APNIC RPKI CPS

1. Introduction

This document is the Certification Practice Statement (CPS) of APNIC. It describes the practices employed by the APNIC Certification Authority (CA) in the Resource PKI [RFC6480]. These practices are defined in accordance with the requirements of the Certificate Policy (CP), [RFC6484] for this PKI.

The RPKI aims to support verifiable attestations about resource controls, e.g., for improved routing security. The goal is that each entity that delegates IP addresses or AS numbers to an entity will, in parallel, issue a certificate reflecting this delegation. These certificates will enable verification that the holder of the associated private key has been delegated the resources indicated in the certificate, and is the current, unique holder of these resources. The certificates and Certificate Revocation Lists (CRLs), in conjunction with ancillary digitally signed data structures, will provide critical inputs for routing security mechanisms, e.g., generation of route filters by Internet Service Providers (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 the RPKI 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 7382. A number of sections contained in the template were omitted from this CPS because they did not apply to the RPKI. 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].

1.1. 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 delegating address blocks and/or AS numbers, and for each address space (AS number) holder.
- End-entity (EE) certificates for organizations to use to validate digital signatures on RPKI-signed objects (see definition in Section 1.6).

1.2. Document name and identification

The name of this document is “APNIC RPKI Certification Practice Statement”.

1.3. PKI participants

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 (Local Internet Registry)/ISP. Thus, in this PKI, the term “subscriber” can refer both to LIRs/ISPs, which can be subscribers of RIRs (Regional Internet Registries), NIRs (National Internet Registries), 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.

1.3.1. Certification authorities

APNIC operates seven CAs for the RPKI: an “offline” CA, an “intermediate” CA, and five “production” CAs.

- The offline CA contains RFC 3779 extensions encompassing all Internet Number Resources (INRs), i.e., all IPv4 and IPv6 addresses and all ASNs. This broad scope is employed to facilitate INR transfers among the RIRs. It provides a secure revocation and recovery capability in case of compromise of the “intermediate” CA. It issues certificates only to instances of the “intermediate” CA and the CRLs it issues are used to revoke only a certificate issued to that CA. This CA is a trust anchor for the RPKI, and its certificate is made available to relying parties using the Trust Anchor Locator (TAL) mechanism defined in RFC 7730.

- The intermediate CA inherits the RFC 3779 resources from the “offline” CA. It issues certificates only to the instances of the “production” CAs.

- The production CAs contain the INR ranges allocated to APNIC from IANA, or by transfers from other RIRs (there is one CA for IANA, and one for each of the other RIRs). These CAs are used to issue RPKI certificates to delegates of INR from APNIC, the holders of APNIC accounts, to which address space or AS numbers have been delegated.

APNIC also operates an unbounded number of APNIC-hosted CAs, on behalf of account holders, by way of the Resource Manager application in the MyAPNIC portal (https://my.apnic.net).

The intermediate, production, and APNIC-hosted CAs are referred to collectively as the ‘online’ CAs.

1.3.2. Registration authorities

APNIC does not make use of explicit registration authorities for the production CAs or the hosted CAs, since APNIC already manages delegation of the INRs that are represented in the RPKI certificates. Hosted CAs are managed by APNIC INR holders through the Resource Manager in the MyAPNIC portal.

1.3.3. Subscribers

Organizations receiving INR delegations from this CA are subscribers in the RPKI.

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 1.6 for the definition of an RPKI-signed object.)

1.3.5. Other participants

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

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 RFC 6484.

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 APNIC.

1.5.2. Contact person

The APNIC CPS point of contact is the Infrastructure and Development Director. The phone number for the point of contact is +61-7-3858-3188. The postal address for the point of contact is 6 Cordelia St, South Brisbane, QLD 4101, Australia.

1.5.3. Person determining CPS suitability for the policy

Not applicable. Each organization issuing a certificate in this PKI is attesting to the delegation 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 delegation hence they are authoritative with respect to the accuracy of this binding.

1.5.4. CPS approval procedures

APNIC may amend the terms of this CPS from time to time. When this happens, the new version of the CPS will be posted to APNIC's website, and the long-lived CPS URL (https://www.apnic.net/RPKI/CPS.pdf) will be updated to point to the new version of the CPS.

1.6. Definitions and acronyms

BPKI - Business PKI. A BPKI is an additional PKI used by an organization to facilitate provisioning protocol [RFC6492] and publication protocol [RFC8181] interactions. APNIC operates a BPKI for this purpose. Self-hosted RPKI clients must also operate a BPKI to make use of the services that rely on these protocols.

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.

