http://nic.lat/politicas/DNSSEC-Practice-Statement-LAT.pdf is available to the general public and it is protected against unauthorized reproduction, deletion or modification by unauthorized parties.

3. Operational requirements

The following section lists the operational requirements.

3.1. Meaning of domain names

DNSSEC provides origin authentication of DNS data. DNSSEC does NOT provide a mechanism to determine the legal entity behind the domain name.

3.2. Activation of DNSSEC for child zone

DNSSEC for a child zone is activated when a signed DS record is published in the LAT zone for that child zone. The signed DS record allows the creation of a chain of trust from LAT zone to the child zone.

3.3. Identification and authentication of child zone manager

The Registry Operator through the RSP only creates and modifies objects when a Registrar sends the appropriate credentials and transaction commands. Neither the RSP nor the Registry Operator performs any verification of the identity or authority of the child zone manager. This is within Registrar's responsibility.

3.4. Registration of delegation signer (DS) records

The Registry Operator through the RSP only creates and modifies objects when a Registrar sends the appropriate credentials and transaction commands. The registrar requests the registration of DS Record on behalf of the registrant. The Registry Operator accepts the registration of DS records trough EPP using RFC5910 and a WEB interface. Up to four DS records can be registered per domain name.

3.5. Removal of DS Record

The removal of all DS records from a domain name deactivates DNSSEC for the child zone. The RSP accepts the removal of DS records trough EPP using RFC5910 and a WEB interface.

3.5.1. Who can request removal

The RSP only creates and modifies objects when a Registrar sends the appropriate credentials and transaction commands. The registrar requests the removal of DS Record on behalf of the registrant.

4. Management, operational and physical control

The following section list the management, operational and physical control.

4.1. Physical controls

NIC Mexico's physical policies and controls comply with the requirements specified in this DPS.

4.1.1. Site location and construction

NIC Mexico's operations are conducted in two geographically dispersed datacenters. NIC Mexico use 1+1 redundancy in all the components of its infrastructure. The main datacenter has a Level 5 certification from ICREA (International Computer Room Expert Association) and the backup datacenter has a Level 3 certification from ICREA.

4.1.2. Physical Access

The facilities operators' implement the sufficient controls to protect the facility and access is limited to authorized personnel only. NIC Mexico space in the datacenter is protected by two factor authentication mechanism and entry requires a biometric authentication (fingerprint) and proximity token. Entry is logged and security cameras inside the datacenter allow the continuous monitoring of NIC Mexico equipment.

4.1.3. Power and air conditioning

Both facilities are equipped with primary and backup systems for power and environmental control (temperature and humidity).

4.1.4. Water exposure

The facilities have flooding protection, control and detection mechanisms.

4.1.5. Fire prevention and protection

The facilities operators have implemented fire detection and extinguishing systems. The systems use chemical elements that are not harmful to human beings.

4.1.6. Media storage

All media is stored within NIC Mexico's facilities. Physical and logical controls have been implemented to limit access to the media to authorized personnel only. On-site backups are stored in UL Class 125 3-hour compliant data safes.

4.1.7. Waste disposal

All media that is discarded is destroyed in a secure manner, physical documents are shredded, magnetic media goes to degaussing process and any other kind of media is destroyed by a contracted party.

4.1.8. Offsite backup

Each backup cycle two set of tapes are generated. One set remains in NIC Mexico custody and the second set is stored by a third-party. Before leaving NIC Mexico's facilities the backup set is

encrypted. The encrypted encryption key is stored in each backup set and only NIC Mexico authorized personnel have access to the encryption secret.

4.2. Procedural Controls

The following section describes the procedural controls.

4.2.1. Trusted roles

The defined trusted roles are:

Security Officer, SecOff

System Administrator, SysAdmin

Physical Security Officer, PhyOff

The following activities are performed by persons that have one of the previous roles assigned to them:

Generation, protection and use of the private component of the keys.

Export of the public components of the keys.

Signing of zone data.

4.2.2. Number of persons required per task

NIC Mexico has implemented the necessary controls to segregate the responsibilities and privileges held by the personnel.

The following tasks require that at least two persons that held one of the SecOff and SysAdmin roles to be present:

Hardware Security Module activation.

Private component of keys generation.

The export of public components of the keys.

The persons with physical access to the HSM hold the PhyOff role. The person with the PhyOff role verifies the identity of the persons that held the SecOff and SysAdmin role.

4.2.3. Identification and authorization of people for each role

NIC Mexico's employees can held the PhyOff, SecOff and SysAdmin role. NIC Mexico's Human Resource Department performs an exhaustive background check of each person before they become NIC Mexico's employees.

Refer to 4.3 to a detail explanation of the controls used to verify identity.

