Table of Contents

1. Version	2010-11-16	8:30

1. Introduction

This document is the Certification Practice Statement (CPS) of Latin American and Caribbean Internet Address Registry (LACNIC). It describes the practices employed by the LACNIC Certification Authority (CA) in the Resource Public Key Infrastructure (RPKI). These practices are defined in accordance with the requirements of the Certificate Policy (CP, [RFCxxxx]) of this PKI.

The RPKI is designed to support validation of claims by current holders of Internet Number Resources (INRs, see definition in 1.7) in accordance with the records of the organizations that act as CAs in this PKI. The ability to verify such claims is essential to ensuring the unique, unambiguous distribution of these resources

This PKI parallels the existing INR distribution hierarchy. These resources are distributed by the Internet Assigned Numbers Authority (IANA) to the Regional Internet Registries. In some regions, National Internet Registries (NIRs) form a tier of the hierarchy below the RIRs for internet number resource (INR) distribution. ISPs and network subscribers form additional tiers below registries.

1.1. Overview

This CPS describes:

- Participants
- Publication of the certificates and CRLs
- How certificates are issued, managed, and revoked
- Facility management (physical security, personnel, audit, etc.)
- Key management
- Audit procedures
- Business and legal issues

This PKI encompasses several types of certificates (see IETF document draft-ietf-sidr-arch-xx [ARCH] for more details):

- CA certificates for each organization distributing INRs and for each subscriber (INR holder)
- End entity (EE) certificates for organizations to use to validate digital signatures on RPKI-signed objects (see definition in 1.7).
- In the future, the PKI also may include end entity certificates in support of access control for the repository system as described in 2.4.

1.2. Document name and identification

The name of this document is ''LACNIC's Certification Practice Statement for the Resource Public Key Infrastructure (RPKI)''.

1.3. PKI participants

Note: In a PKI, the term ''subscriber'' refers to an individual or organization that is a Subject of a certificate issued by a CA. The term is used in this fashion throughout this document, without qualification, and should not be confused with the networking use of the term to refer to an individual or organization that receives service from an ISP. In such cases the term ''network subscriber'' will be used. Also note that, for brevity, this document always refers to PKI participants as organizations or entities, even though some of them are individuals.

1.3.1. Certification authorities

The offline CA is the top level CA for the LACNIC portion of the RPKI. It provides a secure revocation and recovery capability in case the production CA is compromised or becomes unavailable. Thus the offline CA issues certificates only to instances of the production CA; and the CRLs it issues are used to revoke only certificates issued to the production CA. The production CA is used to issue RPKI certificates to LACNIC members, to whom INRs have been distributed.

1.3.2. Registration authorities

There is no registration authority (RA) for either the offline or the production CA operating under this CPS. The former needs no RA capability because it issues certificates only to the production CA. The production CA relies upon registry information hold by the LACNIC's Registry System to identify individuals authorized to requests certificates under the RPKI. LACNIC already establishes a business relationship with each subscriber (LACNIC member) and assumes responsibility for allocating and tracking the current allocation of INRs.

1.3.3. Subscribers

Two types of organizations receive distributions of IP addresses and AS numbers from this CA and thus are subscribers in the PKI sense: network subscribers and Internet Service Providers (ISPs). Additionally, this CA issues certificates to National Internet Registries, who, in turn, issue certificates to network subscribers or ISPs.

1.3.4. Relying parties

Entities or individuals that act in reliance on certificates or RPKI-signed objects issued under this PKI are relying parties. Relying parties may or may not be subscribers within this PKI. (See section 1.7 for the definition of an RPKI-signed object.)

1.3.5. Other participants

LACNIC will operate a repository that holds certificates, CRLs, and other RPKI-signed objects.

1.4. Certificate usage

1.4.1. Appropriate certificate uses

The certificates issued under this hierarchy are for authorization in support of validation of claims of current holdings of INRs.

Additional uses of the certificates, consistent with the basic goal cited above, are also permitted under the RPKI certificate policy.

Some of the certificates that may be issued under this PKI could be used to support operation of this infrastructure, e.g., access control for the repository system as described in 2.4. Such uses also are permitted under the RPKI certificate policy.

1.4.2. Prohibited certificate uses

Any uses other than those described in Section 1.4.1 are prohibited.

1.5. Policy administration

1.5.1. Organization administering the document

This CPS is administered by LACNIC.

1.5.2. Contact person

The RPKI CPS point of contact is the Chief Technology Office for LACNIC. He may be reached at Rambla Republica de Mexico 6125, C.P. 11400, Montevideo, Uruguay.

1.5.3. Person determining CPS suitability for the policy

Not applicable. Each organization issuing a certificate in this PKI is attesting to the distribution of INRs to the holder of the private key corresponding to the public key in the certificate. The issuing organizations are the same organizations as the ones that perform the distribution hence they are authoritative with respect to the accuracy of this binding.

1.5.4. CPS approval procedures

Not applicable. Each organization issuing a certificate in this PKI is attesting to the distribution of INRs to the holder of the private key corresponding to the public key in the certificate. The issuing organizations are the same organizations as the ones that perform the distribution hence they are authoritative with respect to the accuracy of this binding.

