AMERICAN REGISTRY FOR INTERNET NUMBERS, LTD.

CERTIFICATION PRACTICE STATEMENT FOR RESOURCE CERTIFICATION

1. INTRODUCTION

This document is the Certification Practice Statement for Resource Certification (CPS) of ARIN. It describes the practices employed by ARIN Certification Authority (CA) in the Internet IP Address and Autonomous System (AS) Number Public Key Infrastructure (PKI). These practices are defined in accordance with the requirements of the Certificate Policy (CP, [RFC 3647]) 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 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 this PKI for any other purpose is a violation of this CPS and relying parties should reject such uses.

Note: This CPS is based on the template specified in RFC 3647. Several 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].

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 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

1.2. Document name and identification

The name of this document is “ARIN Certification Practice Statement for Resource Certification”.

1.3. PKI participants

Note: In a PKI, the term “subscriber” refers to an individual or organization that is a subject of a certificate issued by a CA. The term is used in this fashion throughout this document, without qualification, and should not be confused with the networking use of the term to refer to an individual or organization that receives service from a Local Internet Registry (LIR)/ISP. Thus, in this PKI, the term “subscriber” can refer both to LIRs/ISPs, which can be subscribers of Regional Internet Registries (RIRs), and other LIRs, and 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

ARIN operates three CAs for the RPKI: one is designated “offline”, one is designated “production” that includes non-hosted CAs, and one for several hosted CAs. All three are equivalent so they may be described as a single CA for the purpose of this document.

The offline CA is the top-level CA for ARIN portion of the RPKI. It provides a secure revocation and recovery capability in case the production CA is compromised or becomes unavailable. Thus, this CA issues certificates only in 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 ARIN members, to which address space or AS numbers have been allocated. In the future, the production CA also may be used to communicate with members who prefer to run their own CAs – referred as non- hosted CAs.

In addition, ARIN offers a hosted CA service to its members. These CAs are designated as “hosted CAs”.

1.3.2. Registration authorities

There is no registration authority (RA) for either the offline or the production CA operating under this CPS. The former needs no RA capability because it issues certificates only to the production CA. The production CA relies upon certificates issued by ARIN Business PKI (BPKI) to identify individuals authorized to request certificates under the RPKI. ARIN already establishes a business relationship with each subscriber (ARIN member) and assumes responsibility for allocating and tracking the current allocation of address space and AS numbers. Since ARIN operates the BPKI CA, there is no distinct RA for the RPKI.

1.3.3. 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 and Internet Service Providers (ISPs).

1.3.4. 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 ISPs, multi-homed organizations exchanging Border Gateway Protocol (BGP) traffic with ISPs and subscribers who have received an allocation of address space from an ISP but want to authorize one (or another) 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.

1.3.5. Other participants

ARIN operates a repository that holds certificates, CRLs, 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 solely for authorization in support of validation of claims of current holdings of address space and/or AS numbers, e.g., for routing security. Regarding 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 reasonably 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, may also be permitted, in writing, under this policy in ARIN’s absolute and sole discretion.

1.4.2. Prohibited certificate uses

Any uses other than those described in Section 1.4.1 are strictly prohibited and may be considered a violation of this CPS and/or any agreement between ARIN and an entity using ARIN’s RPKI services.

1.5. Policy administration

1.5.1. Organization administering the document

Since this CPS describes the implementation of the “offline CA”, “production CA” and “hosted CAs” maintained by ARIN, this CPS is also administered by ARIN. However, approval procedures described in section 1.5.3-4 apply.

Whenever the implementation is changed by ARIN, this CPS will be modified and republished by ARIN. When this happens, this will be announced by ARIN through the appropriate communication channels.

1.5.2. Contact person

The RPKI CPS point of contact is the Chief Operating Officer for ARIN, who may be reached at PO Box 232290 Centreville, VA 20120 USA.

1.5.3. Person determining CPS suitability for the policy

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 during the validity period of 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.

1.5.4. CPS approval procedures

An ARIN certificate policy (CP) outlining important decisions, e.g., related to validity times, revocation, re-issuance and access to the services involved is currently available at http://www.arin.net/resources/rpki/cps.pdf. The implementation of the various CAs (“offline”, “production”, and “hosted CAs”) will reflect the CP.

This CPS and the CP is subject to future changes by ARIN. ARIN will update its implementation and this CPS where necessary for consistency with any future changes to the CP.

1.6. Definitions and acronyms

In addition to capitalized terms defined within the context of this CPS, the following **bolded** terms have the following meanings:

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. The CP for the RPKI is [RFC6484].

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

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

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

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

- IP version 4 addresses,
- IP version 6 addresses, and
- Identifiers used in Internet inter-domain routing, currently Border Gateway Protocol-4 ASNs.

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

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

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

RPKI-signed object
An RPKI-signed object is a digitally signed data object (other than a certificate or CRL) declared to be such an object by a Standards Track RFC. An RPKI-signed object can be validated using certificates issued under this PKI. The content and format of these data constructs depend on the context in which validation of claims of current holdings of INRs takes place. Examples of these objects are repository manifests [RFC6486] and Route Origin Authorizations (ROAs)[RFC6482].

CA Certificate Authority. A CA is an entity that issues digital certificates for use by other parties. A CA may issue CA certificates to subordinate CAs. Thus, a tree structure of CAs can be created, often dubbed Public Key Infrastructure (PKI). ARIN operates three levels of CAs in the PKI hierarchy, covered in this CPS:

(i) Offline ARIN offline CA. This CA is kept offline for security reasons when not in use and acts as the top in the hierarchy. For the moment this CA is making itself available as a Trust Anchor as described in [draft-TA-version4] In the future this CA may become subordinate to a top-level single Trust Anchor CA that will issue certificates to all RIRs.

(ii) ARIN production non-hosted CA. This CA is used daily to issue certificates to subordinate member CAs portion of the area covered by ARIN Registry.

(iii) ARIN hosted CA. This CA is used where ARIN performs the certificate issuance from beginning to end - hosting the private key on ARIN’s HSM. ARIN exercises a certificate at the subscriber’s direction using ARIN’s code. For example, the subscriber requests ARIN to create a ROA and sign it with the resource certificate. ARIN takes the private key for that user, creates a ROA, and signs it with the private key associated with that certificate.

ARIN Online Portal

The public online portal provided by ARIN to its members allows them access to various member services, including the hosted member CA service. The portal is also used to access the ARIN Production CA by specific users as described later in this CPS.

ARIN Member

For purposes of this CPS, ARIN Member shall mean a registrant of Internet number resources (i) that are covered by either a Registration Services Agreement (“RSA”) or a Legacy Registration Services Agreement (“LRSA”) and (ii) for which the entity is eligible for a resource certificate issued by a CA.

Resource Certification

The security framework offered under this CPS to assist in verifying the association between Internet number resource holders and their Internet resources.

