Certificate Policy (CP)
for the Resource PKI (RPKI
draft-ietf-sidr-cp-17.txt

Status of this Memo

   This Internet-Draft is submitted to IETF in full conformance with
   the provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF), its areas, and its working groups. Note that
   other groups may also distribute working documents as Internet-
   Drafts.

   Internet-Drafts are draft documents valid for a maximum of six
   months and may be updated, replaced, or obsoleted by other documents
   at any time. It is inappropriate to use Internet-Drafts as
   reference material or to cite them other than as "work in progress."

   The list of current Internet-Drafts can be accessed at
   http://www.ietf.org/ietf/1id-abstracts.txt

   The list of Internet-Draft Shadow Directories can be accessed at
   http://www.ietf.org/shadow.html

   This Internet-Draft will expire on September 30, 2011.

Abstract

   This document describes the certificate policy for a Public Key
   Infrastructure (PKI) used to support attestations about Internet
   Number Resource (INR) holdings. Each organization that distributes
   IP addresses or Autonomous System (AS) numbers to an organization
   will, in parallel, issue a (public key) certificate reflecting this
   distribution. These certificates will enable verification that the
   resources indicated in the certificate have been distributed to the

holder of the associated private key and that this organization is
the current, unique holder of these resources.

Table of Contents

1. **Introduction**

This document describes the certificate policy for a Public Key
Infrastructure (PKI) used to attest to Internet Number Resource
holdings (INRs) (IP addresses or Autonomous System (AS) numbers). An
organization that distributes INRs to another organization MAY, in
parallel, issue a (public key) certificate reflecting this
distribution. These certificates will enable verification that the
resources indicated in the certificate have been distributed to the
holder of the associated private key and that this organization is
the current holder of these resources.

The most important and distinguishing aspect of the PKI for which
this policy was created is that it does not purport to identify an
INR 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 INR 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 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 current INR holdings. This includes any
certificates issued in support of operation of this infrastructure,
e.g., for integrity or access control of the repository system
described in section 2.4. Such transitive uses of certificates also
are permitted under this policy. Use of the certificates and
certificate revocation lists (CRLs) managed under this PKI for any
other purpose is a violation of this CP, and relying parties (RPs)
SHOULD reject certificates presented for such uses.

Note: This document is based on the template specified in the
Internet Engineering Task Force (IETF) standards document RFC 3647
[RFC3647]. In the interest of keeping the document as short as
reasonable, a number of sections contained in the template have been
omitted from this policy because they do not apply to this PKI.
However, we have retained the section numbering scheme employed in
RFC 3647 to facilitate comparison with the outline in Section 6 of
RFC 3647. Each of these omitted sections should be read as "No
stipulation" in CP/CPS parlance.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [RFC2119].

1.1. Overview

This PKI is designed to support validation of claims by current holders of INRs, in accordance with the records of the organizations that act as Certification Authorities (CAs) in this PKI. The ability to verify such claims is essential to ensuring the unambiguous distribution of these resources [ARCH].

The structure of the RPKI is congruent with the number resource allocation framework of the Internet. The IANA allocates number resources for special purposes [RFC5736], to Regional Internet Registries (RIRs), and to others. The RIRs, in turn, manage the allocation of number resources to end users, Internet Service Providers, and others.

This PKI encompasses several types of certificates (see [CERTPROF] for more details):

. CA certificates for each organization distributing INRs, and for
   INR holders

. End-entity (EE) certificates for organizations to validate digital
   signatures on RPKI-signed objects

1.2. Document name and identification

The name of this document is "Certificate Policy (CP) for the Resource PKI (RPKI)".

This policy has been assigned the following OID:

id-cp-ipAddr-asNumber OBJECT IDENTIFIER ::= { iso(1)

                        identified-organization(3) dod(6) internet(1)

                        security(5) mechanisms(5) pkix(7) cp(14) 2 }

1.3. PKI participants

Note: In a PKI, the term "subscriber" refers to an individual or organization that is a Subject of a certificate issued by a CA. The term is used in this fashion throughout this document, without qualification, and should not be confused with the networking use of the term to refer to an individual or organization that receives

service from an ISP. In such cases the term "network subscriber" will be used. Also note that, for brevity, this document always refers to PKI participants as organizations or entities, even though some of them are individuals.

1.3.1. Certification authorities

The organizations that distribute IP addresses and AS numbers (IANA, RIRs, NIRs, ISPs) act as CAs in this PKI.

Organizations that do not distribute INRs, but hold such resources also act as CAs when they create EE certificates.

1.3.2. Registration authorities

This PKI does not require establishment or use of a registration authority (RA) function separate from the one provided inherently in conjunction with the CA function. The RA function MUST be provided by the same entity operating as a CA, e.g., entities listed in Section 1.3.1. An entity acting as a CA in this PKI already has a formal relationship with each organization to which it distributes INRs. These organizations already perform the RA function implicitly since they already assume responsibility for distributing INRs.

1.3.3. Subscribers

These are the organizations receiving distributions of INRs - RIRs, NIRs, ISPs, and other organizations.

Note that any of these organizations may have received distributions from more than one source, over time. This is true even for RIRs, which participate in inter-registry exchanges of address space. This PKI accommodates such relationships.

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

Every organization that undertakes a role as a CA in this PKI is responsible for populating the RPKI distributed repository system with the certificates, CRLs, and RPKI-signed objects that it issues. The organization MAY operate its own publication point or it MAY outsource this function (See sections 2.1 and 2.2.)

