Template for an
Internet Registry's Certification Practice Statement (CPS)
for the Resource PKI (RPKI)
draft-ietf-sidr-cps-irs-05.txt

Status of this Memo

   This Internet-Draft is submitted 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 October 31, 2010.

Abstract

   This document contains a template to be used for creating a
   Certification Practice Statement (CPS) for an Internet Registry
   (e.g., NIR or RIR) that is part of the Resource Public Key
   Infrastructure (RPKI).

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].

Table of Contents

Preface

   This document contains a template to be used for creating a
   Certification Practice Statement (CPS) for an Internet Registry
   (e.g., an NIR or RIR) that is part of the Resource Public Key
   Infrastructure (RPKI). The user of this document should

   1. substitute a title page for page 1 saying, e.g., ''<Name of
      Registry> Certification Practice Statement for the Resource
      Public Key Infrastructure (RPKI)'' with date, author, etc.

   2. delete this Preface

   3. fill in the information indicated below by <text in angle
      brackets>

   4. delete sections 10, 11, 12, 13.1, Acknowledgments, Author's
      Addresses, Intellectual Property Statement, Disclaimer of
      Validity, Copyright Statement, Acknowledgments; leaving a
      reference section with just the references in 13.2

   5. update the table of contents to reflect the deletions and
      additions above.

Note: This CPS is based on the template specified in RFC 3647. A
number of sections contained in the template were omitted from this
CPS because they did not apply to this PKI. However, we have
retained the section numbering scheme employed in the RFC to
facilitate comparison with the outline in the RFC. [There are 4 sub-
sections that I haven't removed yet due to Word problems.)

1. **Introduction**

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

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

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

1.1. **Overview**

This CPS describes:

   . Participants

   . Publication of the certificates and CRLs

   . How certificates are issued, managed, and revoked

   . Facility management (physical security, personnel, audit, etc.)

   . Key management

   . Audit procedures

   . Business and legal issues

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

. CA certificates for each organization distributing INRs and for
  each subscriber (INR holder)

. End entity (EE) certificates for organizations to use to validate
  digital signatures on RPKI-signed objects (see definition in 1.7).

. In the future, the PKI also may include end entity certificates in
  support of access control for the repository system as described
  in 2.4.

1.2. Document name and identification

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

1.3. PKI participants

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

1.3.1. Certification authorities

<Describe the CAs that you will operate for the RPKI. One approach
is to operate two CAs: one designated ''offline'' and the other
designated ''production.'' The offline CA is the top level CA for the
<Name of Registry> portion of the RPKI. It provides a secure
revocation and recovery capability in case the production CA is
compromised or becomes unavailable. Thus the offline CA issues
certificates only to instances of the production CA; and the CRLs it
issues are used to revoke only certificates issued to the production
CA. The production CA is used to issue RPKI certificates to <Name of
Registry> members, to whom INRs have been distributed. >

1.3.2. Registration authorities

<Describe how the registration authority function is handled for the
CA(s) that you operate. The RPKI does not require establishment or

use of a separate registration authority (RA) in conjunction with
the CA function. The RA function will 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

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

1.3.4. Relying parties

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

1.3.5. Other participants

<Name of Registry> will operate a repository that holds
certificates, CRLs, and other RPKI-signed objects.

1.4. Certificate usage

1.4.1. Appropriate certificate uses

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

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

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

1.4.2. Prohibited certificate uses

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

1.5. Policy administration

1.5.1. Organization administering the document

   This CPS is administered by <Name of Registry>.

1.5.2. Contact person

   <Insert Registry contact info here>

1.5.3. Person determining CPS suitability for the policy

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

1.5.4. CPS approval procedures

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

1.6. Definitions and acronyms

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

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

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

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

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

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

          . IP Version 4 addresses,

          . IP version 6 addresses, and

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

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

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

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

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

2. Publication And Repository Responsibilities

2.1. Repositories

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

   The <Name of Registry> RPKI CA will publish certificates, CRLs, and
   RPKI-signed objects via a repository that is accessible via RSYNC at
   rpki.<Name of Registry>.net.