IANA - Internet Assigned Numbers Authority. IANA is responsible for global coordination of the Internet Protocol addressing systems and ASNs used for routing Internet traffic. IANA distributes INRs to RIRs.

INR - Internet Number Resources. Internet Number Resources are IPv4 addresses, IPv6 addresses and Autonomous System Numbers (AS Numbers or ASN)

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-delegates the assignment of IP addresses for a portion of the area covered by a Regional (or National) Registry.

NIR – National Internet Registry. An NIR is an organization that manages the assignment of IP address and AS numbers for a portion of the geopolitical area covered by a Regional Registry. These form an optional second tier in the tree scheme used to manage IP address and AS number delegation.

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: ARIN (North America), RIPE NCC (Europe), APNIC (Asia – Pacific), LACNIC (Latin America and Caribbean), and AfriNIC (Africa).

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. See [RFC6482] and [RFC6483].

2. Publication and Repository Responsibilities

2.1. Repositories

The APNIC RPKI CAs publish certificates, CRLs, and RPKI-signed objects in a repository accessible via rsync [RFC5781] at rpki.apnic.net, and via RRDP [RFC8182] at rrdp.apnic.net.

APNIC also operates a publication service [RFC8181] and associated repository for self-hosted RPKI clients. This repository is available via rsync [RFC5781] at rpki.sub.apnic.net and via RRDP [RFC8182] at rrdp.sub.apnic.net.

2.2. Publication of certification information

APNIC uploads certificates and CRLs issued by it to a local repository system that 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:

- Certificates will be published within 24 hours after issuance.
- The APNIC CAs will each publish a CRL prior to the nextUpdate value in the CRL previously issued by the CA.
- Within 24 hours of effecting revocation, each APNIC CA will publish a CRL with an entry for the revoked certificate.

2.4. Access controls on repositories

For APNIC-hosted CAs, access is mediated by the Resource Manager. User identification and authentication in the Resource Manager is handled by APNIC's single sign-on (SSO) system, with additional authorization handled by the Resource Manager itself. APNIC already establishes a business relationship with each subscriber (APNIC account holder) and assumes responsibility for delegating and tracking the current delegation of address space and AS numbers.

Registration for access to APNIC's publication service for self-hosted RPKI clients is controlled by the Resource Manager [RFC8183], on the basis of the existing business relationship with each subscriber (APNIC account holder).

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). For certificates issued to subscribers, the Subject will consist of a single Common Name (CN) attribute and a single serialNumber attribute. Both the CN and serialNumber values are generated by the issuer.

3.1.2. Need for names to be meaningful 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.

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.

For reference, the CN values used in the subjects are also included in the extended-delegated stats file (see https://ftp.apnic.net/stats/apnic/delegated-apnic-extended-latest, the last column).

3.1.4. Rules for interpreting various name forms None

3.1.5. Uniqueness of names Each APNIC production CA certifies Subject names that are unique among all the certificates that it issues. Although it is desirable that these Subject names be unique throughout the RPKI, 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, APNIC makes no provision to recognize nor authenticate trademarks, service marks, etc.

3.2. Initial identity validation

3.2.1. Method to prove possession of private key Certificates issued under the RPKI do not attest to the individual identity of a resource holder. However, APNIC maintains contact information for each resource holder in support of certificate renewal, re-key, and revocation. The account holder identifier of the registration record in the RPKI system (which links back to our internal registry database) is used to confirm the identity of individuals requesting these services.

3.2.2. Authentication of organization identity For all APNIC-hosted CAs, certificate request and issuance operations are handled by internal APNIC systems. For actions initiated by users for these CAs, access control is as described in section 2.4. All other actions on these CAs are managed internally by APNIC.

For self-hosted CAs, access control is as described in section 2.4.

3.2.3. Authentication of individual identity Certificates issued under this PKI do not attest to the individual identity of a resource holder. However, APNIC maintains contact information for each resource holder in support of certificate renewal, re-key, or revocation, via the account holder identifier of the registration record in the RPKI system (which links back to our internal registry database).

3.2.4. Non-verified subscriber information No non-verified subscriber data is included in certificates issued under this certificate policy, except for Subject Information Access (SIA) extensions [RFC6487] for self-hosted RPKI clients.

3.2.5. Validation of authority For APNIC-hosted CAs, only individuals who have the appropriate authorisation in the Resource Manager may request issuance of an RPKI certificate.

For self-hosted CAs, only individuals who have the appropriate authorisation, per earlier registration of details in the Resource Manager under RFC 8183, may request issuance of an RPKI certificate.

