RIPE NCC Certification Practice Statement (CPS) for the Resource Public Key Infrastructure (RPKI)

Author: RIPE NCC
Document ID: ripe-751
Updates: ripe-549
Date: February 2021

Last updated February 2021

Table of Contents

1. Introduction

As per Certification Policy (CP) [RFC 6484]:

This document is the Certification Practice Statement of the RIPE NCC. It describes the practices employed by the RIPE NCC Certification Authority (CA) in the Resource Public Key Infrastructure (RPKI). These practices are defined in accordance with the requirements of the Certificate Policy (CP) [RFC 6484] for RPKI.

RPKI is designed to support the validation of claims by the current holders of Internet number resources (INRs), in accordance with the records of the organisations that act as CAs in this PKI. The ability to verify these claims is essential to ensuring the unique and unambiguous distribution of these resources.

The structure of the Resource PKI is congruent with the number resource allocation framework of the Internet and parallels the existing INR distribution hierarchy. These INRs are distributed by the Internet Assigned Numbers Authority (IANA) to the Regional Internet Registries (RIRs), among others, as well as for special purposes [RFC 8190]. The RIRs manage the allocation of number resources to End Users, Internet Service Providers (ISPs), and others.

In some regions, National Internet Registries (NIRs) are an additional tier in the INR distribution hierarchy, beneath the RIRs. Internet Service Providers (ISPs) and network subscribers then form further tiers below these registries.

This PKI encompasses several types of certificates (see RFC 6480 for more details):

- CA certificates for each organisation distributing INRs and for each subscriber INR holder
- End-entity (EE) certificates for organisations to use to validate digital signatures on RPKI-signed objects
- In the future, the PKI may also include end-entity certificates in support of access control for the repository system, as described in Section 2.4

In addition to the CP [RFC 6484], relevant information about general PKI concepts may be found in [RFC 5280], "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

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].

1.1. Overview

This CPS describes:

- Participants
- Publication of the certificates and Certificate Revocation Lists (CRLs)
- How certificates are issued, managed, re-keyed, renewed, and revoked
- Facility management (physical security, personnel, audit, etc.)
- Key management
- Audit procedures

The Certification Practice Statement (CPS) is for convenience and informational purposes only. The RIPE NCC Certification Service Terms and Conditions and the RIPE NCC Certification Repository Terms and Conditions prevail over the CPS. The CPS does not affect the interpretation of these Terms and Conditions.

This PKI encompasses several types of certificates:

- CA certificates for each organisation distributing INRs and for each subscriber INR holder
- End-entity (EE) certificates for organisations to validate digital signatures on RPKI-signed objects
- In the future, the PKI may also include end-entity certificates in support of access control for the repository system, as described in Section 2.4.

1.2. Document Name and Identification

The name of this document is "RIPE NCC Certification Practice Statement for the Resource Public Key Infrastructure".

1.3. PKI Participants

As per the CP [RFC 6484]:

Note that in a PKI, the term "subscriber" refers to an individual or organisation 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 organisation 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 organisations or entities, even though some of them are individuals.

1.3.1. Certification Authorities (CAs)

This CPS covers five types of CAs for the RPKI: one Offline CA for the RIPE NCC, one All Resources CA (ACA) for the RIPE NCC, one Production CA, a number of Hosted CAs, and a number of Delegated CAs, which are all equivalent and may be described as a single CA for the purpose of this document.

The Offline CA is the top-level CA for the RIPE NCC portion of RPKI, allowing the RIPE NCC to act as a Trust Anchor in the RPKI.

The ACA allows the RIPE NCC to act as parent of the Production CA, which in turn acts as a parent CA to RIPE NCC Members and the Delegated CA. This three-layer approach provides a secure revocation and recovery capability in case the ACA is compromised or becomes unavailable. Thus, the Offline CA issues certificates only to instances of the ACA, and the CRLs it issues are used to revoke only certificates issued to the ACA.