Resource Certification Services

The services offered by ARIN with respect to Resource Certification under this CPS and/or any other Resource Certification Terms, as applicable.

Resource Certification Terms

The terms and conditions under which ARIN provides the Resource Certification Services (or any part thereof), including this CPS, the Resource Certification Terms of Service Agreement, the Resource Certification Relying Party Agreement, and other policies and procedures that ARIN may adopt from time to time applicable to Resource Certification or any Resource Certification Services the “RPKI Policies”) that are or will be published by ARIN on ARIN’s Website.

ROA or 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.

RP or Relying Party

Relying parties are any organization (human or system) that seeks to use digital objects published under the RPKI for validation purposes.

TA or Trust Anchor

The top CA certificate in the chain that is used for validation. Relying Parties choose which CA certificate they trust as being the top of the validation tree. Relying Parties may choose to trust more than one TA.

End-User

An organization/user connected to the Internet that provides or receives services from an ISP.

Hosted CA

An organization that allows another organization (ARIN in this case) to hold private keys associated with their Resource Certificate and any other certificates that could be generated as part of the RPKI system.

Non-Hosted CA

An ISP/end-user who receives Internet resources from ARIN that elects to operate their own CA within the RPKI system.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

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 ARIN RPKI CA publishes certificates, CRLs, and other signed objects accessible via RSYNC at rsync://rpki.arin.net/repository.

2.2. Publication of certification information

ARIN uploads certificates and CRLs issued by it to a local repository system that operates as part of a worldwide distributed system of repositories.

2.3. Time or Frequency of Publication

The following standards exist for location, publication times and frequency:

Offline CA: rsync://rpki.arin.net/repository/arin-rpki-ta.cer

Online CA: located under rsync://rpki.net/repository/
Hosted CAs are in subdirectories under rsync://rpki.arin.net/repository.

A certificate will be published within one (1) business day after issuance.

ARIN CA will publish its CRL prior to the next Scheduled Update value in the scheduled CRL previously issued by the CA. Within 1 business day of effecting revocation, the CA will publish a CRL with an entry for the revoked certificate.

2.4. Access controls on repositories

Access to the repository system, for modification of entries, must be controlled to prevent denial of service attacks and unauthorized modification. All data (certificates, CRLs and ROAs) uploaded to a repository are digitally signed and limited by generation by systems running the Production and Hosted CAs. Updates to the repository system must be validated to ensure that the data being added or replaced is authorized. This document does not define the means by which updates are verified but use of the PKI itself to validate updates is anticipated.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of Names

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

3.1.2. Need for names to be meaningful

The Subject name in each certificate SHOULD NOT be "meaningful", in the conventional, human-readable sense. The rationale here is that these certificates are used for authorization in support of applications that make use of attestations of INR holdings. They are not used to identify subjects.

3.1.3. Anonymity or pseudonymity of subscribers

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

3.1.4. Rules for interpreting various name forms

None

3.1.5. Uniqueness of names

Subject names may be unique among the certificates that ARIN issues. Although it is desirable that these Subject names be unique throughout the PKI, to facilitate certificate path discovery, such uniqueness is neither mandated nor enforced through technical means.

3.1.6. Recognition, authentication, and role of trademarks

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

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

For the Offline CA, proof of possession of the private keys used for the self-signed ETA and RTA certificates may be determined internally.

For the Production CA that acts as subscriber of the Offline CA, possession of the private keys is affected via the procedures used to generate the key pairs for each of these CAs. Specifically, ARIN uses a hardware security module to generate the key pairs for each of these CAs and thus the private key will be associated with the public key in the certificate issued by each of these CAs.

ARIN also accepts certificate requests via the protocol described in[up/down] for non-hosted CAs. 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.

3.2.2. Authentication of organization identity

For non-hosted CAs: Certificates issued under this PKI do not attest to the organizational identity of resource holders, except for Registries. Certificates are issued to resource holders in a fashion that reflects the accuracy of allocations as represented in ARIN records at the time of issuance of the certificate. Specifically, a BPKI certificate used to authenticate a certificate request serves as a link to the ARIN 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.

For hosted CAs: ARIN can map a logged in user to a specific organization, and the organization can be mapped to a specific public key. Thus, ARIN can map these public keys to a specific set of resources as reflected at the time in ARIN’s records.

3.2.3. Authentication of individual identity

For non-hosted CAs: Certificates issued under this PKI do not attest to the individual identity of a resource holder. However, ARIN maintains contact information as provided by a resource holder for each resource holder in support of certificate renewal, re-key, or revocation, via the BPKI.

ARIN BPKI issues certificates that are used to identify individuals who represent ARIN members that are address space (or AS number) holders.

For hosted CAs: Individual identity is delegated to the ARIN Online user that is associated with that organization and a public key. These users are associated with a private key that is stored locally on the user’s computer. Any subsequent action using RPKI must be signed with that key before any action is performed within the RPKI system.

3.2.4. Non-verified subscriber information

Non-verified subscriber data is not included in certificates issued under this CPS.

3.2.5. Validation of authority

Access to the Offline CA is restricted to the Operations Manager that has access to the Unix account on the server. In addition, the hardware security modules (HSMs) are protected by keys only held by ARIN Security Officers (who are different than the Engineering staff which is comprised of ARIN’s operations, quality assurance, and development teams).

Access to the production CA is restricted to users via ARIN Online. All actions performed by Hosted CA users are both signed locally and subsequently logged via non-repudiable logging.

For non-hosted CAs, only an individual to whom a BPKI certificate has been issued may request issuance of an RPKI certificate. Each certificate issuance request is verified using the BPKI.

3.2.6. Criteria for interoperation

The RPKI is neither intended nor designed to interoperate with any other PKI. However, for non-hosted CAs, ARIN operates a BPKI [cps business-pki] that is used to authenticate members and to enable them to manage their resource allocations. The RPKI relies on this BPKI to authenticate subscribers who make certificate requests, revocation requests, etc.

3.3. Identification and authentication for re-key requests

3.3.1. Identification and authentication for routine re-key

For Offline CA and Production CA, the same identification and authentication mechanisms apply as described in section 3.2.3.

For hosted CAs, routine re-keys are automated by the software and thus no explicit authentication is required. A routine re-key is initiated whenever the current key for the hosted CA is older than 20 years.

For non-hosted CAs that use up/down, routine re-key is affected 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.

3.3.2. Identification and authentication for re-key after revocation

For Offline and Production CAs, the old key can be revoked as the final steps in a key roll over algorithm <rekey draft here> after the new key has been activated.

For non-hosted CAs, re-key after revocation is affected 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.

3.4. Identification and authentication for revocation request

For hosted CAs, user actions in the interface will result in revocation of EE certificates used for objects such as ROAs.

For non-hosted CAs, a user 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 ARIN 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.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Who can submit a certificate application?

Any entity enrolled under ARIN RSA or LRSA and who have entered and/or accepted ARIN's terms and conditions with respect to RPKI certification, as required by ARIN, may request a certificate under the RPKI.

