AFRINIC Certification Practice Statement for the Resource PKI

Version: 2.0

V1.0: published January 2011

V2.0 published – March 2015

Table of Contents

Article I. Introduction

This document is the Certification Practice Statement (CPS) of AFRINIC. It describes the practices employed by the AFRINIC Certification Authority (CA) in the Internet IP Address and Autonomous System (AS) Number PKI. These practices are defined in accordance with the requirements of the Certificate Policy (CP, [RFC6484]) of this PKI.

The Internet IP Address and AS Number PKI is aimed at supporting verifiable attestations about resource controls, e.g., for improved routing security. The goal is that each entity that allocates IP addresses or AS numbers to an entity will, in parallel, issue a certificate reflecting this allocation. These certificates will enable verification that the holder of the associated private key has been allocated the resources indicated in the certificate, and is the current, unique holder of these resources. The certificates and CRLs, in conjunction with ancillary digitally signed data structures, will provide critical inputs for routing security mechanisms, e.g., generation of route filters by ISPs.

The most important and distinguishing aspect of the PKI for which this CPS was created is that it does not purport to identify an address space holder or AS number holder via the subject name contained in the certificate issued to that entity. Rather, each certificate issued under this policy is intended to enable an entity to assert in a verifiable fashion, that it is the current holder of an address block or an AS number, based on the current records of the entity responsible for the resources in question. Verification of the assertion is based on two criteria: the ability of the entity to digitally sign data producing a signature that is verifiable using the public key contained in the corresponding certificate, and validation of that certificate in the context of this PKI. This PKI is designed exclusively for use in support of validation of claims related to address space and AS number holdings, with emphasis on support of routing security mechanisms. Use of the certificates and CRLs managed under this PKI for any other purpose is a violation of this PKI’s CP, and relying parties should reject such uses.

Note: This CPS is based on the template specified in RFC 3647. A number of sections contained in the template were omitted from this CPS because they did not apply to this PKI. However, we have retained section heading “place holders” for these omitted sections, in order to facilitate comparison with the section numbering scheme employed in that RFC, i.e., the relevant section headings are included and marked [OMITTED]. In the Table of Contents the relevant sections are also marked [OMITTED].

Section I.1 Overview

This CPS describes:

- Participants
- Distribution 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

The PKI encompasses several types of certificates:

- CA certificates for each organization allocating address blocks and/or AS numbers, and for each address space (AS number) holder
- End entity (EE) certificates for organizations to use in verifying signatures of Route Origination Authorizations (ROAs) and other (non-certificate/CRL) signed objects
- In the future, the PKI also may include end entity certificates in support of access control for the repository system

Section I.2 Document name and identification

The name of this document is "AFRINIC Certification Practice Statement for the Resource PKI".

Section I.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 LIR/ISP. Thus, in this PKI, the term "subscriber" can refer both to LIRs/ISPs, which can be subscribers of RIRs, NIRs, and other LIRs, and also to organizations that are not ISPs, but which are subscribers of ISPs in the networking sense of the term. Also note that, for brevity, this document always refers to subscribers as organizations, even though some subscribers are individuals. When necessary, the phrase "network

subscriber” is used to refer to an organization that receives network services from an LIR/ISP.

(a) Certification authorities

AFRINIC operates two CAs for the RPKI: one is designated “offline” and the other is designated “production.” The offline CA is the top level CA for the AFRINIC portion of the RPKI. It provides a secure revocation and recovery capability in case the production CA is compromised or become unavailable Thus this CA issues certificates only to instances of the production CA and the CRLs it issues are used to revoke only a certificate issued to that CA. The production CA is used to issue RPKI certificates to AFRINIC members, to which address space or AS numbers have been allocated. In the future, the production CA also may issue other types of end entity (EE) certificates, e.g., EE certificates to operations personnel in support of repository maintenance.

(b) 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 certificates issued by the AFRINIC Business PKI (BPKI) (see Section 3.2.6) to identify individuals authorized to requests certificates under the RPKI. AFRINIC already establishes a business relationship with each subscriber (AFRINIC member) and assumes responsibility for allocating and tracking the current allocation of address space and AS numbers. Since AFRINIC operates the BPKI CA, there is no distinct RA for the RPKI.

(c) Subscribers

Two types of organizations receive allocations of IP addresses and AS numbers from this CA and thus are subscribers in the PKI sense: network subscribers i.e.

End-Users and LIRs or ISPs.

(d) Relying parties

Entities that need to validate claims of address space and/or AS number current holdings are relying parties. Thus, for example, entities that make use of address and AS number allocation certificates in support of improved routing security are relying parties. Registries are relying parties because they transfer resources between one another and thus will need to verify (cross) certificates issued in conjunction with such transfers. This includes LIRs/ISPs, multi-homed organizations exchanging BGP [BGP4] traffic with LIRs/ISPs, and subscribers who have received

an allocation of address space from one ISP or from a registry, but want to authorize an (or another) LIR/ISP to originate routes to this space.