The ACA 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 RIPE NCC members, End Users, and Delegated CAs, to whom Internet number resources have been distributed.

In addition, the RIPE NCC offers a hosted CA service to RIPE NCC members and End Users. These CAs are designated "hosted CAs". Hosted CAs are highly automated, taking care of the major part of the operational burden for RIPE NCC Members who want to act as CAs in the RPKI.

See section 1.6 for definitions and acronyms used in this document.

1.3.2. Registration Authorities

There is no distinct Registration Authority (RA) for either the Offline CA, ACA, and the Production CA operating under this CPS. The former needs no distinct RA capability because it issues certificates only to the Online CA. The Online CA depends on the single sign-on (SSO) mechanism used by the LIR Portal to identify individuals authorised to make requests. One of the possible sign-on mechanisms is by using an X.509 client certificate issued by the RIPE NCC Business PKI (see section 3.2.6. for more details). The RIPE NCC already establishes a contractual relationship with each subscriber (RIPE NCC member) and assumes responsibility for distributing

and tracking the current allocation of address space and AS Numbers. Since the RIPE NCC operates the LIR Portal sign-on service and BPKI CA, no distinct RA is used.

1.3.3. Subscribers

Organisations receiving Provider Aggregatable (PA) INR allocations from this CA, as well as organisations receiving Provider Independent (PI) INR resources, are subscribers to the RPKI service. All RIPE NCC members and End Users can receive distributions of IP addresses and AS Numbers from the RIPE NCC CA and thus are subscribers in the PKI.

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

The RIPE NCC operates a repository that holds certificates, CRLs and other RPKI-signed objects, such as Route Origin Authorisation (ROA) objects. RIPE NCC Repository is regulated by the RIPE NCC Certification Repository Terms and Conditions.

1.4. Certificate Usage

1.4.1. Appropriate certificate uses

The certificates issued under this hierarchy are for authorisation in support of validation of claims of current holdings of INRs. Additional uses, consistent with the basic goal cited above, are also permitted under [RFC 6484].

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 Section 2.4.) Such uses are also permitted under the RPKI certificate policy.

With regard to routing security, an initial goal of this PKI is to enable the holder of a set of address blocks to declare, in a secure fashion, the AS Number of each entity that is authorised to originate a route to these addresses, including the context of ISP proxy aggregation. Additional uses of the PKI, consistent with the basic goal cited above, are also permitted under this policy.

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. Organisation administering the document

This CPS is administered by

RIPE NCC
Stationsplein 11
1012 AB Amsterdam
The Netherlands

Whenever the implementation is changed, this CPS will be modified and republished as a RIPE Document. This will be announced through the appropriate channels, such as the RIPE NCC's Membership Announce mailing list (ncc-announce@ripe.net).

1.5.2. Contact person

The contact information is:

Email: ncc@ripe.net
Phone: +31 20 535 4444

1.5.3. Person determining CPS suitability for the policy

This document is reviewed by qualified RIPE NCC staff, as well as by an external party during the review process.

1.5.4. CPS approval procedures

This CPS is not subject to the RIPE Policy Development Process (PDP). It provides a detailed outline of the implementation of the RPKI by the RIPE NCC. The CPS is publicly available. When necessary, additional reporting mechanisms, such as mailing lists or presentations at RIPE Meetings, will be used to communicate its contents. In the event that RPKI implementation becomes inconsistent with applicable policies, the RIPE NCC will update the implementation of this CPS.