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, also are permitted under this policy. For example,
   certificates may be issued in support of integrity and access
   control for the repository system described in 2.4. Such transitive
   uses are permitted under this policy.

1.4.2. Prohibited certificate uses

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

1.5. Policy administration

1.5.1. Organization administering the document

   This CP is administered by

   Internet Engineering Steering Group
   c/o Internet Society
   1775 Wiehle Avenue, Suite 201
   Reston, VA 20190-5108
   U.S.A.

1.5.2. Contact person

   The contact information is

      iesg@ietf.org

      +1-703-439-2120 (Internet Society)

1.5.4. CP approval procedures

   If a replacement BCP is needed that updates or obsoletes the current
   BCP, then the replacement BCP MUST be approved by the IESG following
   the procedures of the IETF Standards Process as defined in RFC 2026
   [RFC2026].

[1.6](#). Definitions and acronyms

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

Distribution of INRs - A process of distribution of the INRs along the
        respective number hierarchy. IANA distributes blocks of IP
        addresses and AS Numbers to the five Regional Internet
        Registries (RIRs). RIRs distribute smaller address blocks and AS
        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 IP addressing systems and AS numbers
        used for routing internet traffic. IANA distributes INRs to
        Regional Internet Registries (RIRs).

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

        . IP Version 4 addresses,

        . IP version 6 addresses, and

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

ISP -   Internet Service Provider. This is an organization managing and
        providing Internet services to other organizations.

LIR -   In some regions, the term Local Internet Registry (LIR) is used
        to refer to what is called an ISP in other regions.

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

RIR -   Regional Internet Registry. This 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) that is declared to be
        such by a standards track RFC, and that can be validated using
        certificates issued under this PKI. The content and format of
        these data constructs depend on the context in which validation

of claims of current holdings of INRs takes place. Examples of
these objects are repository manifests and ROAs.

2. Publication And Repository Responsibilities

2.1. Repositories

   Certificates, CRLs, and RPKI-signed objects (intended for public
   consumption) MUST be made available for downloading by all relying
   parties, to enable them to validate this data. This motivates use of
   a robust, distributed repository system. Each CA MUST maintain a
   publicly accessible online repository and publish all RPKI-signed
   objects (intended for public consumption) via this repository in a
   manner that conforms with "A Profile for Resource Certificate
   Repository Structure" [REPOS]. (This function MAY be outsourced, as
   noted in Section 2.2 below.) The collection of repositories forms
   the RPKI distributed repository system.

2.2. Publication of certification information

   Each CA MUST publish the certificates (intended for public
   consumption) that it issues via the repository system.

   Each CA MUST publish the CRLs (intended for public consumption) that
   it issues via the repository system.

   Each CA MUST publish its RPKI-signed objects (intended for public
   consumption) via the repository system.

   Each CA that issues certificates to entities outside of its
   administrative domain SHOULD create and publish a CPS that meets the
   requirements set forth in this CP. Publication means that the
   entities to which the CA issues certificates MUST be able to acquire
   a copy of the CPS, and MUST be able to ascertain when the CPS
   changes. (An organization that does not allocate or assign INRs does
   not need to create or publish a CPS.)

   An organization MAY choose to outsource publication of RPKI data -
   certificates, CRLs, and other RPKI-signed objects.

   The CP will be published as an IETF RFC and will be available from
   the IETF RFC repository.

2.3. Time or frequency of publication

   The CPS for each CA MUST specify the following information:

   The period of time within which a certificate will be published
   after the CA issues the certificate.

The period of time within which a CA will publish a CRL with an
entry for a revoked certificate after it revokes that certificate.

Expired and revoked certificates SHOULD be removed from the RPKI
repository system, upon expiration or revocation, respectively.
Also, please note that each CA MUST publish its CRL prior to the
nextUpdate value in the scheduled CRL previously issued by the CA.

2.4. Access controls on repositories

Each CA or repository operator MUST implement access controls to
prevent unauthorized persons from adding, modifying or deleting
repository entries. A CA or repository operator MUST NOT
intentionally use technical means of limiting read access to its
CPS, certificates, CRLs or RPKI-signed objects. This data is
intended to be accessible to the public.

3. Identification and Authentication

3.1. Naming

3.1.1. Types of names

   The distinguished name for every CA and end-entity consists of a
   single Common Name (CN) attribute with a value generated by the
   issuer of the certificate. 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",
   i.e., the name is not intended to convey the identity of the Subject
   to relying parties. The rationale here is that certificates issued
   under this PKI 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 (and Issuer) names 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

   There is no guarantee that subject names are globally unique in this
   PKI. Each CA certifies subject names that MUST be unique among the
   certificates that it issues. Although it is desirable that these
   subject names be unique throughout the PKI, name uniqueness within
   the RPKI cannot be guaranteed.

   However, subject names in certificates SHOULD be constructed in a
   way that minimizes the chances that two entities in the RPKI will be
   assigned the same name. The RPKI certificate profile [CERTPROF]
   provides an example of how to generate (meaningless) subject names
   in a way that minimizes the likelihood of collisions.

[3.2](#). Initial identity validation

[3.2.1](#). Method to prove possession of private key

Each CA operating within the context of this PKI MUST require each
Subject to demonstrate proof-of-possession (PoP) of the private key
corresponding to the public key in the certificate, prior to issuing
the certificate. The means by which PoP is achieved is determined by
each CA and MUST be declared in the CPS of that CA.