To the extent that repositories make use of certificates for access control – checking for authorization to upload certificate, CRL, and ROA update packages – they too act as relying parties.

(e) Other participants

AFRINIC operates a repository that holds certificates, CRLs, and other RPKI signed objects, e.g., ROAs.

Section I.4 Certificate usage

(a) Appropriate certificate uses

The certificates issued under this hierarchy are for authorization in support of validation of claims of current holdings of address space and/or AS numbers, e.g., for routing security. With regard to routing security, an initial goal of this PKI is to allow the holder of a set of address blocks to be able to declare, in a secure fashion, the AS number of each entity that is authorized to originate a route to these addresses, including the context of ISP proxy aggregation. Additional uses of the PKI, consistent with the basic goal cited above, are also permitted under this policy.

Some of the certificates that may be issued under this hierarchy could be used to support operation of this infrastructure, e.g., access control for the repository system. Such uses also are permitted under this policy.

(b) Prohibited certificate uses

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

Section I.5 Policy administration

(a) Organization administering the document

This CPS is administered by AFRINIC.

(b) Contact person

The RPKI CPS point of contact is the CEO for AFRINIC. He may be reached at AFRINIC Ltd, 11th Floor, Raffles Tower, Ebène, Mauritius.

(c) Person determining CPS suitability for the policy

Not applicable. Each organization issuing a certificate in this PKI is attesting to the allocation of resources (IP addresses, AS numbers) 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 allocation hence they are authoritative with respect to the accuracy of this binding.

(d) CPS approval procedures

Not applicable. Each organization issuing a certificate in this PKI is attesting to the allocation of resources (IP addresses, AS numbers) 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 allocation hence they are authoritative with respect to the accuracy of this binding.

Section I.6 Definitions and acronyms

BPKI - Business PKI: A BPKI is 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.

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

LIR - Local Internet Registry. This is an organization, typically a network service provider, that sub-allocates the assignment of IP addresses for a portion of the area covered by a Regional (or National) Registry.

RIR - Regional Internet Registry. An RIR is an organization that manages the assignment of IP address and AS numbers for a specified geopolitical area. At present, there are five RIRs: AFRINIC (Africa and Indian Ocean). APNIC (Asia – Pacific), ARIN (North America), LACNIC (Latin America and Caribbean) and RIPE NCC (Europe, Russia and Middle-East).

ROA – Route Origination Authorization. This is a digitally signed object that identifies a network operator,

identified by an AS, that is authorized to originate routes to a specified set of address blocks.

Article II. Publication And Repository Responsibilities

Section II.1 Repositories

As per the CP, certificates and CRLs, are made available for downloading by all network operators, to enable them to validate this data for use in support of routing security. The AFRINIC RPKI CA publishes certificates, CRLs, and other signed objects accessible via RSYNC or HTTPS at rpki.afrinic.net.

Section II.2 Publication of certification information

AFRINIC uploads certificates and CRLs issued by it to a local repository system that operates as part of a world-wide distributed system of repositories.

Section II.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.

The AFRINIC CA will publish its CRL prior to the nextScheduledUpdate value in the scheduled CRL previously issued by the CA. Within 24 hours of effecting revocation, the CA will publish a CRL with an entry for the revoked certificate.

Section II.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 ROAs) uploaded to a repository are digitally signed. 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.

Article III. Identification And Authentication

Section III.1 Naming

(a) Types of names

The Subject of each certificate issued by this Registry is identified by an X.500 Distinguished Name (DN). For certificates issued to LIRs/ISPs and subscribers, the Subject will consist of a single CN attribute with a value generated by the issuer.

(b) Need for names to be meaningful

The Subject name in each subscriber certificate will be unique relative to all certificates issued by AFRINIC RPKI CA. However, there is no guarantee that the subject name will be globally unique in this PKI.

Note: The name of the holder of an address block or AS number need not to be “meaningful” in the conventional, human-readable sense, since certificates issued under this PKI are used for authorization in support of routing security, not for identification

(c) 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.

(d) Rules for interpreting various name forms

None

(e) Uniqueness of names

AFRINIC 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.

(f) Recognition, authentication, and role of trademarks

Because the Subject names are not intended to be meaningful, there is no provision to recognize nor authenticate trademarks, service marks, etc.

Section III.2 Initial identity validation

(a) Method to prove possession of private key

AFRINIC accepts certificate requests via the protocol described in [up/down]. This protocol makes use of the PKCS #10 format, as profiled in [res-certificate-profile]. This request format requires that the PKCS #10 request be signed using the (RSA) private key corresponding to the public key in the certificate request. This mechanism provides proof of possession by the requester.