1.6. Definitions and Acronyms

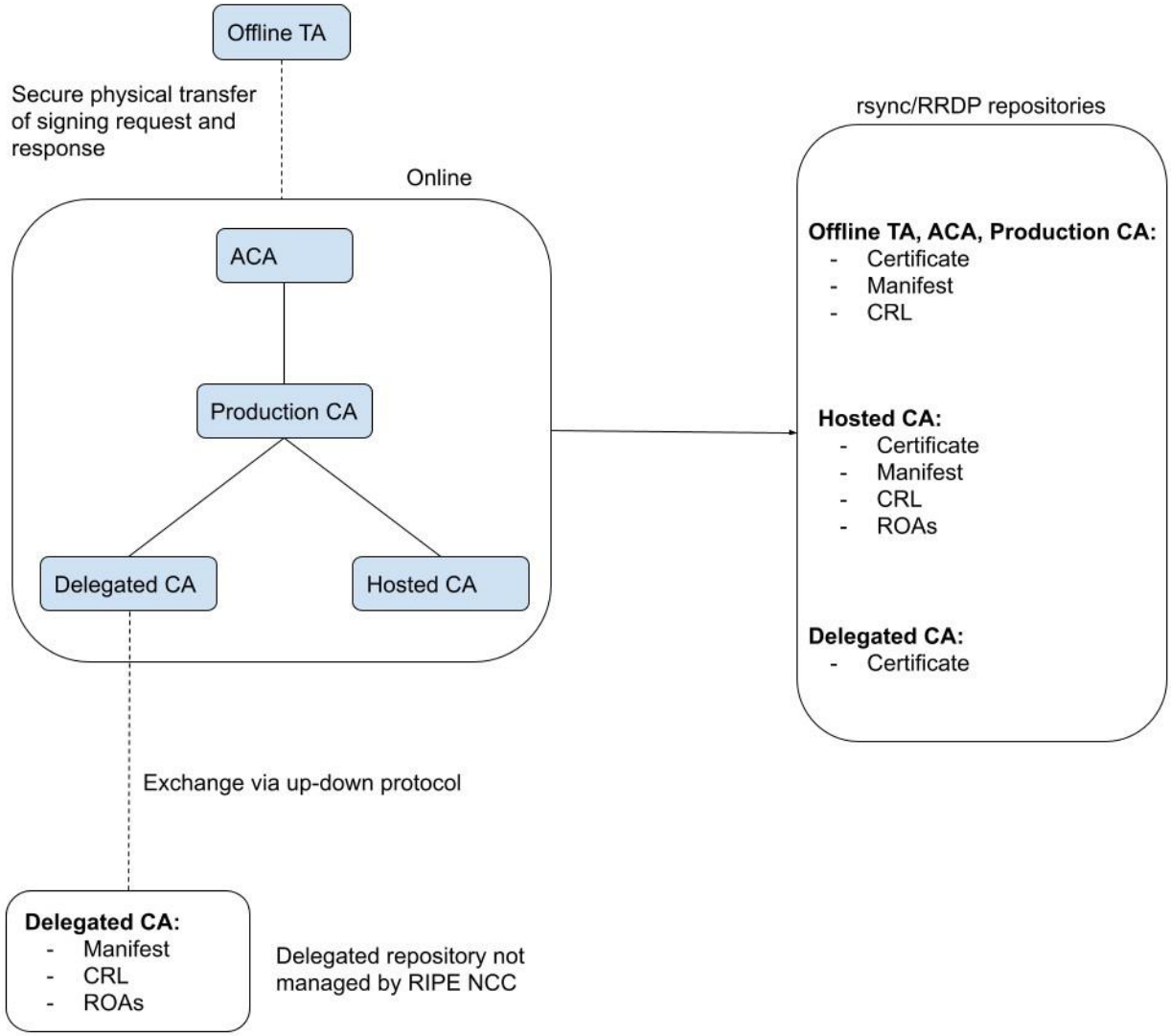
BPKI	Business PKI. A BPKI is used by the RIPE NCC to identify RIPE NCC members to whom RPKI certificates can be issued.
CP	Certificate Policy. A CP is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements. The CP for the RPKI is [RFC 6484].
CPS	Certification Practice Statement. A CPS is a document that specifies the practices that a Certification Authority employs in issuing certificates.
Distribution of INRs	Internet number resources (INRs) are distributed hierarchically. IANA distributes blocks of IP addresses and Autonomous System Numbers (ASNs) to the five Regional Internet Registries (RIRs). The RIRs distribute smaller address blocks and Autonomous System Numbers to organisations 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 ASNs used for routing Internet traffic. IANA distributes INRs to RIRs.
INRs	Internet Number Resources. INRs are number values for three protocol parameter sets, namely: - IP version 4 addresses (IPv4) - IP version 6 addresses (IPv6) - Identifiers used in Internet inter-domain routing, currently Border Gateway Protocol-4 ASNs