2.2. Publication of certification information

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

2.3. Time or Frequency of Publication

   <Describe here your procedures for publication (via the repository)
   of the certificates, CRLs and RPKI-signed objects that you issue. If
   you choose to outsource publication of PKI data, you still need to
   provide this information for relying parties. This should include
   the period of time within which a certificate will be published
   after he CA issues the certificate and the period of time within
   which a CA will publish a CRL with an entry for a revoked
   certificate after it revokes that certificate. >

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

   The <Name of Registry> RPKI CA MUST publish its CRL prior to the
   nextScheduledUpdate value in the scheduled CRL previously issued by
   the CA.

2.4. Access controls on repositories

   Access to the repository system, for modification of entries, must
   be controlled to prevent denial of service attacks. All data
   (certificates, CRLs and RPKI-signed objects) published to a
   repository are digitally signed. RPKI items that <Name of Registry>
   issues MUST be published to the repository that it runs by means not
   accessible to the outside world. <If <Name of Registry> offers
   repository services to its subscribers, then <describe here the
   protocol(s) that you support for their publishing of signed
   objects.>

[3](). Identification And Authentication

[3.1](). Naming

[3.1.1](). Types of names

   The Subject of each certificate issued by this Registry is
   identified by an X.500 Distinguished Name (DN). The distinguished
   name will consist of a single Common Name (CN) attribute with a
   value generated by <Name of Registry>. 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 subscriber certificate will be unique
   relative to all certificates issued by <Name of Registry>. However,
   there is no guarantee that the subject name will be globally unique
   in this PKI. Also, the name of the subscriber need not to be
   ''meaningful'' in the conventional, human-readable sense. The
   certificates issued under this PKI are used for authorization in
   support of applications that make use of attestations of Internet
   resource holding, not for identification

[3.1.3](). Anonymity or pseudonymity of subscribers

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

[3.1.4](). Rules for interpreting various name forms

   None

[3.1.5](). Uniqueness of names

   <Name of Registry> certifies Subject names that are unique among the
   certificates that it issues. Although it is desirable that these
   Subject names be unique throughout the PKI, to facilitate
   certificate path discovery, such uniqueness is neither mandated nor
   enforced through technical means.

[3.1.6](#). **Recognition, authentication, and role of trademarks**

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

[3.2](#). **Initial identity validation**

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

   <Describe the method whereby each subscriber will be required to
   demonstrate proof-of-possession (PoP) of the private key
   corresponding to the public key in the certificate, prior to <Name
   of Registry's> issuing the certificate. One possible approach makes
   use of the PKCS #10 format, as profiled in [[RFCyyyy](#)]. 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**

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

   <Describe the method whereby this is accomplished. For example, a
   BPKI certificate could be used to authenticate a certificate request
   that serves as a link to the <Name of Registry> subscriber database
   that maintains the INR distribution records. The certificate request
   could be matched against the database record for the subscriber in
   question, and an RPKI certificate would be issued only if the INRs
   requested were a subset of those held by the subscriber.>

[3.2.3](#). **Authentication of individual identity**

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

   < Describe the procedures that MUST be used to identify at least one
   individual as a representative of each subscriber. This is done in
   support of issuance, renewal, and revocation of the certificate
   issued to the organization. For example, one might say ''The <Name of
   Registry> BPKI (see [Section 3.2.6](#)) issues certificates that MUST be

used to identify individuals who represent <Name of Registry>
subscribers.'' The procedures should be commensurate with those you
already employ in authenticating individuals as representatives for
INR holders. Note that this authentication is solely for use by you
in dealing with the organizations to which you distribute (or sub-
distribute) INRs, and thus must not be relied upon outside of this
CA-subscriber relationship>