(b) Authentication of organization identity

Certificates issued under this PKI do not attest to the organizational identity of resource holders, with the exception of registries. However, certificates are issued to resource holders in a fashion that preserves the accuracy of allocations as represented in AFRINIC records. Specifically, a BPKI certificate used to authenticate a certificate request serves as a link to the AFRINIC member database that maintains the resource allocation records. The certificate request is matched against the database record for the member in question, and an RPKI certificate is issued only if the resources requested are a subset of those held by the member.

(c) Authentication of individual identity

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

The AFRINIC BPKI (see Section 3.2.6) issues certificates that are used to identify individuals who represent AFRINIC members that are address space (or AS number) holders.

(d) Non-verified subscriber information

No non-verified subscriber data is included in certificates issued under this certificate policy.

(e) Validation of authority

Only an individual to whom a BPKI certificate (see Section 3.2.6) has been issued may request issuance of an RPKI certificate. Each certificate issuance request is verified using the BPKI.

(f) Criteria for interoperation

The RPKI is neither intended nor designed to interoperate with any other PKI. However, AFRINIC operates a BPKI [cps-

business-pki] that is used to authenticate members and to enable them to manage their resource allocations. The Resource PKI relies on this BPKI to authenticate Subscribers who make certificate requests, revocation requests, etc.

Section III.3 Identification and authentication for re-key requests

(a) Identification and authentication for routine re-key

Routine re-key is effected via a Certificate Issuance Request message as described in [up/down]. This digitally signed CMS message is authenticated using a BPKI certificate associated with the requester.

(b) Identification and authentication for re-key after revocation

Re-key after revocation is effected via a Certificate Issuance Request message as described in [up/down]. This digitally signed CMS message is authenticated using a BPKI certificate associated with the requester.

Section III.4 Identification and authentication for revocation request

An RPKI Subscriber makes an explicit revocation request using the protocol defined in [up/down]. Revocation requests in this protocol are digitally signed CMS messages, and are verified using a public key bound to an authorized representative via the AFRINIC BPKI.

When a Subscriber requests a new resource allocation, an existing resource certificate issued to the subscriber is NOT revoked, so long as the set of resources allocated to the Subscriber did not “shrink,” i.e., the new resources are a superset of the old resource set. However, if a new resource allocation results in “shrinkage” of the set of resources allocated to a Subscriber, this triggers an implicit revocation of the old resource certificate(s) associated with that Subscriber.

Article IV. Certificate Life-Cycle Operational Requirements

Section IV.1 Certificate Application

(a) Who can submit a certificate application

Any entity that holds ASN and/or IP addresses and is in good standing may request a certificate under the RPKI. The entity should be enrolled under the AFRINIC BPKI.

(b) Enrollment process and responsibilities

AFRINIC members who are resource holders are enrolled in the AFRINIC BPKI via the process described in [www.afrinic.net/ca/index.html]. Only a member who holds a certificate issued under the BPKI is eligible to make an RPKI certificate request.

Section IV.2 Certificate application processing

An AFRINIC resource holder requests a certificate via a Certificate Issuance Request message [up/down], which is authenticated via the digital signature on the CMS envelope. The certificate used to authenticate the message is issued under the AFRINIC BPKI. AFRINIC processes the resource request as described in [up/down]. The Certificate Issuance Response message [up/down] either provides the certificate to the Subscriber, or provides a response indicating why the request was not fulfilled.

(a) Performing identification and authentication functions

The AFRINIC BPKI is used to identify an AFRINIC member representative applying for a certificate via a certificate issuance request in the up/down protocol. See the AFRINIC BPKI CPS for additional details [cps-business-pki]

(b) Approval or rejection of certificate applications

The Certificate Issuance Response message [up/down] either provides the certificate to the Subscriber, or provides a response indicating why the request was not fulfilled. Certificate approval/rejection, for a syntactically valid request, is based on the AFRINIC resource allocation policy described at [http://www.afrinic.net/rs/eligibility.htm].

(c) Time to process certificate applications

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

Section IV.3 Certificate issuance

(a) CA actions during certificate issuance

A Subscriber generates a draft certificate using the PKCS #10 format, as profiled in [res-certificate-profile]. This draft certificate is encapsulated in a CMS message, signed by the requester, and submitted as a Certificate Issuance Request as described in [up/down]. The CA verifies the request message as described in [up/down] and generates a Certificate Issuance Response message. That message either contains the requested certificate, or provides a response indicating why the request was not fulfilled.

(b) Notification to subscriber by the CA of issuance of certificate

A Subscriber is notified of the issuance of a new certificate by the Certificate Issuance Response message.