4.1.2. Enrollment process and responsibilities

For the Offline CA, the operations manager and security officers can configure and initialize the CA on a server controlled by ARIN.

For the Production CA, the operations manager can install and initialize the application and initialize the Production CA.

For hosted CAs: Members may use a member CA hosted by ARIN as part of the ARIN Online member portal. In order to activate the hosted CA an admin user must log in, select the 'certification' portion of the application and upload a public key that will be used in all future RPKI transactions. The user that has the certification role will then be able to click the certification link in ARIN Online. After activation, a largely automated hosted CA will be created. Authentication and authorization for further automated processes should be considered transitive from the moment that user opted-in and activated the hosted CA as described here.

4.2. Certificate application processing

For hosted CAs a new, initial, CA certificate is requested by the system automatically when the authorized user chooses to opt-in.

For non-hosted CAs: An ARIN 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 ARIN BPKI. ARIN 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.

4.2.1. Performing identification and authentication functions

See section 3.2.3.

4.2.2. Approval or rejection of certificate applications

The production CA will issue certificates to member CAs. The production CA will include all resources covered under RSA or LRSA known by ARIN for the member in the member CA certificate.

4.2.3. Time to process certificate applications

ARIN expects to issue a certificate attesting to a resource allocation within one (1) business day after approval of the allocation.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

In the non-hosted CA model, the subscriber generates a draft certificate using the PKCS #10 format, as profiled in [recertificate-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.

In the hosted CA scenario, the subscriber directs ARIN to generate and sign the certificate.

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

Publication of a certificate in the repository operated by ARIN is the means by which a subscriber is notified of certificate issuance. This procedure is employed by all CAs covered by this CPS.

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

Publication of a certificate in the repository operated by ARIN is the means by which other entities other are notified of certificate issuance.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

A subscriber is presumed to have accepted a certificate issued by the Production CA and published in ARIN repository unless the subscriber otherwise provides written notice to ARIN.

4.4.2. Publication of the certificate by the CA

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

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

Same as section 4.3.3.

4.5. Key pair and certificate usage

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

4.5.1. Subscriber private key and certificate usage

The hosted CAs receive CA certificates from the Production CA. This means that these certificates could in principle be used to issue subordinate CA certificates. However, the hosted system does not provide this functionality. The hosted CA certificates will only be used (by the system) to issue EE certificates used for signed objects (such as ROAs) and manifests.

The non-hosted CA must create their own private keys and manage them according to its CPS within its own facility.

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 [RFC6484] for additional guidance with respect to acts of reliance on RPKI certificates.

4.6. Certificate renewal

Note that the hosted CAs do not issue CA certificates to subordinate CAs and there is no need for certificate renewal for EE certificates used for signed objects. However, they are mentioned in this section as subordinates of, and bound to, the ARIN Production CA.

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 certificate Subject. The request may be implicit, a side effect of renewing a resource holding agreement, or explicit. If ARIN initiates the renewal process based on the certificate expiration date, then ARIN will notify the subscriber at least one month in advance of the expiration date. The validity interval of the new (renewed) certificate will overlap that of the previous certificate by one month 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 (see Section 4.9.1). If a new key pair is being used, the stipulations of Section 4.7 will apply.

For non-hosted CAs: When new IPv4, IPv6, or ASN resources are associated with a member, the up/down protocol will be used to notify the subscriber of the change.

4.6.2. Who may request renewal?

The subscriber or ARIN may initiate the renewal process. For hosted CAs, this is fully automated.

For non-hosted CAs, the subscriber may initiate the renewal process. For the case of the certificate holder, only an individual to whom a BPKI certificate has been issued may request renewal of an RPKI certificate. Each certificate issuance request is verified using the BPKI.

For the Production CA, ARIN staff with the Production CA administrator role can request renewal from the Offline CA.

For the Offline CA, resources may have to be added to the self-signed RTA. ARIN staff with the appropriate role may perform this action.

4.6.3. Processing certificate renewal requests

The same stipulations listed in section 4.2.2 apply here.

4.6.4. Notification of new certificate issuance to subscriber

See 4.3.2.

4.6.5. Conduct constituting acceptance of a renewal certificate

See 4.4.1.

4.6.6. Publication of the renewal certificate by the CA

Both the Offline CA and Production CA will publish renewed subordinate CA certificates within 1 business day after issuance.

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

See 4.3.2.

4.7. Certificate re-key

Note that the hosted CAs do not issue CA certificates to subordinate CAs and there is no need for certificate re-key for EE certificates used for signed objects. However, they are mentioned in this section as subordinates of, and bound to, ARIN Production CA.

Non-hosted CAs will be notified of the re-key via the up/down protocol.

4.7.1. Circumstance for certificate re-key

As per RFC 6484, re-key of a certificate will be performed only when requested or based on:

a) knowledge or suspicion of compromise or loss of the associated private key, or
b) the expiration of the cryptographic lifetime of the associated key pair.
c) 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 or loss of the associated private key, then the previous certificate will be revoked.

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

4.7.2. Who may request certification of a new public key?

For the hosted CAs, an automated key roll over is performed when the key has been in use for ten (10) years. Authentication and authorization for this is considered transitive from opt-in (see Section 4.1.2).

For non-hosted CAs, the holder of the certificate may request a re-key. In addition, ARIN may initiate a re-key based on a verified compromise report. If the Subscriber (certificate Subject) requests the re-key, authentication is affected using the ARIN BPKI.

For ARIN Production CA, a manual key roll-over is planned to be performed every twenty
(20) years. This manual roll-over can be initiated by ARIN staff in the Production CA administration role.

4.7.3. Processing certificate re-keying requests

The same stipulations listed in section 4.3 apply here.

4.7.4. Notification of new certificate issuance to subscriber

See 4.3.2.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

See 4.4.1.

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

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

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

See 4.3.3.

4.8. Certificate modification

4.8.1. Circumstance for certificate modification

Certificate modification is not applicable to the CAs described here. Renewal is used when new resources may be certified, or a new validity time is applicable, as described in Section 4.6.

4.8.2. Who May Request Certificate Modification?

The subscriber or ARIN may initiate the certificate modification process. Only users linked to the org as Admin, Tech or routing POC can make the request.

4.8.3. Processing Certificate Modification Requests

Certificate modification takes place during the addition or removal of resources. Privileged users may also make a certificate modification request by contacting the ARIN Helpdesk.

4.8.4. Notification of Modified Certificate Issuance to Subscriber

Users are notified with a message on the user dashboard interface on ARIN Online when a certificate modification is completed.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

When a modified certificate is issued, ARIN will publish it to the repository and notify the subscriber. See Section 4.4.1.