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 Routine re-key is effected via a Certificate Issuance Request message as described in RFC 6492. This digitally signed CMS message is authenticated using a BPKI certificate associated with the requester.

3.3.2. Identification and authentication for re-key after revocation

Re-key after revocation is effected via a Certificate Issuance Request message as described in RFC 6492. This digitally signed CMS message is authenticated using a BPKI certificate associated with the requester.

3.4. Identification and authentication for revocation request

An RPKI subscriber makes an explicit revocation request using the protocol defined in RFC 6492. Revocation requests in this protocol are digitally signed CMS messages, and are verified using a public key bound to an authorized representative via the APNIC BPKI.

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

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who can submit a certificate application Any entity registered as an APNIC account holder and which has accepted APNIC’s terms and conditions with respect to RPKI certification, as required by APNIC, may request a certificate under the RPKI.

4.1.2. Enrollment process and responsibilities Users for APNIC account holders are registered in the APNIC SSO system, and associated with APNIC accounts by way of APNIC’s internal registry database. A user who has the appropriate authorization in the SSO system and the Resource Manager is eligible to set up either an APNIC-hosted CA or a self-hosted CA. For an APNIC-hosted CA, certificate issuance is managed by internal APNIC systems. For a self-hosted CA, the user registers their BPKI with APNIC as described in RFC 8183, and from that point the account holder (authorised under that BPKI) may make an RPKI certificate request.

4.2. Certificate application processing

For an APNIC-hosted CA, certificate requests and responses are processed by internal APNIC systems using RFC 6492, with details provided to the user by way of the Resource Manager.

For a self-hosted CA, an APNIC account holder requests a certificate via a Certificate Issuance Request message [RFC6492], which is authenticated via the digital signature on the CMS envelope. The certificate used to authenticate the message is issued under the account holder's BPKI, previously registered in the Resource Manager per RFC 8183. APNIC processes the resource request as described in RFC 6492. The Certificate Issuance Response message [RFC6492] either provides the certificate to the subscriber, or provides a response indicating why the request was not fulfilled.

4.2.1. Performing identification and authentication functions As part of account setup, APNIC verifies the identity of an administrative user for the account. That user can then register in the SSO system and be linked to the associated APNIC account. Once registered, that user can carry out RPKI operations directly, or delegate authorization for RPKI operations to other users, by way of the Resource Manager.

4.2.2. Approval or rejection of certificate applications For an APNIC-hosted CA, certificate approval/rejection is communicated to the user by way of the Resource Manager.

For a self-hosted CA, the Certificate Issuance Response message [RFC6492] either provides the certificate to the subscriber, or provides a response indicating why the request was not fulfilled.

4.2.3. Time to process certificate applications APNIC expects to issue a certificate attesting to a resource delegation within 1 business day after approval of the delegation.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance For an APNIC-hosted CA, certificate issuance is handled by APNIC's internal systems.

For a self-hosted CA, a subscriber generates a draft certificate using the PKCS #10 format, as profiled in RFC 6487. This draft certificate is encapsulated in a CMS message, signed by the requester, and submitted as a Certificate Issuance Request as described in RFC 6492. The CA verifies the request message as described in RFC 6492 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.

4.3.2. Notification to subscriber by the CA of issuance of certificate For an APNIC-hosted CA, the subscriber is notified of the issuance of the initial certificate by way of the Resource Manager. Subsequent certificate issuance is handled by APNIC's internal systems.

For a self-hosted CA, a subscriber is notified of the issuance of a new certificate by the Certificate Issuance Response message [RFC6492].

4.3.3. Notification of certificate issuance by the CA to other entities APNIC implicitly notifies all RPKI RPs when a certificate is published. These RPs will detect publication of the certificate when interacting with the RPKI repository system during periodic downloads.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance A subscriber is deemed to have accepted a certificate issued by this CA unless the subscriber 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 will be published at the repositories mentioned in Section 2.1 once issued, following the conduct described in Section 4.4.1. This will be done within 1 business day.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities See Section 4.3.3.

4.5. Key pair and certificate usage

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

4.5.1. Subscriber private key and certificate usage The certificates issued by each APNIC production CA 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.

If a subscriber delegates resources to another organization, the subscriber will issue a subordinate (CA) certificate to that organization, using the subscriber CA's private key. A subscriber also will use its private CA key to issue EE certificates for ROAs, manifests, and other RPKI-signed objects.

4.5.2. Relying party public key and certificate usage The primary relying parties in this PKI are organizations that use RPKI EE certificates to verify RPKI-signed objects. Relying parties are referred to Section 4.5.2 of RFC 6484 for additional guidance with respect to acts of reliance on RPKI certificates.