[3.2.2](#). Authentication of organization identity

Each CA operating within the context of this PKI MUST employ
procedures to ensure that each certificate it issues accurately
reflects its records with regard to the organization to which the CA
has distributed the INRs identified in the certificate. The specific
procedures employed for this purpose MUST bedescribed by the CPS for
each CA. Relying parties can expect each CA to employ procedures
commensurate with those it already employs as a registry or ISP, in
the management of the INRs. This authentication is solely for use by
each CA in dealing with the organizations to which it distributes
INRs, and thus should not be relied upon outside of this CA-
subscriber relationship.

[3.2.3](#). Authentication of individual identity

Each CA operating within the context of this PKI MUST employ
procedures to identify at least one individual as a representative
of each organization that is an INR holder. The specific means by
which each CA authenticates individuals as representatives for an
organization MUST be described by the CPS for each CA. Relying
parties can expect each CA to employ procedures commensurate with
those it already employs as a registry or ISP, in authenticating
individuals as representatives for INR holders.

[3.2.4](#). Non-verified subscriber information

A CA MUST NOT include any non-verified subscriber data in
certificates issued under this certificate policy except for Subject
Information Access (SIA) extensions.

[3.2.5](#). Validation of authority

Each CA operating within the context of this PKI MUST employ
procedures to verify that an individual claiming to represent an
organization to which a certificate is issued, is authorized to
represent that organization in this context. The procedures MUST be
described by the CPS for the CA. Relying parties can expect each CA

to employ procedures commensurate with those it already employs as a
registry or ISP, in authenticating individuals as representatives
for INR holders.

3.2.6. Criteria for interoperation

This PKI 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

Each CA operating within the context of this PKI MUST employ
procedures to ensure that an organization requesting a re-key is the
legitimate holder of the certificate to be re-keyed and associated
INRs and MUST require PoP of the private key corresponding to the
new public key. The procedures employed for these purposes MUST be
described in the CPS for the CA. With respect to authentication of
the holder of the INRs, relying parties can expect each CA to employ
procedures commensurate with those it already employs as a registry
or ISP, in the management of INRs.

Note: An issuer MAY choose to require periodic re-keying consistent
with contractual agreements with the recipient. If so, this MUST be
described by the CPS for the CA.

3.3.2. Identification and authentication for re-key after revocation

Each CA operating within the context of this PKI MUST employ
procedures to ensure that an organization requesting a re-key after
revocation is the same entity to which the revoked certificate was
issued and is the legitimate holder of the associated INR. The CA
MUST require PoP of the private key corresponding to the new public
key. The specific procedures employed for these purposes MUST be
described by the CPS for the CA. With respect to authentication of
the holder of the INRs, relying parties can expect each CA to employ
procedures commensurate with those it already employs as a registry
or ISP, in the management of INRs. Note that there MAY be different
procedures for the case where the legitimate subject still possesses
the original private key as opposed to the case when it no longer
has access to that key.

3.4. Identification and authentication for revocation request

Each CA operating within the context of this PKI MUST employ
procedures to ensure that:

.   an organization requesting revocation is the legitimate holder
    of the certificate to be revoked.

.   each certificate it revokes accurately reflects its records
    with regard to the organization to which the CA has distributed
    the INRs identified in the certificate.

.   an individual claiming to represent an organization for which
    a certificate is to be revoked, is authorized to represent that
    organization in this context.

The specific procedures employed for these purposes MUST be
described by the CPS for the CA. Relying parties can expect each CA
to employ procedures commensurate with those it already employs as a
registry or ISP, in the management of INRs.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who can submit a certificate application

   Any entity that distributes INRs SHOULD acquire a certificate. This
   includes Internet Registries and ISPs. Additionally, entities that
   hold INRs from an Internet Registry, or that are multi-homed, MAY
   acquire a certificate under this PKI. The (CA) certificates issued
   to these entities MUST include one or both of the extensions defined
   by RFC 3779 [RFC3779], X.509 Extensions for IP Addresses and AS
   Identifiers, as appropriate.

   The application procedure MUST be described in the CPS for each CA.

4.1.2. Enrollment process and responsibilities

   The enrollment process and procedures MUST be described by the CPS
   for each CA. An entity that desires one or more certificates should
   contact the organization from which it receives its INRs.

4.2. Certificate application processing

   CAs SHOULD make use of existing standards for certificate
   application processing. Section 6 of the resource certificate
   profile [CERTPROF] defines the standard certificate request formats
   that MUST be supported

   Each CA MUST define the certificate request/response standards that
   it employs, via its CPS.

4.2.1. Performing identification and authentication functions

   Existing practices employed by registries and ISPs to identify and
   authenticate organizations that receive INRs form the basis for
   issuance of certificates to these subscribers. It is important to
   note that the Resource PKI SHOULD NOT be used to authenticate the
   identity of an organization, but rather to bind subscribers to the
   INRs they hold. Because identity is not being vouched for by this
   PKI, certificate application procedures need not verify legal
   organization names, etc.

4.2.2. Approval or rejection of certificate applications

   Certificate applications MUST be approved based on the normal
   business practices of the entity operating the CA, based on the CA's
   records of INR holders. Each CA MUST follow the procedures specified

in 3.2.1 to verify that the requester holds the private key
corresponding to the public key that will be bound to the
certificate the CA issues to the requestor. The details of how
certificate applications are approved MUST be described in the CPS
for the CA in question.