4.2.4. Separation of duties

The roles mentioned in 4.2.1 are not held simultaneously by the same NIC Mexico employee.

4.3. Personnel controls

The following section lists the personnel controls.

4.3.1. Background and qualifications

NIC Mexico's employees that assume any of the roles mentioned in 4.2.1 must comply with the training requirements mentioned in 4.3.3.

4.3.2. Background control procedures

NIC Mexico's Human Resource Department performs an exhaustive background check of each person before they become NIC Mexico's employees. The following requisites must be cleared before a person became a NIC Mexico employee:

Provide Personal and Business References.

HR will perform a background verification to validate if the aspiring employee has a criminal record, or if he or she is subject of a criminal investigation, or if the references confirm its affirmations regarding previous employments or if he or she has undisclosed previous employments.

Go through psychometric tests.

4.3.3. Training requirements

NIC Mexico provides its personnel with training.

NIC Mexico training programs are designed for each role the person must perform. Any NIC Mexico employee that will perform one of the roles mentioned in 4.2.1 must complete before assuming its role the following internal courses:

- Basic DNS
- Advanced DNS
- DNSSEC
    - Security and operational procedures
    - Incident management procedures
- Disaster recovery procedures

4.3.4. Retraining frequency and requirements

NIC Mexico retrains its personal to ensure that they maintain the required level of proficiency to perform their job responsibilities.

4.3.5. Work rotation frequency and sequence

NIC Mexico rotates and replaces its personnel as needed.

4.3.6. Sanctions for unauthorized actions

Violations by NIC Mexico personnel of this DPS or other NIC Mexico's policies results in the appropriate disciplinary actions and this can include the job termination.

4.3.7. Contracting personnel requirements

Only NIC Mexico's employees can hold the roles listed in 4.2.1 and perform the activities listed in 4.2.2.

4.3.8. Documentation supplied to personnel

NIC Mexico provides the necessary documentation to their personnel in order to perform their job responsibilities. This documentation must be returned to NIC Mexico in order to be securely destroyed.

4.4. Audit logging procedures

The following section lists the audit logging procedures.

4.4.1. Events that are logged

The following events are included in the logging:

Access to any of the system administration gateways.
Operations that requires privilege escalation.

Entries to the facilities and headquarters.
All operations performed in the HSM.

Access to the VPN concentrators that allow access to the NIC Mexico internal network.
Modifications to SRS objects.

The logs contain the date and information of the logged event.

4.4.2. Frequency of control of log information

The operators group (7x24) of NIC Mexico continually analyzes with automated and manual tools the logging information to detect anomalies.

4.4.3. Retention period for log information

Log information is stored at last for 30 days in the online backup servers. Logs of the last 30 days are stored in backup tapes every day.
A monthly tape backup is stored for at least ten years in a remote facility.

All tape backups that leave the facilities are encrypted. The backup encryption key is stored encrypted in each tape. Only NIC Mexico personnel have access to the secret of the backup encryption key.

4.4.4. Protection of log information

Logs are sent to the online backup servers in almost real-time. The online backup servers synchronize their information in almost real-time between the main and backup datacenter.

4.4.5. Audit log backup procedures

Log information is stored at last for 30 days in the online backup servers. Logs of the last 30 days are stored in backup tapes every day.
A monthly tape backup is stored for at least ten years in a remote facility.

All tape backups that leave the facilities are encrypted. The backup encryption key is stored encrypted in each tape. Only NIC Mexico personnel have access to the secret of the backup encryption key.

4.4.6. Audit collection system

Applications, RDBMS, HSM, network devices and operating systems generate audit data automatically that is transferred in almost real-time to the online backup servers. Manual logs are recorded on paper, scanned, and transferred to the online backup servers.

Log information is stored at last for 30 days in the online backup servers. Logs of the last 30 days are stored in backup tapes every day.
A monthly tape backup is stored for at least ten years in a remote facility.

All tape backups that leave the facilities are encrypted. The backup encryption key is stored encrypted in each tape. Only NIC Mexico personnel have access to the secret of the backup encryption key.

4.4.7. Notification to event-causing subject

No personnel need to be informed that logging is taking place. No personnel are entitled to request to view log data.

4.4.8. Vulnerability assessments

All anomalies detected by the operators group are investigated, If a vulnerability is detected the required actions take place to resolve the problem.

4.5. Compromise and disaster recovery

The following section describes the compromise and disaster recovery.

4.5.1. Incident management

Incidents are critical security related events that require that the incident management procedures are used.
Incidents are handled using NIC Mexico's incident management procedures.

NIC Mexico's incident management procedures are designed to investigate, control, learn and prevent future events from recurring.

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

The corruption of computing resources, software, and/or data triggers the use of NIC Mexico's management procedures.