4.6. Certificate renewal

4.6.1. Circumstance for certificate renewal As per RFC 6484, a certificate will be processed for renewal based on its expiration date or a renewal request from the subscriber. The request may be implicit, a side effect of renewing a resource holding agreement, or may be explicit. If APNIC initiates the renewal process based on the certificate expiration date, then APNIC will notify the subscriber at least 4 months in advance of the expiration date. Resource certificates are set to expire 3 months after the issuance of the invoice associated with renewal of the resource holding agreement. Additionally, until the corresponding account is closed, the resource certificates for the account will be reissued periodically with new, later expiry dates, in order to ensure that the certificates remain valid.

Certificate renewal will incorporate the same public key as the previous certificate, unless the private key has been reported as compromised (see Section 4.9.1). 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 APNIC may initiate the renewal process. For an APNIC-hosted CA, only an individual with the appropriate authorization in the Resource Manager may request renewal of an RPKI certificate. For a self-hosted CA, only an individual with authorization pursuant to the subscriber's BPKI may request renewal.

4.6.3. Processing certificate renewal requests For an APNIC-hosted CA, a subscriber requests certificate renewal by contacting the APNIC helpdesk via email (helpdesk@apnic.net).

For a self-hosted CA, a subscriber requests certificate renewal by sending a Certificate Issuance Request message [RFC6492].

4.6.4. Notification of new certificate issuance to subscriber For an APNIC-hosted CA, a subscriber is notified of the issuance of a new certificate by the APNIC helpdesk.

For a self-hosted CA, a subscriber is notified of the issuance of a new certificate via the Certificate Issuance Response message, if the subscriber initiated the renewal. A subscriber can also discover a certificate renewed by APNIC through use of the List message [RFC6492].

For all CAs, if APNIC initiated the renewal process, the subscriber is notified by the posting of the renewed certificate in the repository.

4.6.5. 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 APNIC RPKI repository system, as described in Section 4.9.3.

4.6.6. Publication of the renewal certificate by the CA APNIC will publish a renewed certificate in the APNIC 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 See Section 4.3.3.

4.7. Certificate re-key

4.7.1. Circumstance for certificate re-key As per the CP [RFC6484], 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;

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

(3) an explicit request from the subscriber.

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.

4.7.2. Who may request certification of a new public key The holder of the certificate may request a re-key. In addition, APNIC may initiate a re-key based on a verified compromise report.

For an APNIC-hosted CA, only individuals who have the appropriate authorisation in the Resource Manager may request rekey.

For a self-hosted CA, only individuals who have the appropriate authorisation, per earlier registration of details in the Resource Manager under [RFC8183], may request rekey.

4.7.3. Processing certificate re-keying requests For an APNIC-hosted CA, a subscriber requests rekey by contacting the APNIC helpdesk via email (helpdesk@apnic.net).

For a self-hosted CA, a subscriber requests rekey by sending 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.

4.7.4. Notification of new certificate issuance to subscriber For an APNIC-hosted CA, a subscriber is notified of the issuance of a re-keyed certificate by the APNIC helpdesk.

For a self-hosted CA, a subscriber is notified of the issuance of a re-keyed certificate via the Certificate Issuance Response message.

4.7.5. Conduct constituting acceptance of a re-keyed certificate A subscriber is deemed to have accepted a certificate issued by this CA unless the subscriber 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

See Section 4.3.3.

4.8. Certificate modification

4.8.1. Circumstance for certificate modification

As per the CP [RFC6484], modification of a certificate occurs to implement changes to the RFC 3779 extension values or the SIA extension 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, or as a result of change of the repository publication point data.

If a subscriber is to receive a distribution of INRs in addition to a current distribution, and if the subscriber does not request that a new certificate be issued containing only these additional INRs, 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 will be revoked and a new certificate (reflecting the new distribution) issued.

4.8.2. Who may request certificate modification

The subscriber or APNIC may initiate the certificate modification process.

For an APNIC-hosted CA, only individuals who have the appropriate authorisation in the Resource Manager may request modification.

For a self-hosted CA, only individuals who have the appropriate authorisation, per earlier registration of details in the Resource Manager under RFC 8183, may request modification.

4.8.3. Processing certificate modification requests

For an APNIC-hosted CA, a subscriber requests modification by contacting the APNIC helpdesk via email (helpdesk@apnic.net).