4.8.6. Publication of the Modified Certificate by the CA

Certificates will be published in the Repository system within one (1) business day of being issued by this CA. See Section 4.4.2

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

See section 4.4.3

4.9. Certificate revocation and suspension

4.9.1. Circumstances for revocation

Certificates can be revoked for several reasons, including, without limitation, the following:

(i) a signed object needs to be invalidated.

(ii) one or more listed resources are no longer associated with the member.

(iii) as the last steps when doing a planned re-key (clean up); and

(iv) as the last steps when doing an unplanned re-key because of a loss or compromise of the old key.

4.9.2. Who can request revocation?

A hosted CA’s users cannot request revocation of their CA certificate as they have no way of knowing or suspecting compromise or loss of the private keys in the system that is hosted by ARIN for them. ARIN staff can request revocation in this case. The other circumstances for revocation are managed automatically by the system.

For non-hosted CAs, the certificate holder or ARIN may request a revocation. A Subscriber requests certificate revocation using the Certificate Revocation Request message described in [up/down].

For the Production CA, ARIN may manually request revocation of the old CA certificate as soon as a key roll over has been performed. Other circumstances for revocation, most notably EE certificates used for manifests, are managed by the system.

4.9.3. Procedure for revocation request

For the Production CA: When one or more of the resources are no longer associated with a member, the Production CA will:

(i) re-issue a new certificate, minus the lost resources, but maintaining all other properties,
(ii) publish the new certificate using the same publication point as before, thus replacing the old certificate, and
(iii) revoke any non-expired certificates held by the member CA that lists the lost resources, thus invalidating any signed objects, such as ROAs that refer to these resources.

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

4.9.4. Revocation request grace period

Any party that can identify the need for revocation that is not already handled by the system, or its operators must notify ARIN within one (1) business day of discovery of the need for revocation.

4.9.5. Time within which CA must process the revocation request

ARIN will process a revocation request within one (1) business day of receipt and validation of the request.

4.9.6. Revocation checking requirement for relying parties

As per 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 will carry a next Scheduled Update value and a new CRL will be published at or before that time. ARIN will set the next Scheduled Update value when it issues a CRL to signal when the next scheduled CRL will be issued. The CAs covered by this CPS use different values:

Six (6) months from the moment of Offline CA: issuance Production CA/non-One (1) business day from the moment of hosted CAs: issuance One (1) business day from the moment of Hosted CAs: issuance

All CAs covered by this CPS will strive to republish and re-issue a new CRL before the next Scheduled Update value in time to deal with any operational problems.

The values listed here may be used by relying parties to determine the need to obtain an updated CRL. This means that it is possible that a revocation by the Offline CA may go unnoticed for three months. A revoked ROA for a hosted member CA may not be noticed for one (1) business day. The values here should be regarded as a compromise between various aspects: operational burden of resigning (for Offline CA), time needed to be able to do an emergency restore, efficiency of caching in the global RPKI, and propagation time of revocation in the global RPKI.

4.9.8. Maximum latency for CRLs

A CRL will be posted to the repository system as soon as reasonably practicable after generation.

4.9.9. On-line revocation/status checking availability [OMITTED]

4.9.10. On-line revocation checking requirements [OMITTED]

4.9.11. Other forms of revocation advertisements available [OMITTED]

4.9.12. Special requirements re key compromise [OMITTED]

4.9.13. Circumstances for suspension [OMITTED]

4.9.14. Who can request suspension [OMITTED]

4.9.15. Procedure for suspension request [OMITTED]

4.9.16. Limits on suspension period [OMITTED]

4.10. Certificate status services

ARIN does not support the Online Certificate Status Protocol (OCSP) or the Server-based Certificate Validation Protocol (SCVP). ARIN issues CRLs.

4.10.1. Operational characteristics [OMITTED]

4.10.2. Service availability [OMITTED]

4.10.3. Optional features [OMITTED]

4.11. End of Subscription [OMITTED]

4.12. Key escrow and recovery [OMITTED]

4.12.1. Key escrow and recovery policy and practices [OMITTED]

4.12.2. Session key encapsulation and recovery policy and practices [OMITTED]

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical controls

5.1.1. Site location and construction

For the Offline CA, operations are conducted within a physically protected area of an office building in which ARIN is a tenant. This building is in Chantilly VA, USA. ARIN leased space within the Chantilly VA facility includes offices, meeting spaces, and one machine room. A disaster recovery site which replicates all functions performed at ARIN’s office is located at a separate location.

For the Production CA and hosted member CAs, core cryptographic operations are performed by two machines physically located at an Equinix colocation facility in Ashburn VA USA.

5.1.2. Physical access

For the Offline, Hosted and Production CAs, physical access is restricted to ARIN operations staff and senior engineering management. The access system relies on key code access and card key access. Each instance of access to the restricted areas is logged on ARIN’s access system.

In the Equinix colocation facility, biometric scan, card key access and a numeric code are required. The systems are located in a cage dedicated to ARIN only. CCTV is in operation and recordings are kept for at least one (1) week.

For the disaster recovery site, operations staff may request access for themselves. Operations management may request access for others. The server is physically located in a locked cage. The racks are housed in a special suite dedicated to ARIN only. Only staff of the disaster recovery site can open the cage for ARIN and access is logged by the disaster recovery site. Within the cage, the HSMS are in locked racks that require two physical sets of keys that are held by separate personnel.

5.1.3. Power and air conditioning

The offline CA server is in an air-conditioned server room in the ARIN office building. Power outages are not expected to have any impact on this CA since it is kept offline when not in use.

The production and hosted CA’s servers at the Equinix colocation facility are in an air-conditioned server rooms. The Equinix Colocation facility, as stipulated in the contracted service agreement has UPS systems to overcome immediate power failures, and generator capacity to maintain power with enough fuel to cover for reasonable arrival of more fuel and/or restoration of power from the utility.

For the disaster recovery site, power consumption and air conditioning are monitored. The disaster recovery site is required to have a UPS to overcome immediate power failures, and a generator with enough fuel to cover for arrival of more fuel and/or restoration of power from the utility.

5.1.4. Water Exposures

The ARIN Office space and the Equinix Colocation facility in Ashburn VA are located in areas at no risk of flooding.

5.1.5. Fire prevention and protection

The ARIN server room used by the Offline, Production, and Hosted CAs has fire-extinguishing equipment. The server room is monitored. In the event of an alarm, the security company will call the local fire company.

The disaster recovery facility used by the CAs has fire-extinguishing equipment. The server room is monitored. In the event of an alarm, the security company will call the local fire company.

5.1.6. Media storage

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

5.1.7. Waste disposal

Sensitive documents and materials associated with the 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 with the manufacturer's guidance prior to disposal.

5.1.8. Off-site backup

ARIN performs regular, offsite backups of critical system data, audit log data, and other information via network-accessible storage. Updates made at ARIN's office are immediately reflected at ARIN's disaster recovery site.

5.2. Procedural controls

5.2.1. Trusted roles

Two trusted roles are defined for managing ARIN RPKI CAs:

(i) Systems administrator: has access to the CA server.
(ii) Security Officers: have access to the multi-part keys to the HSM.