4.2.3. Time to process certificate applications

No stipulation. Each CA MUST declare its expected time frame to
process (approve, issue and publish) a certificate application as
part of its CPS.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

If a CA determines that the request is acceptable, it MUST issue the
corresponding certificate and publish it in the RPKI distributed
repository system via publication of the certificate at the CA's
repository publication point.

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

The CA MUST notify the subscriber when the certificate is published.
The means by which a subscriber is notified MUST be defined by each
CA in its CPS.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

Within the timeframe specified in its CPS, the CA MUST place the
certificate in the repository and notify the subscriber. This MAY
be done without subscriber review and acceptance. Each CA MUST state
in its CPS the procedures it follows for publishing of the
certificate and notification to the subscriber.

4.4.2. Publication of the certificate by the CA

Certificates MUST be published in the RPKI distributed repository
system via publication of the certificate at the CA's repository
publication point as per the conduct described in 4.4.1. The
procedures for publication MUST be defined by each CA in its CPS.

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

The CPS of each CA MUST indicate whether any other entities will be
notified when a certificate is issued.

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**

   Each holder of an INR is eligible to request an X.509 CA certificate
   containing appropriate RFC 3779 extensions. Holders of CA resource
   certificates also MAY issue EE certificates to themselves to enable
   verification of RPKI-signed objects that they generate.

4.5.2. **Relying party public key and certificate usage**

   Reliance on a certificate must be reasonable under the
   circumstances. If the circumstances indicate a need for additional
   assurances, the relying party must obtain such assurances in order
   for such reliance to be deemed reasonable.

   Before any act of reliance, relying parties MUST independently (1)
   verify that the certificate will be used for an appropriate purpose
   that is not prohibited or otherwise restricted by this CP (see
   section 1.4), and (2) assess the status of the certificate and all
   the certificates in the chain (terminating at a Trust Anchor (TA)
   accepted by the RP) that issued the certificates relevant to the
   certificate in question. If any of the certificates in the
   certificate chain have been revoked or have expired, the relying
   party is solely responsible to determine whether reliance on a
   digital signature to be verified by the certificate in question is
   acceptable. Any such reliance is made solely at the risk of the
   relying party.

   If a relying party determines that use of the certificate is
   appropriate, the relying party must utilize appropriate software
   and/or hardware to perform digital signature verification as a
   condition of relying on the certificate. Moreover the relying party
   MUST validate the certificate in a manner consistent with the RPKI
   certificate profile [CERTPROF], which specifies the extended
   validation algorithm for RPKI certificates.

4.6. **Certificate renewal**

   This section describes the procedures for certificate renewal.
   Certificate renewal is the issuance of a new certificate to replace
   an old one prior to its expiration. Only the validity dates and the
   serial number (the field in the certificate not the DN attribute)
   are changed. The public key and all other information remain the
   same.

4.6.1. **Circumstance for certificate renewal**

   A certificate MUST be processed for renewal based on its expiration
   date or a renewal request from the subscriber. Prior to the
   expiration of an existing subscriber's certificate, it is the
   responsibility of the subscriber to renew the certificate to
   maintain continuity of certificate usage. If the issuing CA
   initiates the renewal process based on the certificate expiration
   date, then that CA MUST notify the holder in advance of the renewal
   process. The validity interval of the new (renewed) certificate
   SHOULD overlap that of the previous certificate, to ensure
   continuity of certificate usage. It is RECOMMENDED that the renewed
   certificate be issued and published at least 1 week prior to the
   expiration of the certificate it replaces.

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

4.6.2. **Who may request renewal**

   Only the certificate holder or the issuing CA may initiate the
   renewal process. The certificate holder MAY request an early
   renewal, for example, if it wishes to change the public key, or if
   it expects to be unavailable to support the renewal process during
   the normal expiration period. An issuing CA MAY initiate the renewal
   process based on the certificate expiration date.

4.6.3. **Processing certificate renewal requests**

   Renewal procedures MUST ensure that the person or organization
   seeking to renew a certificate is in fact the subscriber (or
   authorized by the subscriber) of the certificate and the legitimate
   holder of the INR associated with the renewed certificate. Renewal
   processing MUST verify that the certificate in question has not been
   revoked.

4.6.4. **Notification of new certificate issuance to subscriber**

   No additional stipulations beyond those of section 4.3.2.

4.6.5. **Conduct constituting acceptance of a renewal certificate**

   No additional stipulations beyond those of section 4.4.1.

4.6.6. Publication of the renewal certificate by the CA

No additional stipulations beyond those of section 4.4.2.

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

No additional stipulations beyond those of section 4.4.3.

4.7. Certificate re-key

This section describes the procedures for certificate re-key.
Certificate re-key is the issuance of a new certificate to replace
an old one because the key needs to be replaced. Unlike with
certificate renewal, the public key is changed.

4.7.1. Circumstance for certificate re-key

Re-key of a certificate SHOULD be performed only when required,
based on:

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

2. the expiration of the cryptographic lifetime of the associated
   key pair

A CA re-key operation has dramatic consequences, requiring the re-
issuance of all certificates issued by the re-keyed entity. So it
should be performed only when necessary and in a way that preserves
the ability of relying parties to validate certificates whose
validation path includes the re-keyed entity. CA key rollover MUST
follow the procedures defined in "CA Key Rollover in the RPKI"
[KEYROLL].