3.2.4. Non-verified subscriber information

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

3.2.5. Validation of authority

<Describe what procedures that MUST be used to verify that an
individual claiming to represent a subscriber, is authorized to
represent that subscriber in this context. For example, one could
say, ''Only an individual to whom a BPKI certificate (see Section
3.2.6) has been issued may request issuance of an RPKI certificate.
Each certificate issuance request is verified using the BPKI.'' The
procedures should be commensurate with those you already employ as a
registry in authenticating individuals as representatives of
subscribers.>

3.2.6. Criteria for interoperation

The RPKI is neither intended nor designed to interoperate with any
other PKI. <If you operate a separate, additional PKI for business
purposes (BPKI), then describe (or reference) how the BPKI is used
to authenticate subscribers and to enable them to manage their
resource distributions.>

3.3. Identification and authentication for re-key requests

3.3.1. Identification and authentication for routine re-key

<Describe the conditions under which routine re-key is required and
the manner by which it is requested. Describe the procedures that
MUST be used to ensure that a subscriber requesting routine re-key
is the legitimate holder of the certificate to be re-keyed. State
the approach for establishing PoP of the private key corresponding
to the new public key. If you operate a BPKI, describe how that BPKI
is used to authenticate routine re-key requests.>

3.3.2. Identification and authentication for re-key after revocation

   <Describe the procedures that MUST be used to ensure that an
   organization requesting a re-key after revocation is the legitimate
   holder of the INRs in the certificate being re-keyed. This should
   also include the method employed for verifying PoP of the private
   key corresponding to the new public key. If you operate a business-
   based PKI, describe how that BPKI is used to authenticate re-key
   requests and refer to 3.2.6. With respect to authentication of the
   subscriber, the procedures should be commensurate with those you
   already employ in the maintenance of INR distribution records.>

3.4. Identification and authentication for revocation request

   <Describe the procedures that MUST be used by an RPKI subscriber to
   make a revocation request. Describe the manner by which it is
   ensured that the subscriber requesting revocation is the subject of
   the certificate (or an authorized representative thereof) to be
   revoked. 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.
   These procedures should be commensurate with those you already
   employ in the maintenance of subscriber records.>

   Note that if a Subscriber requests a new INR distribution, an
   existing RPKI certificate issued to the subscriber is NOT revoked,
   so long as the set of INRs distributed to the subscriber did not
   ''shrink,'' i.e., the new INRs are a superset of the old INR set.
   However, if a new INR distribution results in ''shrinkage'' of the set
   of INRs distributed to a subscriber, this triggers an implicit
   revocation of the old RPKI 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 subscriber who holds INRs distributed by this registry may
   submit a certificate application to this CA.

4.1.2. Enrollment process and responsibilities

   <Describe your enrollment process for issuing certificates both for
   initial deployment of the PKI and as an ongoing process. Note that
   most of the certificates in this PKI are issued as part of your
   normal business practices, as an adjunct to INR distribution, and
   thus a separate application to request a certificate may not be
   necessary. If so, reference should be made to where these practices
   are documented.>

4.2. Certificate application processing

   <Describe the certificate request/response processing that you will
   employ. You should make use of existing standards for certificate
   application processing. Relevant standards include RFC 4210,
   Internet X.509 Public Key Infrastructure Certificate Management
   Protocol (CMP), RFC 2797, Certificate Management Messages over CMS,
   and RSA Labs standards PKCS #7 and PKCS #10. >

4.2.1. Performing identification and authentication functions

   <Describe your practices for identification and authentication of
   certificate applicants. Often, existing practices employed by you
   to identify and authenticate organizations can be used as the basis
   for issuance of certificates to these subscribers. Reference can be
   made to documentation of such existing practices.>

4.2.2. Approval or rejection of certificate applications

   <Describe your practices for approval or rejection of applications
   and refer to documentation of existing business practices relevant
   to this process. Note that according to the CP, certificate
   applications will be approved based on the normal business practices
   of the entity operating the CA, based on the CA's records of
   subscribers. The CP also says that each CA will 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 requester.>