5.2.2. Number of persons required per task

ARIN 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 Section 4.2.1. 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.

5.2.3. Identification and authentication for each role

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

The offline CA server is a computer stored with the offline CA cryptographic module in a secure container. Only individuals filling the CA system administrator role have physical access to the server and cryptographic module for this CA. Only individuals filling the CA system administrator role have logical access to the CA server and cryptographic modules.

5.2.4. Roles requiring separation of duties

The Systems Administrator and Chief Operating Officer roles require separation of duties.

5.3. Personnel controls

5.3.1. Qualifications, experience, and clearance requirements

Only full-time ARIN staff may fulfill the trusted roles described in Section 4.2.1. 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 ARIN staff undergo normal employment reference checks.

5.3.3. Training requirements

ARIN provides its CA staff with training upon assignment to a CA role as well as on-the-job training. ARIN maintains records of such training and periodically reviews and modifies its training programs as ARIN determines to be necessary.

5.3.4. Retraining frequency and requirements

ARIN provides refresher training and updates for CA personnel to the extent and frequency as ARIN determines to be necessary.

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 ARIN RPKI CA staff are determined to have performed activities inconsistent with ARIN RPKI policies and procedures, ARIN will take disciplinary actions as ARIN determines to be appropriate.

5.3.7. Independent contractor requirements

No independent contractor or consultant is used to perform ARIN RPKICA trusted roles. Contractors who are needed to perform any maintenance functions on CA servers or cryptographic modules must be escorted and directly always supervised by ARIN staff when in sensitive areas.

Independent contractors and consultants may be a part of the development team, but never constituting over 60% of the total team.

5.3.8. Documentation supplied to personnel

Training for staff assigned to a trusted CA role is primarily via mentoring. An internal document system is maintained by ARIN 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, and summary content data relating to the event. Messages requesting CA actions, i.e., certificate requests and certificate revocation requests, are logged via the HSM for non-repudiable verification. 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, ARIN reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within ARIN CA and RA systems.

5.4.3. Retention period for audit log

Audit logs are retained onsite for at least six (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 Section 4.1.7 apply to audit logs and extend the retention to two (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

ARIN employs an outside firm to perform periodic vulnerability assessments for computer and network systems. These reports are provided to ARIN’s security managers and to ARIN’s Chief Operating Officer.

5.5. Records archival [OMITTED]

5.5.1. Types of records archived [OMITTED]

5.5.2. Retention period for archive [OMITTED]

5.5.3. Protection of archive [OMITTED]

5.5.4. Archive backup procedures [OMITTED]

5.5.5. Requirements for time stamping of records [OMITTED]

5.5.6. Archive collection system (internal or external) [OMITTED]

5.5.7. Procedures to obtain and verify archive information [OMITTED]

5.6. Key changeover

The ARIN production CA key pair changes on a scheduled basis. In anticipation of this re-key activity, ARIN reissues all the certificates issued under the old key prior to expiration of the old certificate. ARIN then creates a new key pair and acquires and publishes a new certificate containing the new public key, a minimum of one (1) week in advance of the scheduled re-key. 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.

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

ARIN has been granted sole authority by IANA to manage allocation of IP address space and AS number resources in the North American region. ARIN 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 ARIN.

6.1. Key pair generation and installation

6.1.1. Key pair generation

For the production and CAs operated by ARIN, key pairs are generated using a hardware cryptographic module. The module used for this purpose is certified as complying with FIPS 140-2 level 4. The hardware cryptographic module employed for this process is provided by IBM.

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

6.1.2. Private key delivery to subscriber

Private keys cannot be extracted from the HSM in unencrypted form. The Offline CA and Production CA only require the public key from their subscribers. The hosted CAs have no subscribers.

6.1.3. Public key delivery to certificate issuer

For the Offline CA a custom mechanism has been developed to transfer certificate sign requests and/or revocation requests that include the Production CA public key hash. Since the Offline CA is not connected to a network, the transfer is performed via files on removable storage.

6.1.4. CA public key delivery to relying parties

For the production CA and hosted CAs, public keys are included in CA and EE certificate issued by these CAs. The keys are delivered to relying parties by publication of the CA certificates and signed objects that include EE certificates (ROAs and manifests) to the repository.

For the Offline CA, the trust anchor described in the [TA draft] is used to publish the RTA certificates. The self-signed RTA that includes the RTA public key will be made available for relying parties out of band using the ARIN Online site once consent is given with the relying party agreement.

6.1.5. Key sizes

The CAs covered by this CPS use a 2048 RSA key for all keys, including keys using EE certificates.

6.1.6. Public key parameters generation and quality checking

The HSMs used by ARIN’s CAs were certified as complying with FIPS140-2 level 4. The details of the key generation implementation used by these HSMs are not known by ARIN.

Subscribers using up/down are responsible for key pair generation and are responsible for performing checks on the quality of their key pairs. ARIN is not responsible for performing such checks for subscribers.

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

The Key usage extension bit values are consistent with RFC 5280. For ARIN’s CA certificates, the keyCertSign and cRLSign bits are set TRUE. All other bits (including digital Signature) are set FALSE, and the extension is marked critical.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards and controls

The Offline CA employs a cryptographic module evaluated under FIPS140-2 at level 4 requiring 3 of 6 security officers to be present for key pair generation and signing operations.

The Production CA and hosted CAs employ cryptographic modules evaluated under FIPS 140-2 at Security Level 4.

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

Activation of the private key for offline CA requires three-person control. The cryptographic module for the offline CA is stored in a secure container. Six separate security officers have the combination (or key) to the container. Access to the private key for this CA, for key recovery purposes also requires three of six-person control, as further described in Section 5.2.4.

6.2.3. Private key escrow

No private key escrow procedures are provided for this PKI.

6.2.4. Private key backup

For all CAs covered by this CPS, the keys containing the partial keys and other necessary information are copied and stored in three separate safes at the disaster recovery site. Access to the safes is controlled by the security officers and escorted by members of the operations team. Any access by the Security Officers to the access-controlled disaster recovery site is logged.

6.2.5. Private key archival

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

6.2.6. Private key transfer into or from a cryptographic module

The private keys for ARIN's CA are generated by the cryptographic module specified in Section 5.2.1. 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 ARIN'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])

6.2.8. Method of activating private key

Activation of either the production or offline CA private key requires three security officers represented by individual senior staff as described in 4.1.2.

6.2.9. 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 Section 4.1.

6.2.10. Method of destroying private key

When either the offline or production CA keys are superseded, or upon cessation of operations, ARIN will destroy the old CA private keys. When keys are no longer in use they are deleted from the disk. Since they were encrypted, no additional action is taken to zero the bites or purge them from backups.

6.2.11. Cryptographic Module Rating

The cryptographic module(s) used by ARIN for the offline, production, and hosted RPKI CAs are certified under FIPS 140-2, at level 4 [FIPS].