4.5.3. Private Key compromise procedures

The following section describes the procedures when a private key is compromised.

4.5.3.1. KSK compromise

A KSK compromise triggers the use of the incident management procedures.

In case of a KSK compromise, a new KSK will be generated and use immediately. NIC Mexico will contact IANA in order to update the DS information for .LAT in the root zone. The compromised KSK will remain in production until it's safe to remove it.

4.5.3.2. ZSK compromise

A ZSK compromise triggers the use of the incident management procedures.

In case of a ZSK compromise, a new ZSK will be generated immediately and added to the keyset. The old ZSK will be removed from the keyset as soon as its signatures have been expired or time out.

4.5.4. Business Continuity

NIC Mexico continuously tests its business continuity plan.

The main and backup datacenters located in Monterrey, MX are synchronized in almost real time. The production datacenter can be switch between the main and backup datacenter in four hours. At least twice year the active datacenter is switched to the backup datacenter and used as the active datacenter for at least a week.

Daily full backups are stored in a remote facility in case the datacenter must be reconstructed from scratch. NIC Mexico has a third datacenter in Dallas, US that can be used as the active datacenter in case of a major disaster.

All business operations can be done remotely and NIC Mexico personnel have portable equipment in order to work if headquarters are unavailable.

The facilities operators have implemented fire detection and extinguishing systems. The systems use chemical elements that are not harmful to human beings.

4.5.5. Entity termination

In case NIC Mexico needs to transition the registry operator function for .LAT to another entity it will coordinate with it to transition the DNSSEC responsibilities.

5. Technical security controls

The following section describes the technical security controls.

5.1. Key pair generation and installation

The following section describes key pair generation and installation.

5.1.1. Generation of key pairs

An HSM is used for key generation and it takes place in the hardware module.

Key generation ceremonies for KSK and ZSK take place in accordance with NIC Mexico procedures. The entire key-generation ceremony is logged and records are written on paper by the SecOff.

The key-generation ceremony stipulates that at least a SecOff and a SysAdmin must be present and supply their security tokens in a secure entry device for key generation. The PhyOff have under his control the secure entry device and he review that the personnel requesting access have assigned the SecOff or SysAdmin roles, and that at least one person of each role is present.

5.1.2. Public key distribution

The public component of the ZSK and KSK is exported from the HSM and verified by the SecOff.

5.1.3. Quality control of key parameters

The SecOff verifies the key length before it is in the signing system.

5.1.4. Key usage purposes

Any generated KSK or ZSK is only used for DNSSEC of the zone .LAT TLD.

All signatures in the .LAT zone have a validity period of no more than nine days (seven days plus a random 48 hours jitter).

5.2. Private Key protection and cryptographic modules engineering controls

All cryptographic functions that require the private component of the KSK or ZSK are performed in the HSM.

5.2.1. Cryptographic module standards and controls

The HSM is FIPS 140-2 level 3 certified.

5.2.2. Private Key (m-of-n) multi-person control

In order to activate the HSM a person with the SecOff role is required to use its security token and the PhyOff must allow the access to the secure entry device.

5.2.3. Key escrow

Key escrow is not performed.

5.2.4. Private Key backup

NIC Mexico uses HSMs to perform private key backups. The backup procedure and HSMs used to perform the backups meet the requirements of this DPS.

5.2.5. Private Key storage on cryptographic module

Keys stored in the HSM are encrypted.

5.2.6. Private Key archival

The keys are maintained within the HSM and backup HSMs and are destroyed when the HSM is no longer used.

5.2.7. Private Key transfer into or from a cryptographic module

The keys are transferred between the master and secondary HSM and between the master and backup HSMs. The transferred is done in encrypted form.

5.2.8. Method of activating private key

During HSM activation the private key is activated. Refer to 5.2.2 to activation procedure.

5.2.9. Method for deactivation of private key

The keys are deactivated when the HSM is shutdown or rebooted.

5.2.10. Destruction of private keys

When the HSM is no longer in use the private keys stored in it is destroyed using the HSM function for this purpose. The destruction is logged.

Destruction of private keys can be done if required (for example if NIC Mexico will no longer be the backend registry services provider for .LAT).

5.3. Other aspects of key pair management

The following section describes other aspects of key pair management.

5.3.1. Public key archival

Public key components of the KSK and ZSK are stored in backups in the normal backup procedures of NIC Mexico.

5.3.2. Useful life of keys

During the process of key rollover a key can became obsolete and it's no longer reused.

5.4. Activation data

The activation data is the PIN for the security token that is assigned to the SecOff or SysAdmin roles, that is used for key generation and HSM activation.

5.4.1. Generation and installation of activation data

NIC Mexico personnel are responsible for establishing a secure PIN for its security token.