(c) Notification of certificate issuance by the CA to other entities [OMITTED]

Section IV.4 Certificate acceptance

(a) 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.

(b) Publication of the certificate by the CA

Certificates will be published in the Repository system within 1 business day of being issued by this CA.

Section IV.5 Key pair and certificate usage

A summary of the use model for the IP Address and AS Number PKI is provided below.

(a) Subscriber private key and certificate usage

The certificates issued by this registry to resource holders 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 will issue certificates to any organizations to which it allocates resources and one or more EE certificates for use in verifying signatures on ROAs signed by the subscriber. Subscribers that are LIRs issue certificates to organizations to which they have allocated address space. Subscribers also will issue certificates to operators in support of repository access control.

(b) Relying party public key and certificate usage

The primary relying parties in this PKI are LIRs/ISPs, who will use RPKI EE certificates to verify ROAs and other signed objects, e.g., in support of generating route filters.

Section IV.6 Certificate renewal

(a) Circumstance for certificate renewal

As per the CP, a certificate will 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 AFRINIC initiates the renewal process based on the certificate expiration date, then AFRINIC will notify the resource holder 3 months prior to the expiration date. The validity interval of the new (renewed) certificate will overlap that of the previous certificate by 3 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.

(b) Who may request renewal

The certificate holder or AFRINIC may initiate the renewal process. For the case of the certificate holder, only an individual to whom a BPKI certificate (see Section 3.2.6) has been issued may request renewal of an RPKI certificate. Each certificate issuance request is verified using the BPKI.

(c) Processing certificate renewal requests

A Subscriber requests certificate renewal by sending a Certificate Issuance Request message [up/down].

(d) Notification of new certificate issuance to subscriber

A Subscriber is notified of the issuance of a new certificate via the Certificate Issuance Response message, if the Subscriber initiated the renewal. If AFRINIC initiated the renewal process, the Subscriber is notified by the posting of the renewed certificate in the repository. A Subscriber can discover a certificate renewed by AFRINIC through use of the List message [up/down].

(e) Conduct constituting acceptance of a renewal certificate

A Subscriber is deemed to have accepted a certificate unless the subscriber explicitly requests revocation of the

certificate after publication in the AFRINIC RPKI repository system, as described in Section 4.9.3.

(f) Publication of the renewal certificate by the CA

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

(g) Notification of certificate issuance by the CA to other entities [OMITTED]

Section IV.7 Certificate re-key

(a) Circumstance for certificate re-key

As per the CP, re-key of a certificate will be performed only when requested, 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.

(b) Who may request certification of a new public key

The holder of the certificate may request a re-key. In addition, AFRINIC may initiate a re-key based on a verified compromise report. If the Subscriber (certificate Subject) requests the rekey, authentication is effected using the AFRINIC BPKI.

(c) Processing certificate re-keying requests

A Subscriber requests a re-key of a certificate by issuing a Certificate Issuance Request message in which the resources are ones that the Subscriber already holds, but a

new public key is provided in the PKCS #10 portion of the request.

(d) Notification of new certificate issuance to subscriber

A Subscriber is notified of the issuance of a re-keyed certificate via the Certificate Issuance Response message.

(e) 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.

(f) 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.

(g) Notification of certificate issuance by the CA to other entities [OMITTED]

Section IV.8 Certificate modification

(a) 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 resource holdings of the subscriber. The request may be implicit, a side effect of the allocation of additional resources, or may be explicit. A subscriber also may request that its existing set of resources be redistributed among multiple certificates. This example of certificate modification is effected through issuance of new certificates, and revocation of the previous certificates.

If a subscriber is to be allocated address space or AS numbers in addition to a current allocation, and if the subscriber does not request that a new certificate be issued containing only these 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 address space and AS allocations expanded. When previously allocated address space or AS numbers are to be removed from a certificate, then the old certificate MUST

be revoked and a new certificate (reflecting the new allocation) issued.

(b) Who may request certificate modification

The certificate holder or AFRINIC may initiate the certificate modification process. If a certificate holder requests the modification, the request is authenticated using the AFRINIC BPKI, as described in [up/down]. AFRINIC will modify a certificate, and revoke the old certificate, if, for example, a Subscriber fails to renew membership in a timely fashion.

(c) 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.

(d) 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 AFRINIC RPKI repository system.

(e) Conduct constituting acceptance of modified 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.

(f) Publication of the modified certificate by the CA

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

(g) Notification of certificate issuance by the CA to other entities [OMITTED]

Section IV.9 Certificate revocation and suspension

(a) Circumstances for revocation

As per the CP, certificates can be revoked for several reasons. Either AFRINIC 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 resources 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 that certificate.