6.3. Other aspects of key pair management

6.3.1. Public key archival

There is no archive of public keys stored in ARIN’s system.

6.3.2. Certificate operational periods and key pair usage periods

For the Offline CA, the RTA key pairs have an intended maximum validity on or before September 18, 2022, after which it is intended that a re-key is performed, and the Offline CA is changed to act as a normal CA under a TA managed by the IANA.

For the Production and hosted CAs, key pairs have an intended validity interval of 10 years.

6.4. Activation data

6.4.1. Activation data generation and installation

For the Offline CAs, the parts of the master key that protect the internal key and encrypted keys on disk were generated following the procedures for the HSM. The non-public portions of the master key will be distributed among the security officers described in section 4.1.2.

6.4.2. Activation data protection

ARIN staff members filling the trusted roles for a CA stores the cryptographic module secret he/she uses to perform the operations associated with the role in an offsite location.

6.4.3. Other aspects of activation data

None

6.5. Computer security controls

The systems are rebuilt from the distribution media at each key signing ceremony. The Offline CA is kept offline when not in use. It is only switched on when in use and is never connected to any network. All data (requests, responses, backups) are transferred using empty USB sticks. Production CA are behind a segmented network with restricted access control and is available via a proxy system to the Internet. A network security system continuously monitors traffic.

The Offline CA is kept offline when not in use. It is only switched on when in use and not connected to any network. All data (requests, responses, backups) are transferred using otherwise empty USB flash drives.

The Production and hosted CAs are operated on machines within ARIN’s internal network. The user interface is made available through a firewall that load balances requests to different backend systems that then delegate requests for the certification section only to back-end machines.

6.6. Life cycle technical controls

6.6.1. System development controls

CA system software not acquired externally, was developed by ARIN staff and contractors.

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

ARIN uses the same access policy for the servers used to run the Offline CA, Production CAs, and hosted CAs: only staff from the responsible departments have SSH access. SSH access is limited to ARIN’s office and VPN networks. Access to the systems is logged.

Further, access to the RPKI systems is audited, and logged using anon-repudiation module generated from the HSM. These logs are exported to a separate system maintained by the ARIN Chief Operating Officer for later processing and review.

6.6.3. Life cycle security controls

Software and hardware used for the RPKI that was not developed by ARIN and was acquired through normal ARIN 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 backout, 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

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

6.8. Time stamping

The RPKI operated by ARIN does not make use of time stamping as defined in RFC 3161.

7. CERTIFICATE AND CRL PROFILES

Please refer to the Certificate and CRL Profile [RFC6847].

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

ARIN performs periodic vulnerability assessments for computer and network systems, including those that are part of the RPKI CA.

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

8.1. Frequency or circumstances of assessment

Assessments are initiated at the request of the Chief Operating Officer.

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 ARIN.

8.4. Topics covered by assessment

The external vulnerability assessment on ARIN IT systems covers 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.

8.5. Actions taken as a result of deficiency

ARIN’s Operating Officer reviews all recommendations made by the external assessor and takes remedial actions as such Operating Officer determines appropriate.

8.6. Communication of results

The external vulnerability assessment reports are provided to all relevant personnel within ARIN - including ARIN’s Chief Operating Officer.

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 ARIN. The current schedule of fees is published on the ARIN web site at https://www.arin.net.

9.1.2. Certificate Access Fees [OMITTED]

9.1.3. Revocation Status Information Access Fees [OMITTED]

9.1.4. Fees for other services (if applicable)

ARIN charges fees for other services related to the allocation and administration of IP address and Autonomous System number resources. The current schedule of fees is published on the ARIN web site at https://www.arin.net.

9.1.5. Refund policy [OMITTED]

9.2. Financial responsibility [OMITTED]

9.2.1. Insurance coverage [OMITTED]

9.2.2. Other assets [OMITTED]

9.2.3. Insurance or warranty coverage for end-entities [OMITTED]

9.3. Confidentiality of business information [OMITTED]

9.3.1. Scope of confidential information [OMITTED]

9.3.2. Information not within the scope of confidential information [OMITTED]

9.3.3. Responsibility to protect confidential information [OMITTED]

9.4. Privacy of personal information [OMITTED]

9.4.1. Privacy plan [OMITTED]

9.4.2. Information treated as private [OMITTED]

9.4.3. Information not deemed private [OMITTED]

9.4.4. Responsibility to protect private information [OMITTED]

9.4.5. Notice and consent to use private information [OMITTED]

9.4.6. Disclosure pursuant to judicial or administrative process [OMITTED]

9.4.7. Other information disclosure circumstances [OMITTED]

9.5. Intellectual property rights

ARIN retains all intellectual property rights (including but not limited to patent, trademark, copyright and trade secret rights) in and to all Resource Certification Services, including the Resource Certification and Certificates.

Each subscriber, Relying Party and/or any third party is hereby prohibited from the distribution, copying, replication, reverse engineering, or any other use or manipulation of the RPKI and/or Resource Certification services and/or material other than as specifically provided in this CPS or agreed and consented to in writing by ARIN, such agreement and consent which may be withheld in ARIN’s absolute and sole discretion.

Each subscriber, Relying Party and third party acknowledges and agrees that: (i) nothing provided by ARIN in connection with the Resource Services (or any part thereof),including the Resource Certification, is or will be the property (real, personal, or intellectual) of subscriber, Relying Party or any third party; (ii) each subscriber, Relying Party and any third party does not and will not have or acquire, directly or indirectly, any title or property rights in or to anything provided by ARIN in connection with the Resource Certification Services (or any part thereof),including the Resource Certification, for any reason, whether by virtue of the Resource Certification Services, the Resource Certification Service Terms, or otherwise; and (iii) each subscriber, Relying Party and any third party will not attempt, directly or indirectly, to obtain or assert, whether in the United States or any other jurisdiction, any patent, trademark, service mark, copyright, or any other form of intellectual, proprietary or property rights in anything provided by or on behalf of ARIN in connection with the Resource Certification Services (or any part thereof),including the Resource Certification.