For a self-hosted CA, a subscriber requests modification by sending a Certificate Issuance Request message. If the request contains values for the RFC 3779 extensions or SIA extensions that are different from those in the currently issued certificate, the request is interpreted as a request for certificate modification.

4.8.4. Notification of modified certificate issuance to subscriber

For an APNIC-hosted CA, a subscriber is notified of the issuance of a modified certificate by the APNIC helpdesk.

For a self-hosted CA, a subscriber is notified of the issuance of a modified certificate via the Certificate Issuance Response message.

4.8.5. Conduct constituting acceptance of modified certificate A subscriber is deemed to have accepted a certificate issued by this CA unless the subscriber explicitly requests revocation of the certificate using the procedures described in Section 4.9.3.

4.8.6. Publication of the modified certificate by the CA A re-keyed certificate will be published in the APNIC 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 See Section 4.3.3.

4.9. Certificate revocation and suspension

4.9.1. Circumstances for revocation As per the CP [RFC6484], certificates can be revoked for several reasons. Either APNIC or the subscriber 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 subscriber, 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.

4.9.2. Who can request revocation For an APNIC-hosted CA, only individuals who have the appropriate authorisation in the Resource Manager may request revocation.

For a self-hosted CA, only individuals who have the appropriate authorisation, per earlier registration of details in the Resource Manager under RFC 8183, may request revocation.

4.9.3. Procedure for revocation request For an APNIC-hosted CA, a subscriber requests revocation by contacting the APNIC helpdesk via email (helpdesk@apnic.net). The APNIC helpdesk will notify the subscriber on completion of the process.

For a self-hosted CA, a subscriber requests revocation using the Certificate Revocation Request message described in RFC 6492. The Certificate Revocation Response messages confirms receipt of the revocation request by APNIC, and indicates that APNIC will include the revoked certificate in a CRL.

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 APNIC 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 [RFC6484], 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 Each CRL contains a "Next Update" value, and a new CRL will be published at or before that time. The "Next Update" value will be set when a CRL is issued in order to signal when the next scheduled CRL will be issued.

The CAs covered by this CPS use different values:

- Offline CA: one month and one week from the moment of issuance
- Intermediate CA: one month and one week from the moment of issuance
- Production CAs: two days from the moment of issuance
- Hosted CAs: two days from the moment of issuance

As a matter of good operational practice, all CAs covered by this CPS will aim to republish and re-issue a new CRL before the next scheduled update value, to allow time to deal with any operational problems.

4.9.8. Maximum latency for CRLs A CRL will be published to the repository system within 1 business day after generation.

5. Facility, Management, and Operational Controls

5.1. Physical controls

5.1.1. Site location and construction Operations for the APNIC RPKI CAs, including the APNIC-hosted CAs, are conducted within a physically protected area of an office building owned by APNIC. This building is located at 6 Cordelia Street, South Brisbane, QLD 4101, Australia. APNIC space within this facility includes offices, meeting spaces, and a machine room. Through APNIC's machine room, APNIC remotely operates two external data centres that host the APNIC CA systems (computers and cryptographic modules).

5.1.2. Physical access APNIC CA systems are afforded physical security by virtue of being located within the data centre. Only selected APNIC staff have access to the machine room and the data centre. The APNIC staff responsible for CA operation are issued key cards that grant access to the machine room at any time. Members of the APNIC infrastructure services team are granted separate access to the data centre that houses the CA systems.

5.1.3. Power and air conditioning The external data centres that host the APNIC CA computers and cryptographic module are powered by a UPS (uninterruptible power supply) system and a backup generator system, guaranteeing at least 96 hours of power in the event of loss of municipal power. The room containing this equipment makes use of N+1 Computer Room Air Conditioning (CRAC) systems to control temperature and relative humidity.

5.1.4. Water exposures The external data centre is located at 20 Wharf St, Brisbane City, QLD. There is no history of flooding in this area of Brisbane that has reached the elevation of this level of the building.

5.1.5. Fire prevention and protection Fire suppression for the external data centre that hosts the APNIC CA computers and cryptographic modules is provided by an inert gas suppression system.

5.1.6. Media storage All media containing production software and data for the CA functions, plus audit logs, are stored within APNIC facilities or external colocation facilities. Data software on disk is backed up to a separate disk drive daily.

System backup is via storage-level snapshots, which are performed once every two hours, seven days, and four weeks. Access to the backup disks is restricted to staff who have been granted access to the external data centres. Logical access control to the disk backup is effected via user accounts restricted to staff members responsible for computer system operation.