ISP	Internet Service Provider. An ISP is an organisation managing and selling Internet services to other organisations.
NIR	National Internet Registry. NIRs manage the distribution of INRs for a portion of the geopolitical area covered by a Regional Internet Registry. NIRs form an optional second tier in the to INR distribution hierarchy.
RIR	Regional Internet Registry. An RIR is an organisation that manages the distribution of INRs for a geopolitical area.
RPKI-signed object	A digitally signed data object (other than a certificate or CRL) declared to be such an object by the Standards Track RFCs. An RPKI-signed object can be validated using certificates issued under this PKI. The content and format of these data constructs depend on the context in which validation of claims of current holdings of INRs take place. Examples of these objects are repository manifests [RFC 6486] and Route Origin Authorisations (ROAs) [RFC 6482].
CA	Certification Authority. A CA is an entity that issues digital certificates for use by other parties. A CA may issue CA certificates to subordinate CAs. Thus, a tree structure of CAs can be created, often called Public Key Infrastructure (PKI). The RIPE NCC operates three levels of CAs in the PKI hierarchy covered in this CPS.
Offline CA	The RIPE NCC Offline CA. This CA is kept offline when not in use for security reasons, and acts as the top level in the hierarchy. For the moment, this CA is making itself available as a Trust Anchor as described in [RFC 8630].
Hosted CA	A hosted CA that is technically hosted by the RIPE NCC as a RIPE NCC service in the LIR portal.
Delegated CA	Delegated CA is technically hosted by the company behind the CA. The issuing, revocation of its certificate follows the RPKI certificate provisioning protocol, see [RFC 6492].
All Resources CA (ACA)	An Online CA that contains all resources (e.g. 0/0) and is signed by the Trust Anchor. For more information, please see the NRO website.
Production CA	This CA is used on a daily basis to issue certificates to subordinate Hosted CAs. It contains, in contrast to the ACA, only resources in the RIPE NCC region.
Local Internet Registry (LIR)	An organisation, typically a network service provider, that distributes IP addresses and AS Numbers to End Users and/or uses them in their own infrastructure.
LIR Portal	The public portal the RIPE NCC provides for its members to access various RIPE NCC services, including the hosted CA service. The LIR Portal is also used to access the RIPE NCC Online CA by specific users, as described later in this CPS.
RIPE NCC Member	A natural or a legal person that has entered into the RIPE NCC Standard Service Agreement (SSA) with the RIPE NCC.
End User	A natural or a legal person who is assigned provider independent (PI) resources from the RIPE NCC through a sponsoring agreement with a RIPE NCC member.

RP	Relying Party as defined in section 1.3.4. above.
TA	Trust Anchor. The top CA certificate in the chain used for validation. Relying Parties choose which CA certificate they trust as being the top of the validation tree. Relying Parties may choose to trust more than one TA.

RPKI Objects and Certificates

Certificate	An X.509 PKIX Resource Certificate as described in [RFC 7318]. There are two types of certificates: - Certification Authority (CA): Certificates are used by Certification Authorities to issue subordinate certificates and EE certificates. - End Entity (EE): Certificates are embedded in RPKI-signed objects such as Manifests and ROAs and are used to sign these objects (see [RFC 6488]). Note the CAs described in this CPS do not currently issue any multi-use End Entity Certificates as described in [RFC 7318].
ROA	ROA is a digitally signed object that provides a means of verifying that an IP address block holder has authorised an Autonomous System (AS) to originate routes to one or more prefixes within the address block. See [RFC 6482].
CRL	Certificate Revocation List is a time-stamped list identifying revoked certificates that are signed by a CA or CRL issuer and made freely available in a public repository. See [RFC 7318].
Manifest	A signed object under the RPKI listing all subordinate signed objects and certificates for a CA certificate. See [RFC 6486].