4.2.3. **Time to process certificate applications**

<Specify here your expected time frame for processing certificate
applications.>

4.3. **Certificate issuance**

4.3.1. **CA actions during certificate issuance**

<Describe in this section your procedures for issuance and
publication of a certificate.>

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

<Name of registry> MUST notify the subscriber when the certificate
is published. <Describe here any other entities that will be
notified when a new certificate is published.>

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

<Describe here any other entities that will be notified when a new
certificate is published.>

4.4. **Certificate acceptance**

4.4.1. **Conduct constituting certificate acceptance**

When a certificate is issued, the CA MUST publish it to the
repository and notify the subscriber. This will be done without
subscriber review and acceptance.

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 <name of Registry>'s
repository publication. This will be done within <specify the
timeframe within which the certificate will be placed in the
repository and the subscriber will be notified>. <Describe your
procedures for publication of the certificate.>

4.5. **Key pair and certificate usage**

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

4.5.1. Subscriber private key and certificate usage

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

4.5.2. Relying party public key and certificate usage

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

4.6. Certificate renewal

4.6.1. Circumstance for certificate renewal

As per the CP, a certificate MUST be processed for renewal based on its expiration date or a renewal request from the certificate Subject. The request may be implicit, a side effect of renewing its resource holding agreement, or may be explicit. If <Name of Registry> initiates the renewal process based on the certificate expiration date, then <Name of Registry> will notify the subscriber <insert the period of advance warning, e.g., ''2 weeks in advance of the expiration date'', or the general policy, e.g., ''in conjunction with notification of service expiration''.> The validity interval of the new (renewed) certificate will overlap that of the previous certificate by <insert length of overlap period, e.g., 1 week>, to ensure uninterrupted coverage.

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

4.6.2. Who may request renewal

The subscriber or <Name of Registry> may initiate the renewal process. <For the case of the subscriber, describe the procedures that will be used to ensure that the requester is the legitimate holder of the INRs in the certificate being renewed. This should also include the method employed for verifying PoP of the private

key corresponding to the public key in the certificate being renewed
or the new public key if the public key is being changed. With
respect to authentication of the subscriber, the procedures should
be commensurate with those you already employ in the maintenance of
INR distribution records. If you operate a BPKI for this, describe
how that business-based PKI is used to authenticate re-newal
requests and refer to 3.2.6.>

4.6.3. Processing certificate renewal requests

<Describe your procedures for handling certificate renewal requests.
This must include verification that the requester is the subscriber
or is authorized by the subscriber and that the certificate in
question has not been revoked.>

4.6.4. Notification of new certificate issuance to subscriber

<Name of Registry> MUST notify the subscriber when the certificate
is published. <Describe your procedure for notification of new
certificate issuance to the subscriber. This should be consistent
with 4.3.2.>

4.6.5. Conduct constituting acceptance of a renewal certificate

When a renewal certificate is issued, <Name of Registry> MUST
publish it to the repository and notify the subscriber. This will be
done without subscriber review and acceptance.

4.6.6. Publication of the renewal certificate by the CA

<Describe your policy and procedures for publication of a renewal
certificate. This should be consistent with 4.4.2.>

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

<List here any other entities (besides the subscriber) who will be
notified when a renewed certificate is issued.>

4.7. Certificate re-key

4.7.1. Circumstance for certificate re-key

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

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

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

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

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

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

4.7.2. Who may request certification of a new public key

  Only the subscriber may request a re-key. In addition, <Name of
  Registry> may initiate a re-key based on a verified compromise
  report. <If the subscriber (certificate Subject) requests the rekey,
  describe how authentication is effected, e.g., using the <Name of
  Registry> BPKI. Describe how a compromise report received from other
  than a subscriber is verified.>

4.7.3. Processing certificate re-keying requests

  <Describe your process for handling re-keying requests. As per the
  CP, this should be consistent with the process described in Section
  4.3. So reference can be made to that section.>

4.7.4. Notification of new certificate issuance to subscriber

  <Describe your policy regarding notifying the subscriber re:
  availability of the new re-keyed certificate. This should be
  consistent with the notification process for any new certificate
  issuance (see section 4.3.2).>

4.7.5. Conduct constituting acceptance of a re-keyed certificate

  When a re-keyed certificate is issued, the CA will publish it in the
  repository and notify the subscriber. This will be done without
  subscriber review and acceptance.