(b) Who can request revocation

The certificate holder or AFRINIC may request a revocation. A Subscriber requests certificate revocation using the Certificate Revocation Request message described in [up/down].

(c) Procedure for revocation request

A Subscriber requests certificate revocation using the Certificate Revocation Request message described in [up/down]. The Certificate Revocation Response messages confirms receipt of the revocation request by AFRINIC, and indicates that AFRINIC will include the revoked certificate in a CRL.

(d) Revocation request grace period

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

(e) Time within which CA must process the revocation request

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

(f) 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.

(g) CRL issuance frequency

The AFRINIC RPKI CA production will publish a new CRL every 24 hours. The AFRINIC 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. AFRINIC will set the nextScheduledUpdate value when it issues a CRL, to signal when the next scheduled CRL will be issued.

(h) Maximum latency for CRLs

A CRL will be posted to the repository system with minimal delay after generation.

(i) On-line revocation/status checking availability [OMITTED]

(j) On-line revocation checking requirements [OMITTED]

(k) Other forms of revocation advertisements available [OMITTED]

(l) Special requirements re key compromise [OMITTED]

(m) Circumstances for suspension [OMITTED]

(n) Who can request suspension [OMITTED]

(o) Procedure for suspension request [OMITTED]

(p) Limits on suspension period [OMITTED]

Section IV.10 Certificate status services

AFRINIC does not support OCSP. AFRINIC issues CRLs.

(a) Operational characteristics [OMITTED]

(b) Service availability [OMITTED]

(c) Optional features [OMITTED]

Section IV.11 End of subscription [OMITTED]

Section IV.12 Key escrow and recovery [OMITTED]

(a) Key escrow and recovery policy and practices [OMITTED]

(b) Session key encapsulation and recovery policy and practices [OMITTED]

Article V. Facility, Management, And Operational Controls

Section V.1 Physical controls

(a) Site location and construction

Operations for the AFRINIC RPKI CA and RA are conducted within a physically protected area of an office building in which AFRINIC is a tenant. This building is located at AFRINIC Ltd, 11th Floor, Raffles Tower Cyber City, Ebène, Mauritius. AFRINIC space within this facility includes offices and meeting spaces and one machine room. The AFRINIC CA system (including CA and RA computers and cryptographic modules) is in the machine room .

(b) Physical access

The AFRINIC CA systems are protected by two levels of physical security. Only AFRINIC staff have access to AFRINIC space within the building and only AFRINIC system administrators have access to the machine room where the CA systems reside. A receptionist is on duty at the main entrance during normal business hours (9 AM to 5:30 PM, M-F, except Mauritian holidays). AFRINIC staff are issued key cards that grant access to the AFRINIC space at any time. AFRINIC staff authorized for CA roles as noted in 5.2.1 are granted separate access to the space that houses the CA systems.

(c) Power and air conditioning

The AFRINIC CA computers and cryptographic module are 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 room containing this equipment makes use of HVAC (heating/ventilation/air conditioning) systems to control temperature and relative humidity.

(d) Water exposures

Machine room is located in the eleventh level of the building noted in 5.1.1. There is no history of flooding in this area of Mauritius that has reached the elevation of the this level of the building.

(e) Fire prevention and protection

Fire suppression for machine room is provided by portable CO_2 extinguishers.

(f) Media storage

All media containing production software and data for the CA and RA functions, plus audit logs, are stored within AFRINIC facilities. Data software on disk is backed up to a 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 effected via user accounts restricted to staff members responsible for computer system operation.

(g) 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.

(h) Off-site backup

AFRINIC 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. Offsite backup media (tape) are held by a company specializing in secure offsite media storage.

Section V.2 Procedural controls

(a) Trusted roles

Two trusted roles are defined for managing the AFRINIC 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.

(b) Number of persons required per task

AFRINIC assigns two individuals to each role, a primary and a backup. There is no overlap among the individuals assigned to these roles, i.e., there are four distinct individuals staffing the two roles cited in 5.2.1. The staff fulfilling these roles may be shared across the two CAs (offline and production), but no single individual will fulfill the same role for both CAs.

(c) Identification and authentication for each role

For the production CA, access is controlled via password-protected login over a SSH-protected connection via the AFRINIC back-office LAN.

The offline CA server is a laptop computer stored with the offline CA cryptographic module 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.

(d) Roles requiring separation of duties

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

Section V.3 Personnel controls

(a) Qualifications, experience, and clearance requirements

Only full-time AFRINIC 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.

(b) Background check procedures

All AFRINIC staff undergo normal employment reference checks.

(c) Training requirements

AFRINIC 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. AFRINIC maintains records of such training and periodically reviews and enhances its training programs as necessary.