5.4.2. Protection of activation data

NIC Mexico personnel that receive a security token are responsible for protecting it.

In case that a security token is lost it will be immediately deleted as a privilege device in the HSM.

5.5. Computer security controls

The components of the SRS are placed in the main or backup datacenter of NIC Mexico.

Access to the RDBMS, operation system or network devices are logged and it's limited to IT personnel that require such access.

5.6. Network security controls

The network consists of different layers: Internet layer, security layer, application layer and internal layer. All access to the internal layer requires that the personnel access through a VPN using two factor authentication.

Internal and external firewalls are in place.

NIDS are in place in the external and internal network. All communication between the datacenters is encrypted.

5.7. Timestamping

NIC Mexico uses two NTP servers with the GPS as time source.

All logs are time stamped in CST.

5.8. Life cycle technical controls

The following section describes the life cycle technical controls.

5.8.1. System development controls

The software is developed in-house by NIC Mexico.

All source code is stored in control version repositories which are stored in backup in the normal backup procedures of NIC Mexico.

The development methodology is inspired in the Rational Unified Process.

5.8.2. System management controls

Security audits are done in regular basis.

5.8.3. Change management security controls

NIC Mexico change management is inspired in ITIL change management.

6. Zone signing

The following section describes zone signing.

6.1. Key lengths and algorithms

The following key lengths have been defined to prevent other from determining the private component with crypto analysis when the key is in use:

KSK, 2048.
ZSK, 1024.

6.2. Authenticated denial of existence

NIC Mexico uses NSEC3 records as specified in RFC155.

6.3. Signature format

RSA/SHA-256 is used as described in RFC5702 section 3.1.

6.4. Zone signing key roll-over

ZSK rollover is carried out quarterly.

6.5. Key signing key roll-over

KSK rollover is carried when needed.

6.6. Signature life-time and re-signing frequency

The validity period of the signatures is between seven and nine days. Resigning takes place every day or every 5 minutes if DNS updates are pending.

6.7. Verification of zone signing key set

NIC Mexico has implemented an automatically process that verifies the validity of signatures, keyset, and the chain of trust from the root to the .LAT TLD before publication. In case this process failed the zone won't be publish to the public DNS servers.

6.8. Verification of resource records

NIC Mexico has implemented an automatically process that verifies the validity of signatures, keyset, and the chain of trust from the root to the .lat TLD before publication. In case this process failed the zone won't be publish to the public DNS servers. .

6.9. Resource records time-to-live

All resource records in the zone have a TTL of 24 hours.

7. Compliance audit

Compliance audit for DNSSEC operations are performed by external entities.

7.1. Frequency of entity compliance audit

Audits are scheduled by NIC Mexico when necessary. An audit is triggered by the following circumstances:

Detected recurring anomalies by NIC Mexico personnel.

Changes in the Executive Committee, CIO or Deputy CIO of NIC Mexico.
Major changes in the DPS or operational procedures.

7.2. Qualifications of auditor

The compliance audit is performed by an external firm to NIC Mexico that demonstrates proficiency in DNSSEC, DNS and IT Security.

7.3. Auditor's relationship to audited party

The compliance audit is performed by an external firm to NIC Mexico. Personnel of NIC Mexico cannot participate in the auditor team.

7.4. Topics covered by the audit

The scope of the compliance audit includes all DNSSEC operations listed in this DPS.

7.5. Actions taken as result of deficiency

NIC Mexico management will review the auditor's report and take the appropriate actions to any significant nonconformity found.

7.6. Communication of results

The auditor must submit a written report to the Executive Committee, CIO and Deputy CIO of NIC Mexico not later than 30 calendar days after the audit was completed.

8. Legal matters

The following section describes the legal matters.

8.1. Fees

Not applicable.

8.2. Financial responsibility

Not applicable.

8.3. Privacy of personal information

NIC Mexico complies with the Mexican legislation “Ley de protección de datos personales en posesión de particulares” or Personal Data Protection Law.

eCOM-LAC complies with Legislation of The Oriental Republic of Uruguay regarding personal data protection.

8.4. Limitations of liability

Liability is regulated by the Registry Agreement and the Registrar Accreditation Agreement.

8.5. Term and termination

The following section describes the Term and termination of this DPS.

8.5.1. Validity period

This DPS becomes effective upon publication in http://nic.lat/politicas/DNSSEC-Practice-Statement-LAT.pdf.

8.5.2. Termination

This DPS will remain in force until it is replaced by a new version

8.5.3. Dispute resolution

Any dispute resulting from this DPS shall be filled in Montevideo, Oriental Republic of Uruguay.

8.5.4. Governing law

This DPS shall be governed by the laws of the Oriental Republic of Uruguay.