1.6. Definitions and acronyms

BPKI - Business PKI. A BPKI is an optional additional PKI used by an RIR to identify members to whom RPKI certificates can be issued.

CP - Certificate Policy. A CP is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements.

CPS - Certification Practice Statement. A CPS is a document that specifies the practices that a Certification Authority employs in issuing certificates.

Distribution of INRs - A process of distribution of the INRs along the respective number hierarchy. IANA distributes blocks of IP addresses and Autonomous System Numbers to the five Regional Internet Registries (RIRs). RIRs distribute smaller address blocks and Autonomous System Numbers to organizations within their service regions, who in turn distribute IP addresses to their customers.

IANA - Internet Assigned Numbers Authority. IANA is responsible for global coordination of the Internet Protocol addressing systems and Autonomous System (AS) numbers used for routing internet traffic. IANA distributes INRs to Regional Internet Registries (RIRs).

INRs - Internet Number Resources. INRs are number values for three protocol parameter sets, namely:

. IP Version 4 addresses,

. IP version 6 addresses, and

. Identifiers used in Internet inter-domain routing, currently Border Gateway Protocol-4 Autonomous System numbers.

ISP - Internet Service Provider. An ISP is an organization managing and selling Internet services to other organizations.

NIR - National Internet Registry. An NIR is an organization that manages the distribution of INRS for a portion of the geopolitical area covered by a Regional Registry. NIRs form an optional second tier in the tree scheme used to manage INR distribution.

RIR - Regional Internet Registry. An RIR is an organization that manages the distribution of INRs for a geopolitical area.

RPKI-signed object - An RPKI-signed object is a digitally signed data object (other than a certificate or CRL) declared to be such by a standards track RFC, and that can be validated using certificates issued under this PKI. The content and format of these data constructs depend on the context in which validation of claims of current holdings of INRs takes place.

Examples of these objects are repository manifests and CRLs.

2. Publication And Repository Responsibilities

2.1. Repositories

As per the CP, certificates, CRLs and RPKI-signed objects MUST be made available for downloading by all relying parties to enable them to validate this data.

The LACNIC RPKI CA will publish certificates, CRLs, and RPKI-signed objects via a repository that is accessible via RSYNC at rpki.lacnic.net.

2.2. Publication of certification information

LACNIC MUST publish certificates, CRLs, and RPKI-signed objects issued by it to a local repository system that it operates as part of a world-wide distributed system of repositories.

2.3. Time or Frequency of Publication

As per the CP, the following standards exist for publication times and frequency: A certificate will be published within 24 hours after issuance.

As per the CP, the following standard exists for publication times and frequency:

The LACNIC RPKI CA MUST publish its CRL prior to the nextScheduledUpdate value in the scheduled CRL previously issued by the CA.

2.4. Access controls on repositories

Access to the repository system, for modification of entries, must be controlled to prevent denial of service attacks. All data (certificates, CRLs and RPKI-signed objects) published to a repository are digitally signed. RPKI items that LACNIC

issues MUST be published to the repository that it runs by means not accessible to the outside world. Updates to the repository system must be validated to ensure that the data being added or replaced is authorized. This document does not define the means by which updates are verified, but use of the PKI itself to validate updates is anticipated.

3. Identification And Authentication

3.1. Naming

3.1.1. Types of names

The Subject of each certificate issued by this Registry is identified by an X.500 Distinguished Name (DN). The distinguished name will consist of a single Common Name (CN) attribute with a value generated by LACNIC. Optionally, the serialNumber attribute may be included along with the common name (to form a terminal relative distinguished name set), to distinguish among successive instances of certificates associated with the same entity.

3.1.2. Need for meaningful names

The Subject name in each subscriber certificate will be unique relative to all certificates issued by LACNIC. However, there is no guarantee that the subject name will be globally unique in this PKI. Also, the name of the subscriber needs not to be ''meaningful'' in the conventional, human-readable sense. The certificates issued under this PKI are used for authorization in support of applications that make use of attestations of Internet resource holding, not for identification.

3.1.3. Anonymity or pseudonymity of subscribers

Although Subject names in certificates issued by this registry need not be meaningful, and may appear ''random,'' anonymity is not a function of this PKI, and thus no explicit support for this feature is provided.

3.1.4. Rules for interpreting various name forms

None

3.1.5. Uniqueness of names

LACNIC certifies Subject names that are unique among the certificates that it issues. Although it is desirable that these Subject names be unique throughout the

PKI, to facilitate certificate path discovery, such uniqueness is neither mandated nor enforced through technical means.

3.1.6. Recognition, authentication, and role of trademarks

Because the Subject names are not intended to be meaningful, there is no provision to recognize or authenticate trademarks, service marks, etc.

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

For the CA of the subscribers of the LACNIC's RPKI it generates the key pairs for each of these CAs and thus assures that the private key is appropriate associated with the public key in the certificates issued by each of these CAs.

3.2.2. Authentication of organization identity

Certificates issued under this PKI do not attest to the organizational identity of subscribers, with the exception of registries. However, certificates are issued to subscribers in a fashion that preserves the accuracy of distributions as represented in LACNIC records.