(d) Retraining frequency and requirements

AFRINIC 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.

(e) Job rotation frequency and sequence

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

(f) Sanctions for unauthorized actions

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

(g) Independent contractor requirements

No independent contractor or consultant is used to perform AFRINIC 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 AFRINIC staff at all times when in sensitive areas, e.g., machine room.

(h) Documentation supplied to personnel

Training for staff assigned to a trusted CA role is primarily via mentoring. An internal wiki is maintained by AFRINIC staff as a further training aid.

Section V.4 Audit logging procedures

(a) Types of events recorded

Audit records are generated for the basic operations of the CA servers. Audit records include the date, time, responsible user, and summary content data relating to the event. Messages requesting CA actions, i.e., certificate requests and certificate revocation requests, are logged. The cryptographic modules maintain internal logs of operations they perform, although these records do not maintain user ID info.

The physical access control system separately maintains logs for access to the areas housing sensitive CA equipment, i.e., machine room 1.

(b) Frequency of processing log

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

(c) Retention period for audit log

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

(d) Protection of audit log

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

(e) Audit log backup procedures

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

(f) Audit collection system (internal vs. external) [OMITTED]

(g) Notification to event-causing subject [OMITTED]

(h) Vulnerability assessments

AFRINIC employs an outside firm to perform periodic vulnerability assessments for computer and network systems. These reports are provided to the AFRINIC CTO and to the AFRINIC CEO.

Section V.5 Records archival [OMITTED]

(a) Types of records archived [OMITTED]

(b) Retention period for archive [OMITTED]

(c) Protection of archive [OMITTED]

(d) Archive backup procedures [OMITTED]

(e) Requirements for time-stamping of records [OMITTED]

(f) Archive collection system (internal or external) [OMITTED]

(g) Procedures to obtain and verify archive information [OMITTED]

Section V.6 Key changeover

The AFRINIC production CA key pair changes on a scheduled basis. In anticipation of this rekey activity, AFRINIC reissues all of the certificates issued under the old key prior to expiration of the old certificate. AFRINIC then creates a new key pair, and acquires and publishes a new certificate containing the new public key, a minimum of 1 week in advance of the scheduled rekey. Once the new CA certificate has been published, no more certificates are issued under the old CA key. The CA continues to issue CRLs under the old key until the old certificate expires.

Section V.7 Compromise and disaster recovery [OMITTED]

(a) Incident and compromise handling procedures [OMITTED]

(b) Computing resources, software, and/or data are corrupted [OMITTED]

(c) Entity private key compromise procedures [OMITTED]

(d) Business continuity capabilities after a disaster [OMITTED]

Section V.8 CA or RA termination

AFRINIC has been granted sole authority by IANA to manage allocation of IP address space and AS number resources in the Asia-Pacific region. AFRINIC 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.

Article VI. Technical Security Controls

This section describes the security controls used by AFRINIC.

Section VI.1 Key pair generation and installation

(a) Key pair generation

For the production and CAs operated by AFRINIC, key pairs are generated using a hardware cryptographic module. The module used for this purpose is certified as complying with FIPS 140-2 level 3. The hardware cryptographic module employed for this process is the [HSM name] (Authentication method used).

AFRINIC 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.

(b) Private key delivery to subscriber

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

(c) Public key delivery to certificate issuer

Subscribers deliver public keys to the AFRINIC RPKI CA by use of the up/down protocol as described in [up/down].

(d) CA public key delivery to relying parties

CA public keys for all entities other than RIRs are contained in certificates issued by other CAs. These certificates plus certificates used to represent inter-RIR transfers of address space or AS numbers are published via a repository system. Relying parties may download these certificates from this system. Public key values and associated data for the trust anchors (RIRs) are distributed out of band, e.g., embedded in path validation software that will be made available to the Internet community.

(e) Key sizes

AFRINIC CAs use an RSA key of 2048 bits or greater. For subscriber and LIR/ISP certificates, the RSA keys will be of 2048 bits.

(f) Public key parameters generation and quality checking

The RSA algorithm [RSA] is used in this PKI with the public exponent (e) F4 (65,537).

Subscribers are responsible for key pair generation, and are responsible for performing checks on the quality of their key pairs. AFRINIC is not responsible for performing such checks for subscribers.

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

The Key usage extension bit values is consistent with RFC 3280. For AFRINIC's CA certificates, the keyCertSign and cRLSign bits are set TRUE. All other bits (including digitalSignature) are set FALSE, and the extension is marked critical.

Section VI.2 Private Key Protection and Cryptographic Module Engineering Controls

(a) Cryptographic module standards and controls

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

(b) 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 is 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 SafeNet Luna PED.

(c) Private key escrow

No private key escrow procedures are required for this PKI.