9.6. Representations and warranties [OMITTED]

9.6.1. CA representations and warranties [OMITTED]

9.6.2. Subscriber representations and warranties [OMITTED]

9.6.3. Relying party representations and warranties [OMITTED]

9.6.4. Representations and warranties of other participants [OMITTED]

9.7. Disclaimers of warranties

EACH USER, SUBSCRIBER, RELYING PARTY, AND THIRD PARTY RELYING ON, USING OR BENEFITTING FROM THE RESOURCECERTIFICATION SERVICES (OR ANY PART THEREOF) OR ANY RESOURCECERTIFICATION ACKNOWLEDGES AND AGREES THAT THE RESOURCE CERTIFICATION SERVICES, INCLUDING THE RESOURCE CERTIFICATION, ARE PROVIDED ON AN “ASIS” BASIS WITH ALL RISKS AND FAULTS ASSOCIATED THEREWITH. ARIN MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND WITH RESPECT TO ANY RESOURCE CERTIFICATION OR

OTHER RPKI SERVICES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTION OF REQUIREMENTS, NONINFRINGEMENT, OR ANY WARRANTY ARISING OUT OF A COURSE OF PERFORMANCE, DEALING, TRADE OR USAGE. ANY AND ALL REPRESENTATIONS, WARRANTIES AND COVENANTS ARE HEREBY DISCLAIMED BY ARIN AND WAIVED BY EACH USER, SUBSCRIBER, RELYING PARTY, AND THIRD PARTY RELYING ON, USING OR BENEFITTING FROM THE RESOURCE CERTIFICATION SERVICES (OR ANY PARTTHEREOF), INCLUDING ANY RESOURCE CERTIFICATION. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, ARIN DOES NOT REPRESENT, WARRANT ORCOVENANT THAT ANY RESOURCE CERTIFICATION SERVICES, RESOURCECERTIFICATION, OR ANY ACCESS OR USE THEREOF WILL (i) BE UNINTERRUPTED, (ii) BE FREE OF DEFECTS, INACCURACIES, OR ERRORS, (iii) MEET ANY REQUIREMENTS OF ANY USER, SUBSCRIBER, RELYING PARTY OR THIRD PARTY, OR (iv) OPERATE IN THE CONFIGURATION OR WITH OTHER HARDWARE OR SOFTWARE USED BY ANY USER, SUBSCRIBER, RELYING PARTY OR THIRD PARTY.

9.8. Exclusion of Liabilities and Damages

NOTWITHSTANDING ANYTHING TO THE CONTRARY, ARIN WILL NOT BE LIABLE TO ANY USER, SUBSCRIBER, RELYING PARTY OR THIRD PARTY, INCLUDING ANY CLIENTS OR CUSTOMERS OF ANY USER,SUBSCRIBER, RELYING PARTY OR THIRD PARTY, FOR ANY LIABILITIES AT LAW OR IN EQUITY OR FOR ANY DAMAGES, INCLUDING CONSEQUENTIAL, INCIDENTAL,INDIRECT, PUNITIVE, EXEMPLARY, OR SPECIAL DAMAGES (INCLUDINGLIABILITIES OR DAMAGES RELATING TO LOST PROFITS, LOST DATA, OR LOSS OFGOODWILL) ARISING OUT OF, RELATING TO, OR CONNECTED WITH ANY RESOURCE CERTIFICATION SERVICES, ANY RESOURCE CERTIFICATION, OR OTHERWISE INCONNECTION THEREWITH, WHETHER BASED ON CONTRACT, TORT, STATUTE, OR ANYCAUSE OF ACTION, EVEN IF ANY USER, SUBSCRIBER, RELYING PARTY OR THIRD PARTY IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

9.9. Limitations of liability

IN NO EVENT, WHETHER BASED ON CONTRACT,TORT, STATUTE, OR ANY CAUSE OF ACTION, WILL ARIN’S LIABILITY TO ANYUSER, SUBSCRIBER, RELYING PARTY OR THIRD PARTY, INCLUDING ANY CLIENTS OR CUSTOMERS OF ANY USER, SUBSCRIBER, RELYING PARTY OR THIRD PARTY, EXCEED IN THE AGGREGATE THE GREATER OF (i) THE AMOUNT PAID BYSUBSCRIBER TO ARIN FOR THE RESOURCE CERTIFICATION SERVICES DURING THE SIX (6) MONTHS IMMEDIATELY PRECEDING THE EVENT THAT GIVES RISE TO SUCHLIABILITY OR (ii) ONE HUNDRED U.S. DOLLARS (US$100.00).

9.10. Indemnification

Each user, subscriber, Relying Party, and third party relying on, using or benefitting from the Resource Certification Services (or any part thereof) or any Resource Certification shall indemnify, defend, and hold harmless ARIN and its parent, subsidiaries and other affiliates, each of their respective predecessors, successors and assigns, each of their respective employees, representatives, agents, attorneys, advisors, trustees, directors, officers, managers, and members (collectively, the “Indemnified Parties”) from any and all claims, demands, disputes, actions, suits, proceedings, judgments, damages, injuries, losses, expenses, costs and fees (including, without limitation, costs and fees associated with attorneys, accountants, investigators and experts), interests, fines and penalties of whatever nature, character or description, whether known or unknown, anticipated or unanticipated, fixed or contingent, now existing or which may hereafter accrue (collectively, “Claims”) brought or asserted against any of the Indemnified Parties alleging facts or circumstances that, in any way, whether directly or indirectly, relate to, arise from, or maybe connected with:

any authorized or unauthorized use or access to any Resource Certification or other Resource Certification Services by such user, subscriber, relying party, or third party

or any of its parent, subsidiaries or other affiliates, or any of their respective predecessors, successors or assigns, or any of their respective directors, officers, managers, shareholders, members, employees, contractors, customers, clients, partners, representatives, agents, advisors, or other persons acting by, through, under or in concert with any of them (each an "Indemnifying Party" and collectively the "Indemnifying Parties");
(ii) any authorized or unauthorized use or access to any Resource Certification or other Resource Certification Services by any person who acquired authorized or unauthorized use or access of any Resource Certification or other Resource Certification Services by or through such Indemnifying Party;
(iii) an Indemnifying Party's reliance on a Certificate that is not reasonable under the circumstances. An Indemnifying Party's failure to check the status of a Certificate to determine if the Certificate is expired or revoked; (v) an Indemnifying Party's use of a Certificate for a purpose not specifically identified or permitted by the Resource Certification Terms; and/or (vi) any breach by any Indemnifying Party of this CPS or any other Resource Certification Terms. ARIN may, in its sole and absolute discretion, control the disposition of any Claim at the sole cost and expense of an Indemnifying Party. If ARIN permits an Indemnifying Party to control the disposition of any Claim; such Indemnifying Party shall keep ARIN informed of and consult with ARIN in connection with the progress of such Claim;
b) such Indemnifying Party shall not settle, compromise, or in any manner dispose of any Claim without the prior written consent of ARIN and:
c) ARIN shall have the right to participate in the settlement, compromise and/or disposition of any Claim at such Indemnifying Party sole cost and expense. Such Indemnifying Party shall provide written notice to ARIN promptly of the assertion against any Indemnifying Party or any other person of any Claim or the commencement of any Claim, whether an Indemnified Party is named or identified in the Claim.