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

5.1.8. Off-site backup APNIC 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.

5.2. Procedural controls

5.2.1. Trusted roles Three trusted roles are defined for managing the Offline CA:

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

- CA officer: no access to offline CA server. Has access to security key and pass phrase to activate HSM partition.
- Systems Engineer: performs software release and maintenance of offline CA source code.

Three trusted roles are defined for managing the Online CAs:

- CA administrator: has full access to the online CA server. Performs CA validation for CA officer. Performs CA backup recovery if required.
- CA officer: limited access to online CA server to perform re-key operations and revoke old keys.
- Systems Engineer: performs software release and maintenance of online CA source code.

5.2.2. Number of persons required per task APNIC assigns at least two individuals to each of the CA administrator and CA officer roles. There is no overlap among the individuals assigned to these roles, i.e., there are four distinct individuals staffing these two roles. The staff fulfilling these roles may be shared across the two CA groups (offline and online), but no single individual will fulfill the same role for both CAs.

5.2.3. Identification and authentication for each role For the online CAs, access is controlled via password-protected login over an SSH connection on the APNIC VPN with two-factor authentication.

The offline CA is connected to a secured network with the cryptographic module. Only individuals filling the CA administrator role have login access to the CA server and cryptographic module using a combination of physical security key and password provided by CA officer.

5.2.4. Roles requiring separation of duties The CA administrator and CA officer roles require separation of duties.

5.3. Personnel controls

5.3.1. Qualifications, experience, and clearance requirements Only full-time APNIC 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.

5.3.2. Background check procedures All APNIC staff undergo normal employment reference checks.

5.3.3. Training requirements APNIC 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. APNIC maintains records of such training and periodically reviews and enhances its training programs as necessary.

5.3.4. Retraining frequency and requirements APNIC 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.

5.3.5. Job rotation frequency and sequence There are no requirements for enforced job rotation among staff fulfilling trusted CA roles.

5.3.6. Sanctions for unauthorized actions If APNIC RPKI CA staff are determined to have performed activities inconsistent with APNIC RPKI policies and procedures, appropriate disciplinary actions will be taken.

5.3.7. Independent contractor requirements No independent contractor or consultant is used to perform APNIC 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 APNIC staff at all times when in sensitive areas.

5.3.8. Documentation supplied to personnel Training for staff assigned to a trusted CA role is primarily via mentoring. An internal wiki is maintained by APNIC staff as a further training aid.

5.4. Audit logging procedures

5.4.1. Types of events recorded Audit records are generated for the basic operations of the CA servers. Audit records 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)
- Certificate creation, modification, revocation, or renewal actions
- Key generation

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.

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

5.4.3. Retention period for audit log Audit logs are retained onsite for at least 6 months after processing.

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

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

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

5.4.7. Notification to event-causing subject [OMITTED]

5.4.8. Vulnerability assessments APNIC employs an outside firm to perform periodic vulnerability assessments for computer and network systems. These reports are provided to the APNIC Internet Security Specialist and to the APNIC Executive and Leadership Teams.

5.5. Records archival [OMITTED]

5.6. Key changeover

The offline CA's key is only changed in the event of compromise. If it is compromised, APNIC will reissue all of the certificates issued under the old key under a new key, publish a new TAL [RFC8630], and issue public notifications as to a manual TAL update being needed.

For all other CAs, key changeover follows the procedures described in RFC 6489.

5.7. Compromise and disaster recovery [OMITTED]

5.7.1. Incident and compromise handling procedures [OMITTED]

5.7.2. Computing resources, software, and/or data are corrupted [OMITTED]

5.7.3. Entity private key compromise procedures [OMITTED]

5.7.4. Business continuity capabilities after a disaster [OMITTED]

5.8. CA or RA termination

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

6.1. Key pair generation and installation

6.1.1. Key pair generation For the offline CA operated by APNIC, the key pair is generated using a hardware cryptographic module.

6.1.2. Public key delivery to certificate issuer Subscribers deliver public keys to the APNIC RPKI CA by use of the certificate provisioning protocol described in RFC 6492.

6.1.3. 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.

6.1.4. Key sizes The key sizes used in this PKI are as specified in RFC 7935.

6.1.5. Public key parameters generation and quality checking The public key algorithms and parameters used in this PKI are as specified in RFC 7935.

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

6.1.6. Key usage purposes (as per X.509 v3 key usage field) The KeyUsage extension bit values employed in RPKI certificates are specified in RFC 6487.

6.2. Private Key Protection and Cryptographic Module Engineering

Controls

6.2.1. Cryptographic module standards and controls The APNIC offline CA employs a cryptographic module evaluated under FIPS 140-2, at level 3 [FIPS].