Note that if a certificate is revoked to replace the RFC 3779
extensions, the replacement certificate MUST incorporate the same
public key rather than a new key. This applies to when one is
adding INRs (revocation not required) and to when one is removing
INRs (revocation required (see Section 4.8.1)).

If the re-key is based on a suspected compromise, then the previous
certificate MUST 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,
the CA that issued the certificate MAY chose to initiate a rekey
based on a verified compromise report.

[4.7.3](). **Processing certificate re-keying requests**

   The re-key process follows the general procedures of certificate
   generation as defined in [section 4.3]().

[4.7.4](). **Notification of new certificate issuance to subscriber**

   No additional stipulations beyond those of [section 4.3.2]().

[4.7.5](). **Conduct constituting acceptance of a re-keyed certificate**

   No additional stipulations beyond those of [section 4.4.1]().

[4.7.6](). **Publication of the re-keyed certificate by the CA**

   No additional stipulations beyond those of [section 4.4.2]().

[4.7.7](). **Notification of certificate issuance by the CA to other entities**

   No additional stipulations beyond those of [section 4.4.3]().

[4.8](). **Certificate modification**

[4.8.1](). **Circumstance for certificate modification**

   Modification of a certificate occurs to implement changes to
   selected attribute values in a certificate. In the context of the
   RPKI, the only changes that are accommodated by certificate
   modification are changes to the INR holdings described by the [RFC
   3779]() extension and changes to the SIA extension.

   When a certificate modification is approved, a new certificate is
   issued. If no INR holdings are removed from the certificate, the new
   certificate MUST contain the same public key and the same expiration
   date as the original certificate, (but with the SIA extension and/or
   the INR set expanded). In this case, revocation of the previous
   certificate is not required.

   When previously distributed INRs are removed from a certificate,
   then the old certificate MUST be revoked and a new certificate MUST
   be issued, reflecting the changed INR holdings. (The SIA extension
   in the new certificate will be unchanged, unless the affected INR
   holder supplies a new SIA value.)

[4.8.2](). **Who may request certificate modification**

   Either the certificate holder or the issuer may initiate the
   certificate modification process.

4.8.3. Processing certificate modification requests

The CA MUST determine that the requested modification is appropriate
and that the procedures for the issuance of a new certificate are
followed (see Section 4.3).

4.8.4. Notification of new certificate issuance to subscriber

No additional stipulations beyond those of section 4.3.2.

4.8.5. Conduct constituting acceptance of modified certificate

No additional stipulations beyond those of section 4.4.1.

4.8.6. Publication of the modified certificate by the CA

No additional stipulations beyond those of section 4.4.2.

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

No additional stipulations beyond those of section 4.4.3.

4.9. Certificate revocation and suspension

4.9.1. Circumstances for revocation

A certificate MUST be revoked (and published on a CRL) if there is
reason to believe that there has been a compromise of a subscriber's
private key. A certificate also MAY be revoked to invalidate a data
object signed by the private key associated with that certificate.
Other circumstances that justify revocation of a certificate MAY be
specified in a CA's CPS.

Note: If new INRs are being added to an organization's existing
distribution, the old certificate need not be revoked. Instead, a
new certificate MAY be issued with both the old and the new
resources and the old key. If INRs are being removed or if there has
been a key compromise, then the old certificate MUST be revoked (and
a re-key MUST be performed in the event of key compromise).

4.9.2. Who can request revocation

This MUST be defined in the CPS of the relevant organization.

4.9.3. Procedure for revocation request

A subscriber MAY submit a request to the certificate issuer for a
revocation. This request MUST identify the certificate to be revoked

and MUST be authenticated. The procedures for making the request
MUST be described in the CPS for each CA. The RPKI provisioning
document [PROV] describes a protocol that MAY be used to make
revocation requests.

A certificate issuer MUST notify the subscriber when revoking a
certificate. The notification requirement is satisfied by CRL
publication. The CPS for a CA MUST indicate the means by which the
CA will inform a subscriber of certificate revocation.

4.9.4. Revocation request grace period

A subscriber SHOULD request revocation as soon as possible after the
need for revocation has been identified. There is no specified grace
period for the subscriber in this process.

4.9.5. Time within which CA must process the revocation request

No stipulation. Each CA SHOULD specify its expected revocation
processing time in its CPS.

4.9.6. Revocation checking requirement for relying parties

A relying party MUST acquire and check the most recent, scheduled
CRL from the issuer of the certificate, whenever the relying party
validates a certificate.

4.9.7. CRL issuance frequency

The CRL issuance frequency MUST be determined by each CA and stated
in its CPS. Each CRL carries a nextScheduledUpdate value and a new
CRL MUST be published at or before that time. A CA MUST set the
nextUpdate value when it issues a CRL, to signal when the next
scheduled CRL will be issued.

4.9.8. Maximum latency for CRLs

The CPS for each CA MUST specify the maximum latency associated with
posting its CRL to the repository system.

4.10. Certificate status services

This PKI does not make provision for use of the Online Certificate
Status Protocol (OCSP) [RFC2560] or Server-Based Certificate
Validation Protocol (SCVP) [RFC5055]. This is because it is
anticipated that the primary RPs (ISPs) will acquire and validate
certificates for all participating resource holders. These protocols
are not designed for such large-scale, bulk certificate status

checking. RPs MUST check for new CRLs at least daily. It is
RECOMMENDED that RPs perform this check several times per day, but
no more than 8-12 times per day (to avoid excessive repository
accesses).