(d) Private key backup

AFRINIC creates backup copies of CA private keys for both routine and disaster recovery purposes. Such keys are stored within two password-protected [Nane of the Backup token]. One token is stored onsite in a security container, and the other is stored offsite. Two party control for access to backed-up private keys is effected 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. This password is held by the CA Administrator.

(e) Private key archival

There will be no archive of private keys by this CA.

(f) Private key transfer into or from a cryptographic module

The private keys for AFRINIC's CA are 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.

(g) Private key storage on cryptographic module

The private keys for AFRINIC's CA are stored in the cryptographic module and will be protected from unauthorized use in accordance with the FIPS 140-2 requirements applicable to the module. (See [FIPS])

(h) 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.

(i) Method of deactivating private key

The production CA cryptographic module normally will operate in an unattended mode, on a 24/7 basis, after activation.

The offline CA cryptographic module, when activated, will not be left unattended. When not in use, the module will be deactivated and stored securely, as described in 5.1. Deactivation requires use of the CA administrator password.

(j) Method of destroying private key

When either the offline or production CA keys are superceded, or upon cessation of operations, AFRINIC 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.

(k) Cryptographic Module Rating

The cryptographic module(s) used by AFRINIC for the offline and production RPKI CAs are certified under FIPS 140-2, at level 3 [FIPS].

Section VI.3 Other aspects of key pair management

(a) Public key archival

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

(b) Certificate operational periods and key pair usage periods

The AFRINIC CA's key pair has a validity interval of 10 years.

Section VI.4 Activation data

(a) 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. Each password is generated by the trusted individual serving in the role. Each password is entered by the individual directly into the cryptographic module, via a serial interface to the module, upon module initialization.

(b) Activation data protection

An AFRINIC 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.

(c) Other aspects of activation data

None

Section VI.5 Computer security controls

(a) Specific computer security technical requirement

AFRINIC 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 AFRINIC 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 AFRINIC systems is achieved through use of network protocol filtering, ACLs, and switch configuration.

(b) Computer security rating [OMITTED]

Section VI.6 Life cycle technical controls

(a) System development controls

CA system software was developed by APNIC and currently maintained by AFRINIC staff (not by contractors).

AFRINIC software development follows an 'agile' 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. AFRINIC 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 AFRINIC operations staff. Externally visible issues in deployed systems are tracked using a ticketing system in the operations and software contexts.

(b) Security management controls

Cryptographic module and associated host access control is separated in a private VLAN and is isolated from the general AFRINIC LDAP access control framework.

RPKI front end is accessible via MyAFRINIC but is protected by user login and password and BPKI authentication. The API is also accessible in the general AFRINIC LDAP access control but has a specific group limiting access. Access to RPKI system from outside AFRINIC network is not allowed.

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 AFRINIC security officer, for later processing and review.

(c) Life cycle security controls

Software and hardware used for the RPKI was acquired through normal AFRINIC 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.

Section VI.7 Network security controls

AFRINIC performs all its CA and RA operations using a secured network to prevent unauthorized access and other malicious activity. AFRINIC 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 2048-bit keys, or better for remote access. Offline communications are secured through use of signed objects on physical media.

Section VI.8 Time-stamping

The RPKI operated by AFRINIC does not make use of time stamping.

Article VII. Certificate and CRL Profiles

Article VIII. Please refer to the Certificate and CRL Profile [RFC6487].

Section VIII.1 Certificate profile [OMITTED]

(a) Version number(s) [OMITTED]

(b) Certificate extensions [OMITTED]

(i) Required certificate extensions [OMITTED]

(ii) Deprecated certificate extensions [OMITTED]

(iii) Optional certificate extensions [OMITTED]

(c) Algorithm object identifiers [OMITTED]

(d) Name forms [OMITTED]

(e) Name constraints [OMITTED]

(f) Certificate policy object identifier [OMITTED]

(g) Usage of Policy Constraints extension [OMITTED]

(h) Policy qualifiers syntax and semantics [OMITTED]

(i) Processing semantics for the critical Certificate Policies extension [OMITTED]

Section VIII.2 CRL profile [OMITTED]

(a) Version number(s) [OMITTED]

(b) CRL and CRL entry extensions [OMITTED]

(i) Required CRL extensions [OMITTED]

(ii) Deprecated CRL extensions [OMITTED]

(iii) Optional CRL extensions [OMITTED]

Section VIII.3 OCSP profile [OMITTED]

(a) Version number(s) [OMITTED]

(b) OCSP extensions [OMITTED]

Article IX. Compliance Audit and Other Assessments

AFRINIC employs an outside firm to perform periodic vulnerability assessments for computer and network systems, including those that are part of the RPKI CA.

AFRINIC will not engage an entity to perform a CA compliance audit.