To authenticate a certificate request LACNIC has a subscriber database that maintains the INR distribution records. The certificate request could be matched against the database record for the subscriber in question, and an RPKI certificate would be issued only if the INRs requested were a subset of those held by the subscriber.

3.2.3. Authentication of individual identity

Certificates issued under this PKI do not attest to the individual identity of a subscriber. However, LACNIC maintains contact information for each subscriber in support of certificate renewal, re-key, or revocation.

LACNIC has a database of individuals and logging-in credentials that are used to identify individuals that represent LACNIC members that are INRs holders.

3.2.4. Non-verified subscriber information

No non-verified subscriber data is included in certificates issued under this certificate policy except for SIA/AIA extensions.

3.2.5. Validation of authority

Only an individual to whom logging-in credentials have been issued and are authorized by the own organization that represent may request issuance of an RPKI certificate. Each certificate issuance request is verified using the LACNIC logging-in credentials.

3.2.6. Criteria for interoperation

The RPKI is neither intended nor designed to interoperate with any other PKI.

3.3. Identification and authentication for re-key requests

3.3.1. Identification and authentication for routine re-key

For hosted member CAs routine re-keys are automated by the software and thus no explicit authentication is required. A routine re-key is initiated whenever the current key for a hosted CA is older than 5 years.

The key roll over algorithm is described in [RFCrekey]

3.3.2. Identification and authentication for re-key after revocation

The old key can be revoked as the final steps in key roll over algorithm [RFCrekey], after a new key has been activated.

LACNIC RPKI can revoke old keys for specific hosted member CAs. Identification and authentication for these roles has been described in section 3.2.3

3.4. Identification and authentication for revocation request

For hosted member CAs it should be noted that user actions in the interface may result in revocation of EE certificates used for objects, such as ROAs, that should be invalidated.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who can submit a certificate application

Any subscriber who holds INRs distributed by this registry may submit a certificate application to this CA.

4.1.2. Enrollment process and responsibilities

LACNIC members who are resource holders are enrolled in the LACNIC logging-in system. Users identified as "administrative contact" can access LACNIC RPKI and request enrollment by generating a new CA certificate.

4.2. Certificate application processing

For the LACNIC RPKI a new, initial, CA certificate is requested by the system automatically when the authorized used user choses to opt-in.

4.2.1. Performing identification and authentication functions

LACNIC logging-in is used to identify a LACNIC member representative applying for a certificate.

4.2.2. Approval or rejection of certificate applications

The LACNIC RPKI will issue certificates to member CAs with a validity time to the end of the calendar year, plus a six months grace period to allow for renewal before the certificate expires. The production CA will include all INRs known for the member in the member CA certificate.

For hosted member CAs the system will automatically request renewal of the CA certificate listing all eligible resources, when new resources are received by the member and/or a new validity time is applicable.

4.2.3. Time to process certificate applications

LACNIC expects to issue a certificate attesting to a resource allocation within 1 business day after approval of the allocation.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

[OMITTED]

4.3.2. Notification to subscriber by the CA of issuance of certificate

When a new certificate is issued it appears in the user interface of LACNIC RPKI.

4.3.3. Notification of certificate issuance by the CA to other entities

[OMITTED]

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

A subject is deemed to have accepted a certificate issued by this CA unless the subject explicitly requests revocation of the certificate using the procedures described in Section 4.9.3.

4.4.2. Publication of the certificate by the CA

Certificates MUST be published in the RPKI distributed repository system via publication of the certificate at LACNIC repository publication. This will be done within one business day.

4.5. Key pair and certificate usage

A summary of the use model for the RPKI is provided below.

4.5.1. Subscriber private key and certificate usage

The certificates issued by LACNIC to subscribers are CA certificates. The private key associated with each of these certificates is used to sign subordinate (CA or EE) certificates and CRLs. A subscriber may in turn issue certificates to any organizations to which it distributes INRs and may issue one or more certificates for use in verifying signatures on RPKI-signed objects signed by the subscriber. Subscribers also will issue certificates to operators in support of repository access control.

4.5.2. Relying party public key and certificate usage

The primary relying parties in this PKI are organizations who will RPKI EE certificates to verify RPKI-signed objects. Repositories use operator certificates to verify the authorization of entities to engage in repository maintenance activities, and thus repositories represent a secondary type of relying party.

4.6. Certificate renewal

4.6.1. Circumstance for certificate renewal

As per the CP, a certificate MUST be processed for renewal based on its expiration date or a renewal request from the certificate Subject. The request may be implicit, a side effect of renewing its resource holding agreement, or may be explicit. If LACNIC initiates the renewal process based on the certificate expiration date, then LACNIC will notify the subscriber 6 months in advance of the expiration date, or the general policy, e.g., ''in conjunction. The validity interval of the new (renewed) certificate will overlap that of the previous certificate by 6 months, to ensure uninterrupted coverage.

Certificate renewal will incorporate the same public key as the previous certificate, unless the private key has been reported as compromised. If a new key pair is being used, the stipulations of Section 4.7 will apply.

4.6.2. Who may request renewal

The subscriber or LACNIC may initiate the renewal process. For the case of the certificate holder, only an individual to whom the LACNIC logging-in system identify as the right to use member may request renewal of an RPKI certificate.