Offline TA
Secure physical transfer of signing request and response
Online
ACA
Production CA
Delegated CA
Hosted CA
rsync/RRDP repositories
Offline TA, ACA, Production CA:
- Certificate
- Manifest
- CRL
Hosted CA:
- Certificate
- Manifest
- CRL
- ROAs
Delegated CA:
- Certificate
Exchange via up-down protocol
Delegated CA:
- Manifest
- CRL
- ROAs
Delegated repository not managed by RIPE NCC

2. Publication and Repository Responsibilities

2.1. Repositories

As per the CP [RFC 6484], certificates, CRLs and RPKI-signed objects MUST be made available for downloading by all relying parties, to enable them to validate this data. The RIPE NCC will publish this via a repository that is accessible via rsync and RRDP. This repository conforms to the structure described in [RFC 6481].

2.2. Publication of Certification Information

The RIPE NCC publishes the certificates, CRLs and RPKI-signed objects that are issued to a repository that operates as part of a world-wide distributed system of RPKI repositories.

Offline CA
The CA certificate for the RIPE NCC Offline CA is intended to be used as a Trust Anchor by relying parties. The Trust Anchor Locator, as per [RFC 6490], follows:

```
https://rpki.ripe.net/ta/ripe-ncc-ta.cer
rsync://rpki.ripe.net/ta/ripe-ncc-ta.cer

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0URYSGqUz2myBsOzeW1j
Q6NsxNvlLMyhWknvnl8NiBCs/T/S2XuNKQNZ+wBZxIgPPV2pFBFeQAvoH/WK83Hw
A26V2siwm/MY2nKZ+Olw+wlpzlZ1p3Ipj2eNcKrmit8BwBC8xImzuCGaV0jkRB0G
Z0hoH6Ml03umLprRsn6v0xOP0+l6Qc1ZHMFVFb385IQ7FQQTcVIxrdeMsoyJq9eM
kE6DoclHhF/NlSllXubASQ9KUWqJ0+Ot3QCXr4LXECMfkpkVR2TZT+v5v658bHVs
6ZxRD1b6Uk1uQKAyHUbn/tXvP8lrjAibGzVsXDT2L0x4Edx+QdixPgOji3gBMyL2
VwIDAQAB
```

Online CA
The Online CA publishes subordinate certificates, CRLs and RPKI-signed objects under:
rsync://rpki.ripe.net/repository/33/36711f-25e1-4b5c-9748-e6c58bef82a5/1/

Hosted CAs
The hosted CAs publish subordinate signed objects in the repository that is hosted by the RIPE NCC:
rsync://rpki.ripe.net/repository

The exact URI of the publication point is unique per hosted CA. This can be found in the hosted CA certificate as described in [RFC 7318].

Note the repository structure is defined in [RFC 6481].

2.3. Time or Frequency of Publication

A certificate will be published within eight hours of being issued (or deleted).

The RIPE NCC will publish its CRL prior to the next “Update value” in the scheduled CRL previously issued by the CA.

2.4. Access Controls on Repositories

Write access to the repositories is limited to the systems running the ACA, Production CA, and hosted CAs.

3. Identification and Authentication

3.1. Naming

3.1.1. Types of names

The Subject of each certificate issued by the RIPE NCC 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 the RIPE NCC. Optionally, the Serial Number attribute may be indicated along with the common name (to form a terminal relative distinguished name set), to distinguish between successive instances of certificates associated with the same entity.