6.2.2. Private key (n out of m) multi-person control Activation of the private key for the offline CA requires two-party control. The cryptographic modules for the offline CA are stored in a secure container. The CA administrator has the combination (or key) to the container, while the CA officer has the security key and PIN for activating the cryptographic module. Access to the private key for this CA, for key recovery purposes also requires two-party control, as described in 6.2.4 below.

Online CAs do not make use of multi-person controls.

6.2.3. Private key escrow No private key escrow procedures are required for this PKI.

6.2.4. Private key backup APNIC creates backup copies of CA private keys for both routine and disaster recovery purposes. Such keys are stored within two password-protected Luna SA Backup tokens. 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.

6.2.5. Private key archival There will be no archive of private keys by this CA.

6.2.6. Private key transfer into or from a cryptographic module The private keys for APNIC's offline 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.

6.2.7. Private key storage on cryptographic module The private keys for APNIC's offline CA are stored in the cryptographic module and will be protected from unauthorized use in accordance with the FIPS 140-2 level 3 [FIPS] requirements applicable to the module.

6.2.8. Method of activating private key Activation of the offline CA private key requires use of the CA administrator password, as well as the password used to initiate a secure connection to the cryptographic module.

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

6.2.10. Method of destroying private key When the offline CA's key is superseded, or upon cessation of operations, APNIC will destroy the old offline CA's key. 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(s) used by APNIC for the offline CA is certified under FIPS 140-2, 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 For the offline CA that is intended to be used as a Trust Anchor by relying parties, APNIC is committed to supporting the same key pair for at least five years. This may change if a new RFC is implemented that affects this process, or if the keys are compromised, which makes the CA unable to support the same key pair.

For the online CAs, there is no intended validity period.

6.4. Activation data

6.4.1. Activation data generation and installation Passwords are used to activate the cryptographic module for the offline CA. They are generated and installed in the same fashion. Each password is generated by the trusted individual serving in the CA administrator role. Each password is entered by the individual into the cryptographic module via SSH, upon module initialization. The CA officer uses the security key and PIN via a serial interface to the module to complete the activation process.

6.4.2. Activation data protection An APNIC staff member filling the CA administrator role 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 APNIC 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 APNIC operations. Access authorization uses APNIC LDAP access control, with a specific group limiting access. User authentication is based on use of tightly managed passwords. Logical separation of the CA systems from other APNIC 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 that was not acquired externally, was developed by APNIC staff (not by contractors).

APNIC software development follows an ‘agile’ methodology. All software is developed and maintained under a revision control system and releases are tagged. Code is subject to code review during development. APNIC 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 APNIC 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 APNIC LDAP access control framework. The RPKI engine is in the general APNIC LDAP access control but has a specific group limiting access.

RPKI front end is in the general APNIC LDAP access control but has a specific group limiting access. 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 APNIC 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 APNIC 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

APNIC performs all its CA operations using a secured network to prevent unauthorized access and other malicious activity. APNIC protects communications of sensitive information through the use of encryption and digital signatures. Communications are protected by at least one of TLS 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 operated by APNIC does not make use of time stamping.

7. Certificate and CRL Profiles

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

8. Compliance Audit and Other Assessments

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

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

8.1. Frequency or circumstances of assessment

Assessments are initiated at the behest of the Internet Security Specialist.

8.2. Identity/qualifications of assessor

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

8.3. Assessor's relationship to assessed entity

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

8.4. Topics covered by assessment

The external vulnerability assessment performed on APNIC IT systems covers a variety of topics, including (but not limited to) network port scanning, testing of web application interfaces, and review of user authentication and authorization mechanisms.

The internal vulnerability assessment similarly covers a variety of topics, including (but not limited to) logging and auditing, network security, and configuration management.

8.5. Actions taken as a result of deficiency

The APNIC Internet Security Specialist reviews all recommendations made by the external assessor and takes remedial actions as appropriate.

8.6. Communication of results

The external vulnerability assessment reports are provided to the APNIC Internet Security Specialist and to the APNIC Director General.

9. Other Business And Legal Matters

9.1. Fees

9.1.1. Certificate issuance or renewal fees Certificate issuance and renewal fees may be charged by APNIC. Fees are set from time to time by the Executive Council of APNIC. The current schedule of fees is published on the APNIC web site (https://www.apnic.net/about-apnic/corporate-documents/documents/membership/member-fee-schedule/).