9.11. Term and termination

9.11.1. Term [OMITTED]

9.11.2. Termination

ARIN shall have the right, without prior notice, to immediately terminate this CPS and the Resource Certification Services (or any part thereof) for: (i) any breach or violation of this CPS or other Resource Certification Terms by any user, subscriber, Relying Party, or third party relying on, using or benefitting from the Resource Certification Services (or any part thereof) or any Resource Certification; (ii) a duly authorized request by a law enforcement or other government agency to terminate access to and/or use of the Resource Certification Services (or any part thereof); (iii)discontinuance or modification to the Resource Certification Services (or any part thereof) by ARIN; (iv) technical or security issues or problems; (v) any fraudulent or illegal activities by any user, subscriber, Relying Party, or third party relying on, using or benefitting from the Resource Certification Services (or any part thereof) or any Resource certification; (vi) if a subscriber no longer holds the Internet number resource(s) subject of a Certificate or Resource Certification; (vii) a subscriber fails to make any payment due to ARIN; and/or (viii) in accordance with the other Resource Certification Terms, as applicable. In addition, ARIN shall have the right to terminate this CPS and the Resource Certification Services (or any part thereof) for any or no reason upon fourteen (14) days' prior notice.

9.11.3. Effect of termination and survival.

If this CPS is terminated, no user, subscriber, Relying Party, or third party will be entitled to receive Resource Certification Services or Resource Certification that is covered by this CPS. The defined terms in this CPS and the following Sections shall survive termination or expiration of this CPS:8.5, 8.7, 8.8, 8.9, 8.10, 8.11, 8.14, 8.15, and 8.17.

9.12. Individual notices and communications with participants [OMITTED]

9.13. Amendments

ARIN may amend the terms of this CPS from time to time, and any such amendments will be effective upon posting such amendments on ARIN'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.

9.13.1. Procedure for amendment [OMITTED]

9.13.2. Notification mechanism and period [OMITTED]

9.13.3. Circumstances under which OID must be changed [OMITTED]

9.14. Dispute resolution provisions

In the event of any dispute(s) regarding any term or condition or provision or performance or conduct arising out of or relating to this CPS, the parties each agree to first seek resolution through cooperative settlement negotiations involving themselves or their representatives as they each deem appropriate; and, second, in the event cooperative settlement negotiations are not successful, or do not occur, within thirty (30) days are a party initiates such negotiations, the parties agree to submit any unresolved dispute(s) to binding and final arbitration for resolution. Such arbitration shall be held in Washington, D.C., or by agreement of both parties at any other location, in accordance with the rules of the American Arbitration Association ("AAA") then in effect. A single arbitrator shall be selected by the parties by striking in turn from a list of arbitrators supplied by the AAA or, as applicable, the locally prevalent equivalent of AAA. Each party shall bear their own attorneys' fees, and the initiating party shall initially bear the costs of the arbitration's expenses. The Arbitrator may reallocate the costs of the arbitration's expense between the parties but may not reallocate legal fees incurred by the parties. The Arbitrator is permitted to assess all arbitration costs, including any legal fees incurred by the parties, against any party that has acted in bad faith during the proceeding. Any judgment upon the award rendered pursuant to the arbitration proceeding may be entered in any court having competent jurisdiction. Notwithstanding the foregoing in this Paragraph, either party may bring an action before any court having competent jurisdiction for a temporary restraining order, preliminary injunction and/or other injunctive relief to seek to maintain the status quo between the parties, pending resolution of the dispute(s) in accordance with the terms of this Paragraph.

9.15. Governing law

This CPS and the parties' performance under it shall be governed in all respects by, and construed in accordance with, the laws of the Commonwealth of Virginia and the United States of America.

9.16. Compliance with applicable law [OMITTED]

9.17. Miscellaneous provisions

9.17.1. Entire agreement

This CPS and the other Resource Certification Terms constitute the entire understanding between the parties and replaces and supersedes all prior and contemporaneous agreements and understandings, whether oral or written, express or implied, with respect to the subject matter of this CPS.

9.17.2. Assignment

This CPS may be assigned by ARIN in its sole and absolute discretion. This CPS may not be assigned or transferred, whether voluntarily or by operation of law, by any other party or person without ARIN's prior written consent, which may be withheld or denied in ARIN's absolute and sole discretion. The event of any transaction (whether a merger, acquisition, or sale) in which a party's controlling managerial and/or voting interest changes shall be considered an assignment. Any attempt by creditors of any other party or person to obtain an interest in any rights under this CPS, whether by attachment, levy, garnishment or otherwise, shall be considered an assignment and shall render this CPS voidable at ARIN's option.

9.17.3. Severability

If any provision of this CPS is determined to be illegal, invalid, or otherwise unenforceable by a court or tribunal of competent jurisdiction, then to the extent necessary to make such provision and/or this CPS legal, valid, or otherwise enforceable, such provision will be limited, construed, or severed and deleted from this CPS, and the remaining portion of such provision and the remaining other provisions hereof will survive, remain in full force and effect, and continue to be binding, and will be interpreted to give effect to the intention of the parties insofar as possible.

9.17.4. Enforcement (attorneys' fees) [OMITTED]

9.17.5. Force Majeure

ARIN shall not be deemed in default hereunder, nor shall ARIN be responsible for any cessation, interruption, or delay in the performance of its obligations under this CPS where such failure of performance is the result of any force majeure event, including, but not limited to, earthquake, flood, fire, storm, natural disaster, act of God, civil disturbances, war, terrorism, armed conflict, riots, failure of contractors or subcontractors to perform, labor strike, lockout, boycott, or acts of governmental authorities. In the event a force majeure event extends for a period in excess of thirty (30) days in the aggregate and prevents ARIN from performing its obligations under this CPS, ARIN may, in its discretion, terminate this CPS immediately.

9.17.6. Waiver

No waiver of any provision or consent to any action under this CPS by ARIN will constitute a waiver of any other provisions or consent to any other action, nor will such waiver or consent constitute a continuing waiver or consent or commit ARIN to provide a past or future waiver or consent.

9.18. Other provisions

This CPS will be construed as if it was jointly drafted and may not be construed against either party. The words “including” and “include” means “including, without limitation” and “include, without limitation.” The terms “herein,” “hereof” and “hereunder” and other words of similar import refer to this CPS as a whole and not to any article, section or other subdivision. Unless the context of this CPS otherwise requires, words using singular or plural number also include the plural or singular number, respectively. The headings contained in this CPS are for the purposes of convenience only and are not intended to define or limit the contents of the provisions contained therein.

10.REFERENCES

These references are provided for convenience of the reader only and do not form a part of any agreement, understanding, right or obligation of ARIN or any user, subscriber, Relying Party, or third party relying on, using or benefitting from the Resource Certification Services (or any part thereof) or any Resource Certification.

[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.

[RFC6484] Seo, K., Watro, R., Kong, D., and Kent, S.,"Certificate Policy for the Internet IP Address and AS Number PKI", Feb 2012.

[RFC6487] Huston, G., Loomans, R., Michaelson, G., “A Profile for X.509 PKIX Resource Certificates”, Feb 2012.

[RFC6492] G. Houston, R. Loomis, B. Ellacott, R. Austien, “A Protocol for Provisioning Resource Certificates”, Feb 2012.

[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.