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

   <Describe your policy regarding publication of the new certificate.
   This should be consistent with the publication process for any new
   certificate (see section 4.4.2).>

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

   <List here any entities (other than the subscriber) who will be
   notified when a re-keyed certificate is issued.>

4.8. Certificate modification

4.8.1. Circumstance for certificate modification

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

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

4.8.2. Who may request certificate modification

   The subscriber or <Name of Registry> may initiate the certificate
   modification process. <For the case of the subscriber, state here
   what steps will be taken to verify the identity and authorization of
   the entity requesting the modification.>

4.8.3. Processing certificate modification requests

   <Describe your procedures for verification of the modification
   request and procedures for the issuance of a new certificate. These
   should be consistent with the processes described in Sections 4.2
   and 4.3.1.>

4.8.4. Notification of modified certificate issuance to subscriber

   <Describe your procedure for notifying the subscriber about the
issuance of a modified certificate. This should be consistent with
the notification process for any new certificate (see section
4.3.2).>

4.8.5. Conduct constituting acceptance of modified certificate

   When a modified certificate is issued, the <Name of Registry> will
publish in the repository and notify the subscriber. This will be
done without subscriber review and acceptance.

4.8.6. Publication of the modified certificate by the CA

   <Describe your procedure for publication of a modified certificate.
This should be consistent with the publication process for any new
certificate (see section 4.4.2).>

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

   <List here any entities (other than the subscriber) who will be
notified when a modified certificate is issued.>

4.9. Certificate revocation and suspension

4.9.1. Circumstances for revocation

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

4.9.2. Who can request revocation

   The subscriber or <Name of Registry> may request a revocation. <For
the case of the subscriber, describe what steps will be taken to
verify the identity and authorization of the entity requesting the
revocation.>

4.9.3. Procedure for revocation request

<Describe your process for handling a certificate revocation request. This should include:

o Procedure to be used by the subscriber to request a revocation

o Procedure for notification of the subscriber when the revocation is initiated by <Name of ISP>.>

4.9.4. Revocation request grace period

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

4.9.5. Time within which CA must process the revocation request

<Describe your policy on the time period within which you will process a revocation request.>

4.9.6. Revocation checking requirement for relying parties

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

4.9.7. CRL issuance frequency

<State the CRL issuance frequency for the CRLs that you publish.> Each CRL will carry a nextScheduledUpdate value; and a new CRL will be published at or before that time. <Name of Registry> will set the nextScheduledUpdate value when it issues a CRL, to signal when the next scheduled CRL will be issued.

4.9.8. Maximum latency for CRLs

A CRL will be published to the repository system within <state the maximum latency> after generation.

4.10. Certificate status services

<Name of Registry> does not support OCSP or SCVP. <Name of Registry> issues CRLs.

5. Facility, Management, and Operational Controls

5.1. Physical controls

   <As per the CP, describe the physical controls that you employ for
   certificate management. These should be commensurate to those used
   in the management of INR distribution.>

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

   <As per the CP, describe the procedural security controls that you
   employ for certificate management. These should be commensurate to
   those used in the management of INR distribution.>

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

   <As per the CP, describe the personnel security controls that you
   employ for individuals associated with certificate management. These
   should be commensurate to those used in the management of INR
   distribution.>

[5.3.1](). Qualifications, experience, and clearance requirements

[5.3.2](). Background check procedures

[5.3.3](). Training requirements

[5.3.4](). Retraining frequency and requirements

[5.3.5](). Job rotation frequency and sequence

[5.3.6](). Sanctions for unauthorized actions

[5.3.7](). Independent contractor requirements

[5.3.8](). Documentation supplied to personnel

[5.4](). Audit logging procedures

   <As per the CP, describe in the following sections the details of
   how you implement audit logging.>