4.6.3. Processing certificate renewal requests

The same stipulations listed in section 4.2.2 apply here.

4.6.4. Notification of new certificate issuance to subscriber

See 4.3.2

4.6.5. Conduct constituting acceptance of a renewal certificate

See 4.4.1.

4.6.6. Publication of the renewal certificate by the CA

LACNIC will publish a renewal certificate in the LACNIC RPKI repository within 1 business day after issuance of the renewed certificate.

4.6.7. Notification of certificate issuance by the CA to other entities

[OMITTED]

4.7. Certificate re-key

4.7.1. Circumstance for certificate re-key

As per the CP, re-key of a certificate will be performed only when required, based on:

(1) knowledge or suspicion of compromise or loss of the associated private key, or

(2) the expiration of the cryptographic lifetime of the associated key pair

If a certificate is revoked to replace the RFC 3779 extensions, the replacement certificate will incorporate the same public key, not a new key, unless the subscriber requests a re-key at the same time.

If the re-key is based on a suspected compromise, then the previous certificate will be revoked.

Section 5.6 of the Certificate Policy notes that when a CA signs a certificate, the signing key should have a validity period that exceeds the validity period of the certificate. This places additional constraints on when a CA should request a re-key.

4.7.2. Who may request certification of a new public key

Only the subscriber may request a re-key. In addition, LACNIC may initiate a re-key based on a verified compromise report. If the Subscriber (certificate Subject) requests the rekey, authentication is effected using LACNIC logging-in credentials.

4.7.3. Processing certificate re-keying requests

The same stipulations listed in section 4.2.2 apply here

4.7.4. Notification of new certificate issuance to subscriber

See 4.3.2..

4.7.5. Conduct constituting acceptance of a re-keyed certificate

A subject is deemed to have accepted a certificate issued by this CA unless the subject explicitly requests revocation of the certificate using the procedures described in Section 4.9.3.

4.7.6. Publication of the re-keyed certificate by the CA

A re-keyed certificate will be published in the Repository system within 1 business day of being issued by this CA.

4.7.7. Notification of certificate issuance by the CA to other entities

[OMITTED]

4.8. Certificate modification

4.8.1. Circumstance for certificate modification

As per the CP, modification of a certificate occurs to implement changes to the RFC 3779 extension values in a certificate. A subscriber can request a certificate modification when this information in a currently valid certificate has changed as a result of changes in the INR holdings of the subscriber.

If INRs are to be distributed to a subscriber and the INRs are in addition to a current distribution, and if the subscriber does not request that a new certificate be issued containing only these additional resources, then this is accomplished through a certificate modification. When a certificate modification is approved, a new certificate is issued. The new certificate will contain the same public key and the same expiration date as the original certificate, but with the incidental information corrected and/or the INR distribution expanded. When previously distributed INRs are to be removed from a certificate, then the old certificate MUST be revoked and a new certificate (reflecting the new distribution) issued.

4.8.2. Who may request certificate modification

The subscriber or LACNIC may initiate the certificate modification process in the user inteface of LACNIC RPKI by generating a new certificate. If a certificate holder requests the modification, the request is authenticated using the LACNIC logging-in credentials. Also, LACNIC will modify a certificate, and revoke the old certificate, if, for example, a Subscriber fails to renew membership in a timely fashion.

4.8.3. Processing certificate modification requests

A certificate can be modified (other than for re-key) only by the addition or removal or resources. A Subscriber requests certificate modification by submitting a Certificate Issuance Request. If the request contains values for AS and/or (IPv4 or IPv6) address resource sets that the Subscriber already holds, but which are different from those in the currently issued certificates, the request is interpreted as a request for certificate modification.

4.8.4. Notification of modified certificate issuance to subscriber

A Subscriber is notified of the issuance of a modified certificate by the publication of the certificate in the LACNIC RPKI repository system and by showing it in the user interface of the system.

4.8.5. Conduct constituting acceptance of modified certificate

When a modified certificate is issued, the LACNIC will publish in the repository and notify the subscriber. This will be done without subscriber review and acceptance.

4.8.6. Publication of the modified certificate by the CA

A re-keyed certificate will be published in the LACNIC RPKI Repository system within 1 business day of being issued by this CA.

4.8.7. Notification of certificate issuance by the CA to other entities

[OMITTED]

4.9. Certificate revocation and suspension

4.9.1. Circumstances for revocation

As per the CP, certificates can be revoked for several reasons. Either LACNIC or the subject may choose to end the relationship expressed in the certificate, thus creating cause to revoke the certificate. If one or more of the INRs bound to the public key in the certificate are no longer associated with the subject, that too constitutes a basis for revocation. A certificate also may be revoked due to loss or compromise of the private key corresponding to the public key in the certificate. Finally, a certificate may be revoked in order to invalidate data signed by the private key associated with that certificate.

4.9.2. Who can request revocation

The subscriber or LACNIC may request a revocation using the web interface of LACNICs RPKI system.