Section IX.1 Frequency or circumstances of assessment

Assessments are initiated at the behest of the Security Officer.

Section IX.2 Identity/qualifications of assessor

The outside firm engaged to perform the assessment is a commercial entity specializing in IT security assessment.

Section IX.3 Assessor's relationship to assessed entity

The outside firm engaged to perform the assessment is a paid contractor with no other relationships to AFRINIC.

Section IX.4 Topics covered by assessment

The external vulnerability assessment perform on AFRINIC IT systems cover a variety of topics including (but not limited to) network port scanning, testing of web application interfaces, review of user authentication and authorization mechanisms, logging and auditing, network security, and configuration management.

Section IX.5 Actions taken as a result of deficiency

The AFRINIC Security Officer reviews all recommendations made by the external assessor and takes remedial actions as appropriate.

Section IX.6 Communication of results

The external vulnerability assessment reports are provided to the AFRINIC CTO and to the AFRINIC CEO.

Article X. Other Business And Legal Matters

Section X.1 Fees

(a) Certificate issuance or renewal fees

Certificate issuance and renewal fees may be charged by AFRINIC. Fees are set from time to time by the Board of directors of AFRINIC. The current schedule of fees are published on the AFRINIC web site.

(b) Fees for other services (if applicable)

AFRINIC charges fees for other services related to the allocation and administration of IP address and Autonomous System number resources. Fees are set from time to time by the Board of Directors of AFRINIC. The current schedule of fees are published on the AFRINIC web site.

(c) Refund policy [OMITTED]

Section X.2 Financial responsibility [OMITTED]

(a) Insurance coverage [OMITTED]

(b) Other assets [OMITTED]

(c) Insurance or warranty coverage for end-entities [OMITTED]

Section X.3 Confidentiality of business information [OMITTED]

(a) Scope of confidential information [OMITTED]

(b) Information not within the scope of confidential information [OMITTED]

(c) Responsibility to protect confidential information [OMITTED]

Section X.4 Privacy of personal information [OMITTED]

(a) Privacy plan [OMITTED]

(b) Information treated as private [OMITTED]

(c) Information not deemed private [OMITTED]

(d) Responsibility to protect private information [OMITTED]

(e) Notice and consent to use private information [OMITTED]

(f) Disclosure pursuant to judicial or administrative process [OMITTED]

(g) Other information disclosure circumstances [OMITTED]

Section X.5 Intellectual property rights (if applicable) [OMITTED]

Section X.6 Representations and warranties [OMITTED]

(a) CA representations and warranties [OMITTED]

(b) Subscriber representations and warranties [OMITTED]

(c) Relying party representations and warranties [OMITTED]

(d) Representations and warranties of other participants [OMITTED]

Section X.7 Disclaimers of warranties [OMITTED]

Section X.8 Limitations of liability [OMITTED]

Section X.9 Indemnities [OMITTED]

Section X.10 Term and termination [OMITTED]

(a) Term [OMITTED]

(b) Termination [OMITTED]

(c) Effect of termination and survival [OMITTED]

Section X.11 Individual notices and communications with participants [OMITTED]

Section X.12 Amendments [OMITTED]

(a) Procedure for amendment [OMITTED]

(b) Notification mechanism and period [OMITTED]

(c) Circumstances under which OID must be changed [OMITTED]

Section X.13 Dispute resolution provisions [OMITTED]

Section X.14 Governing law [OMITTED]

Section X.15 Compliance with applicable law [OMITTED]

Section X.16 Miscellaneous provisions [OMITTED]

(a) Entire agreement [OMITTED]

(b) Assignment [OMITTED]

(c) Severability [OMITTED]

(d) Enforcement (attorneys' fees and waiver of rights) [OMITTED]

(e) Force Majeure

Section X.17 Other provisions [OMITTED]

Article XI. References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3280] Housley, R., Polk, W. Ford, W., Solo, D., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", BCP 14, RFC 2119, March 1997.

[RFCxxxx] Seo, K., Watro, R., Kong, D., and Kent, S. , "Certificate Policy for the Internet IP Address and AS Number PKI", work in progress, July 2007.

[RFCyyyy] Huston, G., Loomans, R., Michaelson, G., "A Profile for X.509 PKIX Resource Certificates", work in progress, June 2007.

[res-certificate-profile] Huston, G., Loomans, R., Michaelson, G., "A Profile for X.509 PKIX Resource Certificates".

[up/down] G. Houston, R. Loomis, B. Ellacott, R. Austien, "A Protocol for Provisioning Resource Certificates,"

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

[FIPS] Federal Information Processing Standards Publication 140-2 (FIPS PUB 140-2), "Security Requirements for Cryptographic Modules", Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.

[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.