[5.4.1](). Types of events recorded

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

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

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

   Certificate creation, modification, revocation, or renewal actions

   Posting of any material to a repository

   Any attempts to change or delete audit data

   <List here any additional types of events that will be audited.>

[5.4.2](). Frequency of processing log

   <Describe your procedures for review of audit logs.>

[5.4.3](). Retention period for audit log

   <Describe your policies for retention of audit logs.>

5.4.4. Protection of audit log

   <Describe your policies for protection of the audit logs.>

5.4.5. Audit log backup procedures

   <Describe your policies for backup of the audit logs.>

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

5.4.7. Notification to event-causing subject [OMITTED]

5.4.8. Vulnerability assessments

   <Describe any vulnerability assessments that you will apply (or have
   already applied) to the PKI subsystems. This should include whether
   such assessments have taken place and any procedures or plans to
   perform or repeat/reassess vulnerabilities in the future.>

5.5. Records archival [OMITTED]

5.6. Key changeover

   The <Name of Registry> CA certificate will contain a validity period
   that is at least as long as that of any certificate being issued
   under that certificate. When <Name of Registry> CA wishes to change
   keys, <Name of Registry> will create a new signature key pair, and
   acquire and publish a new certificate containing the public key of
   the pair, <specify here the minimum amount of lead time, e.g., ''a
   minimum of 6 months''> in advance of the scheduled change of the
   current signature key pair.

5.7. Compromise and disaster recovery [OMITTED]

5.8. CA or RA termination

   <Describe your policy for management of your CA's INR distributions
   in case of its own termination.>

6. Technical Security Controls

   This section describes the security controls used by <Name of
   Registry>.

6.1. Key pair generation and installation

6.1.1. Key pair generation

   <Describe the procedures that will be used to generate the CA key
   pair, and, if applicable, key pairs for subscribers. In most
   instances, public-key pairs will be generated by the subscriber,
   i.e., the organization receiving the distribution of INRs. However,
   your procedures may include one for generating key pairs on behalf
   of your subscribers if they so request. (This might be done for
   subscribers who do not have the ability to perform key generation in
   a secure fashion or who want a registry to provide backup for the
   subscriber private key.) 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.>

6.1.2. Private key delivery to subscriber

   <If the procedures in 6.1.1 include providing key pair generation
   services for subscribers, describe the means by which private keys
   are delivered to subscribers in a secure fashion. Otherwise say this
   is not applicable.>

6.1.3. Public key delivery to certificate issuer

   <Describe the procedures that will be used to deliver a subscriber's
   public keys to the <Name of Registry> RPKI CA. These procedures
   should ensure 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 and MUST be published
   to the RPKI repository system. Relying parties MUST download these
   certificates from this system. Public key values and associated data
   for (putative) trust anchors MUST be distributed out of band and
   accepted by relying parties on the basis of locally-defined
   criteria, e.g., embedded in path validation software that will be
   made available to the Internet community.

6.1.5. **Key sizes**

   The key sizes used in this PKI are as specified in RFC ZZZZ
   [RFCzzzz]. <Describe any deviations from this statement.>

6.1.6. **Public key parameters generation and quality checking**

   The public key algorithms and parameters used in this PKI are as
   specified in RFC ZZZZ [RFCzzzz]. <Describe any deviations from this
   statement.>

   <If the procedures in 6.1.1 include subscriber key pair generation,
   EITHER insert here text specifying that the subscriber is
   responsible for performing checks on the quality of its key pair and
   saying that <Name of Registry> is not responsible for performing
   such checks for subscribers OR describe the procedures used by the
   CA for checking the quality of these subscriber key pairs.>

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

   The Key usage extension bit values will be consistent with RFC 5280.
   For <Name of Registry>'s CA certificates, the keyCertSign and
   cRLSign bits will be set TRUE. All other bits (including
   digitalSignature) will be set FALSE, and the extension will be
   marked critical. <Specify whether end entity certificates (e.g.,
   issued by the CA for its operators) will include this extension and
   if so, the appropriate bit values as per RFC 5280.>

6.2. **Private Key Protection and Cryptographic Module Engineering
     Controls**

6.2.1. **Cryptographic module standards and controls**

   The <Name of Registry> CA employs a cryptographic module evaluated
   under FIPS 140-2/3, at level 3 [FIPS].