4.9.3. Procedure for revocation request

When one or more of the resources are no longer associated with a member LACNIC RPKI will:

- re-issue a new certificate, minus the lost resources, but maintaining all other properties
- publish the new certificate using the same publication point as before, thus replacing the old certificate

• revoke any non-expired certificates held by the member CA that lists the lost resources, thus invalidating any signed objects, such as ROAs that refer to these resources.

4.9.4. Revocation request grace period

A subscriber should request revocation as soon as possible after the need for revocation has been identified.

4.9.5. Time within which CA must process the revocation request

LACNIC will process a revocation request within 1 business day of receipt and validation of the request.

4.9.6. Revocation checking requirement for relying parties

As per the CP, a relying party is responsible for acquiring and checking the most recent, scheduled CRL from the issuer of the certificate, whenever the relying party validates a certificate.

4.9.7. CRL issuance frequency

The LACNIC RPKI CA production will publish a new CRL every 24 hours. The LACNIC RPKI offline CA will publish a new CRL on a monthly basis. Each CRL will carry a nextScheduledUpdate value and a new CRL will be published at or before that time. LACNIC will set the nextScheduledUpdate value when it issues a CRL, to signal when the next scheduled CRL will be issued.

4.9.8. Maximum latency for CRLs

A CRL will be published to the repository system within minimal latency after generation.

4.10. Certificate status services

LACNIC does not support OCSP or SCVP. LACNIC issues CRLs.

5. Facility, Management, and Operational Controls

5.1. Physical controls

5.1.1. Site location and construction

Operations for the LACNIC RPKI CA and RA are conducted within a physically protected area. This area serves a collocation data centre where LACNIC maintains their IT infrastructure. All the RPKI infrastructure (servers, cryptographic material and storage) is physically protected from access of unauthorized personnel.

The data centre address is v. das Nações Unidas, 11541, 7° andar 04578-000 - São Paulo – SP, Brazil.

5.2. Physical access

Access to the data centre is provided to all the tenants of the facility. LACNIC CA infrastructure is located in cages. These cages are only accessible to LACNIC's and NIC. BR (see 5.4.7 for more information) systems administrators.

5.2.1. Power and air conditioning

The LACNIC CA infrastructure is powered by a UPS (uninterruptible power supply) system. This system is capable of providing brief support for the CA system and the cryptographic module in the event of loss of municipal power. The data center containing this equipment makes use of HVAC (heating/ventilation/air conditioning) systems to control temperature and relative humidity. The data center also receives backup power supply by means of an external generator. This generator can give as much as 48 hours of autonomous power supply.

5.2.2. Water exposures

There is no history of flooding in this area of São Paulo that has reached the elevation of the level of the building.

5.2.3. Fire prevention and protection

The data center uses a fire prevention system that uses gas FM-200. The system starts automatically in case of fire.

5.2.4. Media storage

All media containing production software and data for the CA and RA functions, plus audit logs, are stored within the NIC.BR facilities. Data software on disk is backed up to separate disk drives daily. Incremental backup to tape is also performed daily. Access to the backup disks (and tapes) is restricted to staff who have been granted access to the machine rooms. Logical access control to the disk backup is done via user accounts restricted to staff members responsible for computer system operation.

5.2.5. Waste disposal

Sensitive documents and materials associated with operation of this CA are shredded before disposal. Data on the unusable computers is erased using a software package that overwrites the disk. Cryptographic devices are physically destroyed or zeroized in accordance the manufacturer's guidance prior to disposal.

5.2.6. Off-site backup

LACNIC performs continuous, offsite backups of critical system data, audit log data, and other information via network-accessible storage. Within 24 hours, all critical data will be sent to the online, offsite backup facility.

5.3. Procedural controls

5.3.1. Trusted roles

Two trusted roles are defined for managing the LACNIC RPKI CAs:

- CA administrator: has full access to the CA server and the associated cryptographic module.

- CA supervisor: has a limited access to the CA server to produce various reports.

5.3.2. Number of persons required per task

LACNIC assigns two individuals to each role, a primary and a backup. The primary role is performed by a member of LACNIC's staff and the backup role is performed by NIC.BR sttaf (see 5.4.7) There is no overlap among the individuals assigned to these roles, i.e., there are four distinct individuals staffing the two roles cited in 5.3.1. No single individual will fulfill the same role for both CAs.

5.3.3. Identification and authentication for each role

For the production CA, access is controlled via password-protected login over a SSH-protected connection via the LACNIC back-office LAN. This connection does not have direct access to the Internet.

The offline CA server is not connected to any network. The server is stored in a secure container. Only individuals filling the CA supervisor role have physical access to the server and cryptographic module for this CA. Only individuals filling the CA administrator role have logical access (password-protected login) to the CA server and cryptographic module.

5.3.4. Roles requiring separation of duties

The CA administrator and CA supervisor roles require separation of duties.

5.4. Personnel controls

5.4.1. Qualifications, experience, and clearance requirements

Only full-time LACNIC staff and full-time NIC.BR staff may fulfill the trusted roles described in 5.2.1. Staff members are assigned to the roles only if supervisory personnel deem them to be sufficiently trustworthy and only after they have undergone in-house training for the role.

5.4.2. Background check procedures

All LACNIC staff undergo normal employment reference checks.