5. Facility, Management, And Operational Controls

5.1. Physical controls

   Each CA MUST maintain physical security controls for its operation
   that are commensurate with those employed by the organization in the
   management of INR distribution. The physical controls employed for
   CA operation MUST be specified in its CPS. Possible topics to be
   covered in the CPS are shown below. (These sections are taken from
   [RFC3647].)

5.1.1. Site location and construction

5.1.2. Physical access

5.1.3. Power and air conditioning

5.1.4. Water exposures

5.1.5. Fire prevention and protection

5.1.6. Media storage

5.1.7. Waste disposal

5.1.8. Off-site backup

5.2. Procedural controls

   Each CA MUST maintain procedural security controls that are
   commensurate with those employed by the organization in the
   management of INR distribution. The procedural security controls
   employed for CA operation MUST be specified in its CPS. Possible
   topics to be covered in the CPS are shown below. (These sections are
   taken from [RFC3647].)

[5.2.1](#). Trusted roles

[5.2.2](#). Number of persons required per task

[5.2.3](#). Identification and authentication for each role

[5.2.4](#). Roles requiring separation of duties

[5.3](#). Personnel controls

   Each CA MUST maintain personnel security controls that are
   commensurate with those employed by the organization in the
   management of INR distribution. The details for each CA MUST be
   specified in its CPS.

[5.4](#). Audit logging procedures

   Details of how a CA implements the audit logging described in this
   section (5.4.1 to 5.4.8) MUST be addressed in its CPS.

[5.4.1](#). Types of events recorded

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

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

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

   . Certificate creation, modification, revocation, or renewal actions

   . Posting of any material to a repository

   . Any attempts to change or delete audit data

   . Key generation

   . Software and/or configuration updates to the CA

   . Clock adjustments

[5.4.2](#). Frequency of processing log

   Each CA MUST establish its own procedures for review of audit logs.

[5.4.3](). Retention period for audit log

   Each CA MUST establish its own polices for retention of audit logs.

[5.4.4](). Protection of audit log

   The audit log SHOULD be protected based on current industry
   standards.

[5.4.5](). Audit log backup procedures

   The audit log SHOULD be backed up based on current industry
   standards.

[5.4.8](). Vulnerability assessments

   The RPKI subsystems of a registry or ISP SHOULD participate in any
   vulnerability assessments that these organizations run as part of
   their normal business practice.

[5.6](). Key changeover

   When a CA wishes to change keys, it MUST acquire a new certificate
   containing its new public key. See [KEYROLL] for a description of
   how key changeover is effected in the RPKI.

[5.8](). CA or RA termination

   In the RPKI, each subscriber acts as a CA authoritative for the
   specified INRs that were distributed to that entity. Procedures
   associated with the termination of a CA MUST be described in the CPS
   for that CA. These procedures MUST include a provision to notify
   each entity that issued a certificate to the organization that is
   operating the CA that is terminating.

   Since the RA function MUST be provided by the same entity operating
   as the CA (see Section 1.3.2), there are no separate stipulations
   for RAs.

6. Technical Security Controls

   The organizations that distribute INRs to network subscribers are
   authoritative for these distributions. This PKI is designed to
   enable ISPs and network subscribers to demonstrate that they are the
   holders of the INRs that have been distributed to them. Accordingly,
   the security controls used by CAs and subscribers for this PKI need
   only to be as secure as those that apply to the procedures for
   administering the distribution of INR data by the extant
   organizations. Details of each CA's security controls MUST be
   described in the CPS issued by the CA.

6.1. Key pair generation and installation

6.1.1. Key pair generation

   In most instances, public-key pairs will be generated by the
   subject, i.e., the organization receiving the distribution of INRs.
   However, some CAs MAY offer to generate key pairs on behalf of their
   subjects at the request of the subjects, e.g., to accommodate
   subscribers who do not have the ability to perform key generation in
   a secure fashion. (The CA has to check the quality of the keys only
   if it generates them (see Section 6.1.6)). Since the keys used in
   this PKI are not for non-repudiation purposes, generation of key
   pairs by CAs does not inherently undermine the security of the PKI.
   Each CA MUST describe its key pair generation procedures in its CPS.

6.1.2. Private key delivery to subscriber

   If a CA provides key pair generation services for subscribers, its
   CPS MUST describe the means by which private keys are delivered to
   subscribers in a secure fashion.

6.1.3. Public key delivery to certificate issuer

   When a public key is transferred to the issuing CA to be certified,
   it MUST be delivered through a mechanism ensuring that the public
   key has not been altered during transit and that the subscriber
   possesses the private key corresponding to the transferred public
   key.

6.1.4. CA public key delivery to relying parties

   CA public keys for all entities (other than trust anchors) are
   contained in certificates issued by other CAs. These certificates
   MUST be published in the RPKI distributed repository system. Relying
   parties download these certificates from the repositories. Public
   key values and associated data for (putative) trust anchors are

distributed out of band and accepted by relying parties on the basis of locally-defined criteria.

6.1.5. Key sizes

The algorithms and key sizes used in the RPKI are specified in "A Profile for Algorithms and Key Sizes for use in the Resource Public Key Infrastructure [ALGKEY].