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

   <If you choose to use multi-person controls to constrain access to
   your CA's private keys, then insert the following text. ''There will
   be private key <insert here n> out of <insert here m> multi-person
   control.''>

6.2.3. **Private key escrow**

   No private key escrow procedures are required for this PKI.

6.2.4. **Private key backup**

   <Describe the procedures used for backing up your CA's private key.
   The following aspects should be included. (1) The copying should be
   done under the same multi-party control as is used for controlling
   the original private key. (2) At least one copy should be kept at
   an off-site location for disaster recovery purposes.>

6.2.5. **Private key archival**

   See sections 6.2.3 and 6.2.4

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

   The private keys for <Name of Registry>'s production CA < if
   appropriate, change ''production CA'' to ''production and offline CAs''>
   MUST be generated by the cryptographic module specified in 6.2.1.
   The private keys will never leave the module except in encrypted
   form for backup and/or transfer to a new module.

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

   The private key for <Name of Registry>'s production CA <if
   appropriate, change ''production CA'' to ''production and offline CAs''>
   MUST be stored in the cryptographic module and will be protected
   from unauthorized use in accordance with the FIPS 140-2/3
   requirements applicable to the module. (See [FIPS])

6.2.8. **Method of activating private key**

   <Describe the mechanisms and data used to activate your CA's private
   key.>

6.2.9. **Method of deactivating private key**

   The cryptographic module, when activated, will not be left
   unattended. After use, it will be deactivated by <Describe the
   procedure for deactivation of your CA's private key.> The module
   will be stored securely when not in use.

6.2.10. **Method of destroying private key**

   <Describe the method used for destroying your CA's private key,
   e.g., when it is superseded. This will depend on the particular
   module.>

6.2.11. Cryptographic Module Rating

   The cryptographic module used by the <Name of Registry> production
   CA will be certified FIPS 140-2/3, at level 3 [FIPS].

6.3. Other aspects of key pair management

6.3.1. Public key archival

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

6.3.2. Certificate operational periods and key pair usage periods

   The <Name of Registry> CA's key pair will have a validity interval
   of <insert number of years -   - Registry
key pairs and certificates
   should have long validity intervals, e.g., 10 years, to minimize the
   disruption caused by key changeover for top tier CAs.>

6.4. Activation data

6.4.1. Activation data generation and installation

   <Describe how activation data for your CA will be generated.>

6.4.2. Activation data protection

   Activation data for the CA private key will be protected by
   <Describe your procedures here>.

6.4.3. Other aspects of activation data

   <Add here any details you wish to provide with regard to the
   activation data for your CA. If there are none, say ''None.''>

6.5. Computer security controls

6.5.1. Specific computer security technical requirement

   <Describe your security requirements for the computers used to
   support this PKI, e.g., requirements for authenticated logins, audit
   capabilities, etc. These requirements should be commensurate with
   those used for the computers used for managing distribution of
   INRs.>

6.6. Life cycle technical controls

6.6.1. System development controls

   <Describe any system development controls that you will apply to the
   PKI systems, e.g., use of Trusted System Development Methodology
   (TSDM) Level 2.>

6.6.2. Security management controls

   <Describe the security management controls that will be used for the
   RPKI software and equipment employed by the CA. These security
   measures should be commensurate with those used for the systems used
   by the CAs for managing and distributing INRs.>