5.4.3. Training requirements

LACNIC provides its CA staff with training upon assignment to a CA role as well as on-the-job training as needed to perform job responsibilities competently. LACNIC maintains records of such training and periodically reviews and enhances its training programs as necessary.

5.4.4. Retraining frequency and requirements

LACNIC provides refresher training and updates for CA personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently.

5.4.5. Job rotation frequency and sequence

There are no requirements for enforced job rotation among staff fulfilling trusted CA roles.

5.4.6. Sanctions for unauthorized actions

If LACNIC RPKI CA staff members are determined to have performed activities inconsistent with LACNIC RPKI policies and procedures, appropriate disciplinary actions will be taken.

5.4.7. Independent contractor requirements

LACNIC data center is located in the offices of NIC.BR. NIC.BR collaborates with LACNIC in several activities regarding the operation and maintenance of LACNIC IT infrastructure located in the Data Center of Sao Paolo. Same controls regarding to LACNIC staff are done to NIC.BR staff. No other independent contractor or consultant is used to perform LACNIC RPKI CA roles. Contractors who are needed to perform any maintenance functions on CA severs or cryptographic modules must be escorted and directly supervised by LACNIC staff at all times when in sensitive areas.

5.4.8. Documentation supplied to personnel

Training for staff assigned to a trusted CA role is primarily via mentoring. An internal wiki and document repository are maintained by LACNIC technical staff as a further training aid.

5.5. Audit logging procedures

5.5.1. Types of events recorded

Audit records will be generated for the basic operations of the certification authority computing equipment. Audit records will include the date, time, responsible user or process, and summary content data relating to the event. Auditable events include:

Access to CA computing equipment (e.g., logon, logout)

Messages received requesting CA actions (e.g., certificate requests, certificate revocation requests, compromise notifications)

Certificate creation, modification, revocation, or renewal actions

Posting of any material to a repository

Any attempts to change or delete audit data

5.5.2. Audit information media

Audit information will be recorded in electronic media where appropiate (system logs, etc.). Also paper records will be kept detailing access to the offline CA, including dates, hours and the corresponding signatures.

5.5.3. Frequency of log processing

Audit logs are examined on at least a weekly basis for significant security and operational events. In addition, LACNIC reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within LACNIC CA and RA systems.

5.5.4. Retention period for audit log

Audit logs are retained onsite for at least 6 months after processing.

5.5.5. Protection of audit log

No special, additional protection is afforded audit logs relative to other, sensitive CA data.

5.5.6. Audit log backup procedures

The offsite backup capabilities described in 5.1.8 apply to audit logs and extend the retention to 2 years.

5.5.7. Audit collection system (internal vs. external)

[OMITTED]

5.5.8. Notification to event-causing subject

[OMITTED]

5.5.9. Vulnerability assessments

No vulnerability assessment is done but there are plans to do it periodically.

5.6. Records archival

[OMITTED]

5.7. Key changeover

The LACNIC CA certificate will contain a validity period that is at least as long as that of any certificate being issued under that certificate. When LACNIC CA wishes to change keys, LACNIC will create a new signature key pair, and acquire and publish a new certificate containing the public key of the pair, a minimum of 1 week in advance of the schedule rekey in advance of the scheduled change of the current signature key pair.

5.8. Compromise and disaster recovery

[OMITTED]

5.9. CA or RA termination

LACNIC has been granted sole authority by IANA to manage allocation of IP address space and AS number resources in the Latin America and Caribbean region. LACNIC has established the RPKI for its region consistent with this authority. There are no provisions for termination and transition of the CA function to another entity.

6. Technical Security Controls

This section describes the security controls used by LACNIC

6.1. Key pair generation and installation

6.1.1. Key pair generation

For the production and CAs operated by LACNIC, key pairs are generated using a hardware cryptographic module. The module used for this purpose is certified as complying with FIPS 140-2 level 2. The hardware cryptographic module employed for this process is DEFINE.

LACNIC takes no responsibility for (and imposes no requirements upon) key pair generation performed by members who submit public keys for certificate issuance under the RPKI.

6.1.2. Private key delivery to subscriber

LACNIC does not generate key pairs for subscribers and thus makes no provisions for delivery of private keys.

6.1.3. Public key delivery to certificate issuer

LACNIC RPKI CA has direct access to the member public keys and no key delivery is involved.

6.1.4. CA public key delivery to relying parties

CA public keys for all entities (other than trust anchors) are contained in certificates issued by other CAs and MUST be published to the RPKI repository system. Relying parties MUST download these certificates from this system. Public

key values and associated data for (putative) trust anchors MUST be distributed out of band and accepted by relying parties on the basis of locally-defined criteria, e.g., embedded in path validation software that will be made available to the Internet community.

6.1.5. Key sizes

LACNIC CAs use an RSA key of 2048 bits. For NIR certificates signed by LACNIC, the RSA keys will be 2048 bits. For subscriber and ISP certificates, the RSA keys will be between 1024 and 2048 bits.

6.1.6. Public key parameters generation and quality checking

The public key algorithms and parameters used in this PKI are as specified in RFC ZZZZ [RFCzzzz].