6.1.6. Public key parameters generation and quality checking

The public key parameters used in the RPKI are specified in [ALGKEY]. Each subscriber is responsible for performing checks on the quality of its key pair. A CA is not responsible for performing such checks for subscribers except in the case where the CA generates the key pair on behalf of the subscriber.

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

The Key usage extension bit values used in the RPKI are specified in RPKI certificate profile [CERTPROF].

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards and controls

The cryptographic module standards and controls employed by each CA MUST be described in the CPS issued by that CA.

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

CAs MAY employ multi-person controls to constrain access to their private keys, but this is not a requirement for all CAs in the PKI. The CPS for each CA MUST describe which, if any, multi-person controls it employs.

6.2.3. Private key escrow

No private key escrow procedures are required for the RPKI.

6.2.4. Private key backup

Because of the adverse operational implications associated with the loss of use of a CA private key in the PKI, each CA MUST employ a secure means to backup its private keys. The details of the procedures for backing up a CA's private key MUST be described in the CPS issued by the CA.

6.2.5. **Private key archival**

   The details of the process and procedures used to archive the CA's
   private key MUST be described in the CPS issued by the CA.

6.2.6. **Private key transfer into or from a cryptographic module**

   The details of the process and procedures used to transfer the CA's
   private key into or from a cryptographic module MUST be described in
   the CPS issued by the CA.

6.2.7. **Private key storage on cryptographic module**

   The details of the process and procedures used to store the CA's
   private key on a cryptographic module and protect it from
   unauthorized use MUST be described in the CPS issued by the CA.

6.2.8. **Method of activating private key**

   The details of the process and procedures used to activate the CA's
   private key MUST be described in the CPS issued by the CA.

6.2.9. **Method of deactivating private key**

   The details of the process and procedures used to deactivate the
   CA's private key MUST be described in the CPS issued by the CA.

6.2.10. **Method of destroying private key**

   The details of the process and procedures used to destroy the CA's
   private key MUST be described in the CPS issued by the CA.

6.2.11. **Cryptographic Module Rating**

   The security rating of the cryptographic module MUST be described in
   the CPS issued by the CA.

6.3. **Other aspects of key pair management**

6.3.1. **Public key archival**

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

6.3.2. Certificate operational periods and key pair usage periods

   The INRs held by a CA may periodically change when it receives new
   distributions. To minimize disruption, the CA key pair MUST NOT
   change when INRs are added to its certificate.

   If ISP and network subscriber certificates are tied to the duration
   of service agreements, these certificates should have validity
   periods commensurate with the duration of these agreements. In any
   case, the validity period for certificates MUST be chosen by the
   issuing CA and described in its CPS.

6.4. Activation data

   Each CA MUST document in its CPS how it will generate, install and
   protect its activation data.

6.5. Computer security controls

   Each CA MUST document the technical security requirements it employs
   for CA computer operation in its CPS.

6.6. Life cycle technical controls

6.6.1. System development controls

   The CPS for each CA MUST document any system development controls
   required by that CA, if applicable.

6.6.2. Security management controls

   The CPS for each CA MUST document the security controls applied to
   the software and equipment used for this PKI. These controls MUST be
   commensurate with those used for the systems used by the CAs for
   managing the INRs.

6.6.3. Life cycle security controls

   The CPS for each CA MUST document how the equipment (hardware and
   software) used for this PKI will be procured, installed, maintained,
   and updated. This MUST be done in a fashion commensurate with the
   way in which equipment for the management and distribution of INRs
   is handled.

6.7. Network security controls

   The CPS for each CA MUST document the network security controls
   employed for CA operation. These MUST be commensurate with the

protection it employs for the computers used for managing
distribution of INRs.

6.8. Time-stamping

The RPKI does not make use of time stamping.

7. Certificate and CRL Profiles

   Please refer to the RPKI Certificate and CRL Profile [CERTPROF].

8. **Compliance Audit And Other Assessments**

   The Certificate Policy for a typical PKI defines the criteria
   against which prospective CAs are evaluated and establishes
   requirements that they must meet. In this PKI, the CAs are already
   authoritative for the management of INRs, and the PKI simply
   supports verification of the distribution of these resources to
   network subscribers. Accordingly, whatever audit and other
   assessments are already used to ensure the security of the
   management of INRs is sufficient for this PKI. The CPS for each CA
   MUST describe what audits and other assessments are used.

9. Other Business And Legal Matters

   As noted throughout this certificate policy, the organizations
   managing the distribution of INRs are authoritative in their roles
   as managers of this data. They MUST operate this PKI to allow the
   holders of INRs to generate digitally signed data that attest to
   these distributions. Therefore, the manner in which the
   organizations in question manage their business and legal matters
   for this PKI MUST be commensurate with the way in which they already
   manage business and legal matters in their existing roles. Since
   there is no single set of responses to this section that would apply
   to all organizations, the topics listed in sections 4.9.1 to 4.9.11
   and 4.9.13 to 4.9.17 of RFC 3647 SHOULD be covered in the CPS issued
   by each CA, although not every CA may choose to address all of these
   topics.

9.12. Amendments

9.12.1. Procedure for amendment

   The procedure for amending this CP is via written notice from the
   IESG in the form of a new (BCP) RFC that updates or obsoletes this
   document.

9.12.2. Notification mechanism and period

   Successive versions of the CP will be published with the statement
   "This CP takes effect on MM/DD/YYYY." MM/DD/YYYY MUST be a minimum
   of 6 months from the date of publication.