For the Offline CA, the self-signed CA certificate is published as a Trust Anchor, as described in Section 2.2. The subject is “CN=ripe-ncc-ta”.

For all other certificates controlled by the ACA, Production CA, and hosted CAs, the subject has the format CN=<pub key hash>, where the public key hash is a Base64 encoded form of the public key SHA-1 hash, as described in section 2.1 of [RFC 4387].

3.1.2. Need for names to be meaningful

The Subject name in each subscriber certificate will be unique to the public key found in the certificates.

The Subject name should not be "meaningful" in a conventional, human-readable sense. The rationale is that these certificates are used for authorisation in support of applications that make use of attestations of INR holdings. They are not used to identify subjects.

3.1.3. Anonymity or pseudonymity of subscribers

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

3.1.4. Rules for interpreting various name forms

None.

3.1.5. Uniqueness of names

The RIPE NCC certifies Subject names that are unique among the certificates that it issues. Although it is desirable that Subject names be unique throughout the PKI (to facilitate certificate path discovery), uniqueness is not required and is not enforced through technical means. The RIPE NCC generates Subject names to minimise the chance that two entities in the RPKI will be assigned the same name. Specifically, the generated subject based on the public key hash (described in Section 3.1.1.) keeps the likelihood of accidental collisions to a negligible minimum.

3.1.6. Recognition, authentication, and role of trademarks

Since the subject names are not intended to be meaningful, the RIPE NCC makes no provision either to recognise or to authenticate trademarks, service marks, etc.

3.2. Initial Identity Validation

3.2.1. Method to prove possession of private key

For the Offline CA, proof of possession of the private keys used for the self-signed certificate can be determined internally.

For the ACA, which acts as a subscriber to the Offline CA, and for the Production CA, which acts as a subscriber to the ACA, possession of the private keys is affected via the procedures used to generate and manage these keys. Specifically, the RIPE NCC uses a hardware security module (HSM) to generate the key pairs for each of these CAs. This assures that the private key is appropriately associated with the public key in the certificates issued by each of these CAs.

For the hosted CAs that act as subscribers to the Production CA, possession of the private keys is affected by the system. Note that the hosted CAs are managed systems and operators do not access the keys directly. These CAs will contact the Production CA as needed, via protocols internal to the RIPE NCC. These protocols also cover proof of possession of the private keys.

The Delegated CA, which acts as a subscriber to the Production CA, holds its own key pair. The issuing or renewal of Certificates is performed via the provisioning protocol. See [RFC 6492].

3.2.2. Authentication of organisation identity

Certificates issued under this PKI do not attest to the organisational identity of subscribers. However, certificates are issued to subscribers in a fashion that preserves the accuracy of INR registrations as represented in the RIPE NCC's records.

The RIPE NCC has already established procedures to verify the identity of Certificate Holders. See section 3.2.3. below.

For hosted CAs, the RIPE NCC is able to map a logged-in user to a specific organisation, and the organisation can be mapped to a specific public key. Thus, the RIPE NCC is able to map these public keys to a specific set of resources as represented in the RIPE NCC records.

3.2.3. Authentication of individual identity

Certificates issued under this PKI do not attest to the individual identity of a subscriber. However, the RIPE NCC maintains contact information for each subscriber to support certificate renewal, re-key, and revocation.

Offline CA
Individuals who are authorised to operate the Offline CA are authenticated by possession of the necessary HSM keycards and via physical and procedural security access controls.

Hosted CAs
For hosted CAs, individual identity is delegated to "Admin" and "Regular" users in the RIPE NCC's LIR Portal. New users can be added by the current admin user and granted either "Admin" or "Regular" status. This user can then also maintain their CA.

For hosted End User CAs, individual identity is delegated to the LIR Portal account associated with the **organisation** object referenced in the PI assignment. For more information, please refer to the documentation on RPKI for End Users.