6.1.7. Key usage purposes (as per X.509 v3 key usage field)

The Key usage extension bit values will be consistent with RFC 5280. For LACNIC's CA certificates, the keyCertSign and cRLSign bits will be set TRUE. All other bits (including digitalSignature) will be set FALSE, and the extension will be marked critical.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards and controls

The LACNIC CA employs a cryptographic module evaluated under FIPS 140-2/3, at level 3 [FIPS].

6.2.2. Private key (n out of m) multi-person control

Activation of the private key for offline CA requires two-party control. The cryptographic modules for the offline CA are stored in a secure container. The CA supervisor has the combination (or key) to the container, while the CA administrator has the password to activate the cryptographic module. Access to the private key for this CA, for key recovery purposes also required two-party control, as described in 6.2.4 below.

Activation of the private key for the production CA also requires two-party control, which is effected through use of the HSM.

6.2.3. Private key escrow

No private key escrow procedures are required for this PKI.

6.2.4. Private key backup

LACNIC creates backup copies of CA private keys for both routine and disaster recovery purposes. Such keys are stored within [ ]. One token is stored onsite in a security container, and the other is stored offsite.
Two party access controls to backed-up private keys are applied using the same procedure described in 6.2.2. A password (separate from the cryptographic module administrator password) is used to enable encryption of the backup copy of the private key. The CA Administrator holds this password in [....].

6.2.5. Private key archival

See sections 6.2.3 and 6.2.4

6.2.6. Private key transfer into or from a cryptographic module

The private keys for LACNIC's production CA MUST be generated by the cryptographic module specified in 6.2.1. The private keys will never leave the module except in encrypted form for backup and/or transfer to a new module.

6.2.7. Private key storage on cryptographic module

The private key for LACNIC's production CA MUST be stored in the cryptographic module and will be protected from unauthorized use in accordance with the FIPS 140-2/3 requirements applicable to the module. (See [FIPS])

6.2.8. Method of activating private key

Activation of either the production or offline CA private key requires use of the CA administrator password, as well as password used to initiate a secure connection to the cryptographic module.

6.2.9. Method of deactivating private key

The cryptographic module, when activated, will not be left unattended. After use, it will be deactivated. The module will be stored securely when not in use.

6.2.10. Method of destroying private key

When either the offline or production CA keys are superseded, or upon cessation of operations, LACNIC will destroy the old CA private keys. Destruction is effected using the zeroization function of the hardware cryptographic modules to ensure

that there are no residual remains of the key that could lead to the reconstruction of the key.

6.2.11. Cryptographic Module Rating

The cryptographic module used by the LACNIC production CA will be certified FIPS 140-2/3, at level 3 [FIPS].

6.3. Other aspects of key pair management

6.3.1. Public key archival

Because this PKI does not support non-repudiation, there is no need to archive public keys.

6.3.2. Certificate operational periods and key pair usage periods

The LACNIC CA's key pair will have a validity interval of 10 years.

6.4. Activation data

6.4.1. Activation data generation and installation

Passwords are used to activate the cryptographic modules for both the production and offline CAs. They are generated and installed in the same fashion. The trusted individual serving in the role generates each password. The individual enters each password directly into the cryptographic module, via a serial interface to the module, upon module initialization.

6.4.2. Activation data protection

A LACNIC staff member filling a trusted role for a CA memorizes the cryptographic module password he/she uses to perform the operations associated with the role. The staff member also memorizes the password used to activate the key used to secure communication between the CA server and the cryptographic module.

6.4.3. Other aspects of activation data

None

6.5. Computer security controls

6.5.1. Specific computer security technical requirement

LACNIC ensures that the systems maintaining CA software and data files are trustworthy. This is achieved by the use of operating systems controls on access to systems as a whole, application- specific controls, regular periodic maintenance, and application of advised bug fixes and patches. CA systems are connected to internal networks protected via firewalls, or operated as offline systems where applicable.

These systems are secured from unauthorized access and are logically separated from other computers used for other LACNIC operations. Access authorization is local to the CA machines and does not depend on any network-based, third-party agents.
User authentication is based on use of tightly managed passwords (with mandated character set diversity and 6-month change cycles) or challenge-response tokens. Logical separation of the CA systems from other LACNIC systems is achieved through use of network protocol filtering, ACLs, and switch configuration.

6.6. Life cycle technical controls

6.6.1. System development controls

CA system software not acquired externally was developed by LACNIC staff (not by contractors) and other RIRs staff.

LACNIC software development follows the 'agile' software development methodology, which includes test driven development. All software is developed and maintained under a revision control system and releases are tagged. Code is subject a code review during development.

LACNIC software development uses bug and issue tracking software for all software development. Prior to release, code is packaged and deployed to a standalone platform for integration tests. Deployment to the production systems is from the same packages used for integration tests. Code deployment is scheduled during known maintenance windows, with post-deployment (live) testing and back-out planning and is performed by LACNIC operations staff. Externally visible issues in deployed systems are tracked using a ticketing system in the operations and software contexts.

6.6.2. Security management controls

Cryptographic module and associated host access control is isolated from the general LACNIC access control framework.

The cryptographic module and associated host have specific ACLs limiting network access to the RPKI host on the web service port. Outbound ACLs are limited to the security audit, backup, and systems management and maintenance tasks.