9.12.3. Circumstances under which OID must be changed

   If the IESG judges that changes to the CP do not materially reduce
   the acceptability of certificates issued for RPKI purposes, there
   will be no change to the CP OID. If the IESG judges that changes to
   the CP do materially change the acceptability of certificates for
   RPKI purposes, then there MUST be a new CP OID.

10. Security Considerations

   According to X.509, a certificate policy (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." A CP may be used by a relying party to help
   in deciding whether a certificate, and the binding therein, are
   sufficiently trustworthy and otherwise appropriate for a particular
   application. This document describes the CP for the Resource Public
   Key Infrastructure (RPKI). There are separate documents
   (Certification Practice Statements (CPS's)) that cover the factors
   that determine the degree to which a relying party can trust the
   binding embodied in a certificate. The degree to which such a
   binding can be trusted depends on several factors, e.g., the
   practices followed by the certification authority (CA) in
   authenticating the subject; the CA's operating policy, procedures,
   and technical security controls, including the scope of the
   subscriber's responsibilities (for example, in protecting the
   private key), and the stated responsibilities and liability terms
   and conditions of the CA (for example, warranties, disclaimers of
   warranties, and limitations of liability).

   Since name uniqueness within the RPKI cannot be guaranteed, there is
   a risk that two or more CAs in the RPKI will issue certificates and
   CRLs under the same Issuer name. Path validation implementations
   that conform to the resource certification path validation algorithm
   (see [CERTPROF]) verify that the same key was used to sign both the
   target (the resource certificate) and the corresponding CRL. So a
   name collision will not change the result. Use of the basic X.509
   path validation algorithm, which assumes name uniqueness, could
   result in a revoked certificate being accepted as valid or a valid
   certificate being rejected as revoked. Relying parties must ensure
   that the software they use to validate certificates issued under
   this policy verifies that the same key was used to sign both the
   certificate and the corresponding CRL, as specified in [CERTPROF].

11. IANA Considerations

   None.

12. Acknowledgments

   The authors would like to thank Geoff Huston, Randy Bush, Andrei
   Robachevsky and other members of the RPKI community for reviewing
   this document and Matt Lepinski for his help with the formatting.

13. References

13.1. Normative References

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

[RFC2026]   Bradner, S., "The Internet Standards Process - Revision 3",
            BCP 9, RFC 2026, October 1996.

[RFC3779]   Lynn, C., Kent, S., Seo, K., "X.509 Extensions for IP
            Addresses and AS Identifiers", RFC 3779, June 2004.

[REPOS] Huston, G., Loomans, R., and Michaelson, G., "A Profile for
            Resource Certificate Repository Structure", draft-ietf-sidr-
            repos-struct-07.txt, work in progress.

[KEYROLL]   Huston, G., Michaelson, G., Kent, S., "CA Key Rollover in
            the RPKI", draft-ietf-sidr-keyroll-06.txt, work in progress.

[CERTPROF] Huston, G., Michaelson, G., Loomans, R., "A Profile for
            X.509 PKIX Resource Certificates", draft-ietf-sidr-res-certs-
            21.txt, work in progress.

[ALGKEY] Huston, G., "A Profile for Algorithms and Key Sizes for use in
            the Resource Public Key Infrastructure", draft-ietf-sidr-rpki-
            algs-05.txt, work in progress.

13.2. Informative References

[ARCH] Lepinski M., Kent S., "An Infrastructure to Support Secure
            Internet Routing", draft-ietf-sidr-arch-12.txt, work in
            progress.

[PROV] Huston, G., Loomans, R., Ellacott, B., Austein, R., "A Protocol
            for Provisioning Resource Certificates", draft-ietf-sidr-
            rescerts-provisioning-09.txt, work in progress.

[RFC2560]   Myers, M., Ankney, R., Maplani, A., Galperin, S., Adams,
            C., "X.509 Internet Public Key Infrastructure Online
            Certificate Status Protocol - OCSP", RFC 2560, June 1999.

[RFC3647]   Chokhani, S., Ford, W., Sabett, R., Merrill, C., Wu, S.,
       "Internet X.509 Public Key Infrastructure Certificate Policy and
       Certification Practices Framework", RFC 3647, November 2003.

[RFC5055]   Freeman T,, Housley, R., Malpani, A., Cooper, D., Polk, W.,
       "Server-Based Certificate Validation Protocol (SCVP)", RFC5055,
       December 2007.

[RFC5736]   Huston G., Cotton, M., Vegoda, L., "IANA IPv4 Special
       Purpose Address Registry", RFC5736, January 2010.

Authors' Addresses:

   Stephen Kent
   BBN Technologies
   10 Moulton Street
   Cambridge MA 02138
   USA

   Phone: +1 617 873 3988
   Email: skent@bbn.com

   Derrick Kong
   BBN Technologies
   Moulton Street
   Cambridge MA 02138
   USA

   Phone: +1 617 873 1951
   Email: dkong@bbn.com

   Karen Seo
   BBN Technologies
   10 Moulton Street
   Cambridge MA 02138
   USA

   Phone: +1 617 873 3152
   Email: kseo@bbn.com

   Ronald Watro
   BBN Technologies
   10 Moulton Street
   Cambridge MA 02138
   USA

   Phone: +1 617 873 2551
   Email: rwatro@bbn.com