9.1.2. Fees for other services (if applicable) [OMITTED]

9.1.3. Refund policy [OMITTED]

9.2. Financial responsibility [OMITTED]

9.3. Confidentiality of business information [OMITTED]

9.4. Privacy of personal information [OMITTED]

9.5. Intellectual property rights

APNIC's intellectual property (agreements, documents, software, databases, website, etc.) may only be used, reproduced and made available to third parties upon prior written authorisation from APNIC.

9.6. Representations and warranties [OMITTED]

9.7. Disclaimers of warranties [OMITTED]

9.8. Limitations of liability

Download of the Repository, access and use of the data contained therein, and use of the service is at the Relying Party's own risk entirely.

The subscriber is liable for all aspects of the use of the Certificate and the creation of RPKI signed objects.

APNIC is not liable for any direct or indirect damages, including but not limited to, damages to the Relying Party's business, loss of profit, damages to third parties, personal injury or damages to property, except in cases involving willful misconduct on the part of APNIC.

Relying Parties are responsible for making decisions based on the most recently published instances of RPKI signed objects contained in the Repository. APNIC is not liable for any decisions made by Relying Parties based on use of other than the most recently published instances of RPKI signed objects contained in the Repository.

Without reducing the effect of the previous paragraphs:

APNIC is not liable for non-performance or damages due to force majeure (including but not limited to industrial action, strikes, occupations and sit-ins, blockades, embargoes, governmental measures, denial of service attacks, war, revolutions or comparable situations, power failures, defects in electronic lines of communication, fire, explosions, damage caused by water, floods and earthquakes).

APNIC is not liable in the case that local legislation prohibits the use of any technical aspects of the Repository, service or the data contained therein.

Any right on the part of the Relying Party towards APNIC in connection with the download of the Repository, the service and the access and use of the data contained therein shall finally and unconditionally lapse one year from the date on which the Relying Party became aware of (or could in all fairness have been aware of) the existence of such rights and entitlements. This one-year term can only be barred or interrupted by actual legal action instituted by the Relying Party against APNIC.

9.9. Indemnities [OMITTED]

9.10. Term and termination [OMITTED]

9.11. Individual notices and communications with participants [OMITTED]

9.12. Amendments

APNIC may amend the terms of this CPS from time to time. Any amendments made to this CPS will be effective upon posting of such amendments on APNIC's website. Continued use of any service covered by this CPS by a user, subscriber, a Relying Party or a third party after the posting of any such amendment shall be deemed to be said party's or person's acceptance and acknowledgement of the amended CPS.

9.13. Dispute resolution provisions [OMITTED]

9.14. Governing law

These Terms and Conditions shall be exclusively governed by the laws of Queensland, Australia. The competent court in Queensland, Australia has exclusive jurisdiction with regard to disputes arising from these Terms and Conditions.

9.15. Compliance with applicable law

If any provision contained in the Terms and Conditions is held to be invalid by a court of law, this shall not in any way affect the validity of the remaining provisions.

9.16. Miscellaneous provisions

Anyone is able to download, access or use the Repository and the data contained therein, to the extent permitted by these Terms and Conditions and provided these Terms and Conditions are followed. By downloading the Repository and accessing and using the data contained therein, the Relying Party agrees to be bound by these Terms and Conditions.

Relying Parties are permitted to download the Repository and to access the service and use the data contained therein, in order to validate Certificates, CRLs and RPKI-signed objects.

Download of the Repository, access to or use of the service and data contained therein for any other purpose, including but not limited to identification purposes, advertising, direct marketing, marketing research or similar purposes, is not permitted.

The use of the Certificate does not support claims of alleged “ownership” of Internet number resources. Internet number resources registered by APNIC are subject to and exclusively governed by the policies adopted by the APNIC community.

Relying Parties should always check revocation information when using a Certificate or RPKI-signed object and should always ensure that they are using the latest version of the Repository, which is updated every 24 hours. The Repository will be available for download on a best effort basis and APNIC may suspend its operation or liability to the Relying Party for technical, legal, anti-abuse or any other reasons within the scope of managing the operations of the Repository.

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

9.17. Other provisions [OMITTED]

10. References

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

[RFC6484] 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.

[RFC6487] Huston, G., Loomans, R., Michaelson, G., “A Profile for X.509 PKIX Resource Certificates”, work in progress, June 2007.

[RFC6487] Huston, G., Loomans, R., Michaelson, G., “A Profile for X.509 PKIX Resource Certificates”.

[RFC6492] G. Houston, R. Loomans, B. Ellacott, R. Austein, “A Protocol for Provisioning Resource Certificates,”

[BGP4] Y. Rekhter, T. Li (editors), A Border Gateway Protocol 4 (BGP-4). IETF RFC4271, 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.