Access to the RPKI systems is audited, and logged. These logs are exported to a separate system maintained by the LACNIC security officer, for later processing and review.

6.6.3. Life cycle security controls

Software and hardware used for the RPKI was acquired through normal LACNIC commercial purchasing procedures. The cryptographic module hardware is acquired on an as-needed basis from suppliers who specialize in FIPS compliant systems. Support contracts are maintained with suppliers to facilitate software maintenance.

Host operating systems are maintained to current patch levels and CERT and other security advisories are tracked for relevant vulnerabilities.

Hosts and network infrastructure are physically maintained and replaced in duty cycle averaging 3 years. Onsite maintenance contracts cover normal business hours support for this hardware.

Software release to deployed services is scheduled, with planned back-out, and post-deployment testing of service. Computers supporting the CA functions are attached physical, and logical networks after consideration of security risks. ACLs are used to limit inter-network segment traffic as needed.

6.7. Network security controls

LACNIC performs all its CA and RA operations using a secured network to prevent unauthorized access and other malicious activity. LACNIC protects communications of sensitive information through the use of encryption and digital signatures. Communications are protected by at least one of TLS/SSL with client and server certificates, and with SSH version 2 with 1024-bit keys, or better. Offline communications are secured through use of signed objects on physical media.

6.8. Time-stamping

The RPKI does not make use of time stamping.

7. Certificate and CRL Profiles

Please refer to the Certificate and CRL Profile [RFCyyyy]

8. Compliance Audit and Other Assessments

LACNIC plan to employ an outside auditor to perform periodic vulnerability assessments for computer and network systems, including those that are part of the RPKI CA.

8.1. Frequency or circumstances of assessment

[OMITTED]

8.2. Identity/qualifications of assessor

[OMITTED]

8.3. Assessor's relationship to assessed entity

[OMITTED]

8.4. Topics covered by assessment

[OMITTED]

8.5. Actions taken as a result of deficiency

[OMITTED]

8.6. Communication of results

9. Other Business And Legal Matters

9.1. Fees

There are no fees for LACNIC members to use the LACNIC RPKI system.

9.1.1. Certificate issuance or renewal fees

There are no fees for LACNIC members to issue or renew certificates in the LACNIC RPKI system.

9.1.2. Fees for other services (if applicable)

[OMITTED]

9.1.3. Refund policy

[OMITTED]

9.2. Financial responsibility

[OMITTED]

9.2.1. Insurance coverage

[OMITTED]

9.2.2. Other assets

[OMITTED]

9.2.3. Insurance or warranty coverage for end-entities

[OMITTED]

9.3. Confidentiality of business information

[OMITTED]

9.3.1. Scope of confidential information

[OMITTED]

9.3.2. Information not within the scope of confidential information

[OMITTED]

9.3.3. Responsibility to protect confidential information

[OMITTED]

9.4. Privacy of personal information

[OMITTED]

9.4.1. Privacy plan

[OMITTED]

9.4.2. Information treated as private

[OMITTED]

9.4.3. Information not deemed private

[OMITTED]

9.4.4. Responsibility to protect private information

[OMITTED]

9.4.5. Notice and consent to use private information

[OMITTED]

9.4.6. Disclosure pursuant to judicial or administrative process

[OMITTED]

9.4.7. Other information disclosure circumstances

[OMITTED]

9.5. Intellectual property rights (if applicable)

[OMITTED]

9.6. Representations and warranties

9.6.1. CA representations and warranties

[OMITTED]

9.6.2. Subscriber representations and warranties

[OMITTED]

9.6.3. Relying party representations and warranties

[OMITTED]

9.7. Disclaimers of warranties

[OMITTED]

9.8. Limitations of liability

[OMITTED]

9.9. Indemnities

[OMITTED]

9.10. Term and termination

[OMITTED]

9.10.1. Term

[OMITTED]

9.10.2. Termination

[OMITTED]

9.10.3. Effect of termination and survival

[OMITTED]

9.11. Individual notices and communications with participants

9.12. Amendments

[OMITTED]

9.12.1. Procedure for amendment

[OMITTED]

9.12.2. Notification mechanism and period

[OMITTED]

9.13. Dispute resolution provisions

[OMITTED]

9.14. Governing law

[OMITTED]

9.15. Compliance with applicable law

[OMITTED]

9.16. Miscellaneous provisions

[OMITTED]

9.16.1. Entire agreement

[OMITTED]

9.16.2. Assignment

[OMITTED]

9.16.3. Severability

[OMITTED]

9.16.4. Enforcement (attorneys' fees and waiver of rights)

[OMITTED]

9.16.5. Force Majeure

[OMITTED]

10. Informative References

[BGP4] Y. Rekhter, T. Li (editors), A Border Gateway Protocol 4 (BGP-4). IETF RFC 1771, March 1995.

[FIPS] Federal Information Processing Standards Publication 140-3 (FIPS-140-3), "Security Requirements for Cryptographic Modules", Information Technology Laboratory, National Institute of Standards and Technology, work in progress.

[RSA] Rivest, R., Shamir, A., and Adelman, L. M. 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21, 2 (Feb.), 120-126.