6.6.3. Life cycle security controls

   <Describe how the equipment (hardware and software) used for RPKI
   functions will be procured, installed, maintained, and updated.
   This should 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

   <Describe the network security controls that will be used for CA
   operation. These should be commensurate with the network security
   controls employed 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

8. Please refer to the Certificate and CRL Profile [RFCyyyy].

Compliance Audit and Other Assessments

   <List here any audit and other assessments used to ensure the
   security of the administration of INRs. These are sufficient for the
   RPKI systems.>

8.1. Frequency or circumstances of assessment

8.2. Identity/qualifications of assessor

8.3. Assessor's relationship to assessed entity

8.4. Topics covered by assessment

8.5. Actions taken as a result of deficiency

8.6. Communication of results

9. Other Business And Legal Matters

   <The sections below are optional. Fill them in as appropriate for
   your organization. The CP says that CAs should cover 9.1 to 9.11 and
   9.13 to 9.17 although not every CA will choose to do so. Note that
   the manner in which you manage your business and legal matters for
   this PKI should be commensurate with the way in which you manage
   business and legal matters for the distribution of INRs.>

9.1. Fees

9.1.1. Certificate issuance or renewal fees

9.1.2. Fees for other services (if applicable)

9.1.3. Refund policy

9.2. Financial responsibility

9.2.1. Insurance coverage

9.2.2. Other assets

9.2.3. Insurance or warranty coverage for end-entities

9.3. Confidentiality of business information

9.3.1. Scope of confidential information

9.3.2. Information not within the scope of confidential information

9.3.3. Responsibility to protect confidential information

9.4. Privacy of personal information

9.4.1. Privacy plan

9.4.2. Information treated as private

9.4.3. Information not deemed private

9.4.4. Responsibility to protect private information

9.4.5. Notice and consent to use private information

9.4.6. Disclosure pursuant to judicial or administrative process

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

9.16.5. Force Majeure

10. Security Considerations

   The degree to which a relying party can trust the binding embodied
   in a certificate depends on several factors. These factors can
   include 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). This document provides a
   framework to address the technical, procedural, personnel, and
   physical security aspects of Certification Authorities, Registration
   Authorities, repositories, subscribers, and relying party
   cryptographic modules, in order to ensure that the certificate
   generation, publication, renewal, re-key, usage, and revocation is
   done in a secure manner. Specifically, Section 3 Identification and
   Authentication (I&A); Section 4 Certificate Life-Cycle Operational
   Requirements; Section 5 Facility Management, and Operational
   Controls; Section 6 Technical Security Controls; Section 7
   Certificate and CRL Profiles; and Section 8 Compliance Audit and
   Other Assessments are oriented towards ensuring secure operation of
   the PKI entities such as CA, RA, repository, subscriber systems, and
   relying party systems.

11. IANA Considerations

   None.

12. Acknowledgments

   The authors would like to thank Geoff Huston for reviewing this
   document, Matt Lepinski for his help with the formatting, and Ron
   Watro for assistance with editing.

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.

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

   [RFCxxxx]   Seo, K., Watro, R., Kong, D., and Kent, S.,
        ''Certificate Policy for the Resource PKI (RPKI),'' work in
        progress.

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

   [RFCzzzz]   Huston, G., ''A Profile for Algorithms and Key Sizes for
        use in the Resource Public Key Infrastructure,'' work in
        progress.

13.2. Informative References

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

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

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

Author's 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
    10 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

Pre-5378 Material Disclaimer

   This document may contain material from IETF Documents or IETF
   Contributions published or made publicly available before November
   10, 2008. The person(s) controlling the copyright in some of this
   material may not have granted the IETF Trust the right to allow
   modifications of such material outside the IETF Standards Process.
   Without obtaining an adequate license from the person(s) controlling
   the copyright in such materials, this document may not be modified
   outside the IETF Standards Process, and derivative works of it may
   not be created outside the IETF Standards Process, except to format
   it for publication as an RFC or to translate it into languages other
   than English.