Production CA and ACA
For the Production CA and the ACA, the mechanism for hosted CA users is used. However, it should be noted that these users require an additional role that cannot be set through the public user management interface. Maintenance can also be performed through the internal admin interface.

3.2.4. Non-verified subscriber information

No non-verified subscriber data is included in certificates issued under this certificate policy, except for Subject Information Access (SIA) extensions [RFC 6487].

3.2.5. Validation of authority

The procedure to verify that an individual claiming to represent the subscriber is authorised to represent the subscriber for different CAs is as follows:

- Access to the Offline CA is restricted to a RIPE NCC engineer with access to the UNIX account on the server. In addition, the HSM key cards are protected by pass phrases known only to individual CA Operators (see Section 5.2.3. for a description of the CA Operator role).
- Access to the Production CA and ACA is restricted to RIPE NCC CA Operators using internal admin interface.
- For access to the hosted CA, see Section 3.2.3. above.

3.2.6. Criteria for interoperation

The RPKI is not intended or 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

The procedure to ensure that a subscriber requesting routine re-key is the legitimate holder of the Certificate is as follows:

- For the Offline CA and ACA, the same identification and authentication mechanisms apply as described in Section 3.2.3.
- For hosted CAs, routine re-keys are automated by the software and no explicit authentication is required. A routine re-key is initiated whenever the current key for a hosted CA is older than five years. The key rollover algorithm is described in [RFC 6489].
- Non-hosted CAs will have to handle re-keys on their own, as the private key is unknown to the RIPE NCC.

3.3.2. Identification and authentication for re-key after revocation

The old key can be revoked as the final step in key rollover algorithm [RFC 6489], once a new key has been activated.

In the RIPE NCC's implementation, old keys are not automatically revoked after a routine re-key. Explicit revocation of old keys can be done by CA Operators of the Offline CA and the Online CA. CA Operators for the Online CA can also revoke old keys for hosted CAs. Identification and authentication for these roles is described in Section 3.2.3.

This may change after further discussion of the key rollover standard, which is currently unclear about whether the old key should be revoked immediately. The current belief is that there is no reason for old keys not to be automatically revoked after a successful re-key. This may therefore be updated in the near future.

3.4. Identification and Authentication for Revocation Request

For hosted CAs, the holder of the INRs can contact the RIPE NCC Registry Services Department to request the certificate revocation. It should be also noted that user actions in the interface may result in revocation of EE certificates used for objects (such as ROAs) that should be invalidated.

For non-hosted CAs, the holder can request the revocation in the user interface.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who is able to submit a certificate application

Any RIPE NCC member or End User holding INRs distributed by the RIPE NCC may submit a certificate application to this CA.

4.1.2. Enrolment process and responsibilities

For the Offline CA, an Engineer can configure and initialise the CA on a server controlled by the RIPE NCC (see Section 5.2.1. for a description of the Engineer role).

For the ACA and the Production CA, an Engineer can install and initialise the application. When this has been done, a CA Operator can log in and initialise the ACA and the Production CA.

For hosted CAs, any RIPE NCC member or End User may choose to use a RIPE NCC-hosted Certification Authority or may choose to set up their own non-hosted CA.

In order to activate the hosted CA, an "Admin" or “Regular” user must log in to the LIR Portal. This user must then ensure that a client certificate has been generated for them (or generate one if this is missing).

The user will then be able to click on a link labelled "RPKI Dashboard". This will take the user to a page where they must explicitly opt in to the hosted CA service. The user does this by clicking "Yes, I want to activate my hosted CA". After activation, an automated hosted CA will be created. Authentication and authorisation for further automated processes should be considered transitive from the moment that user opts-in and activates the hosted CA, as described here.

4.2. Certificate Application Processing

For hosted CAs, an initial CA certificate should be requested by an authorised representative through the RPKI Dashboard in the LIR Portal.

The requester will be asked to choose the type of the CA as described in Section 4.1.2. and agree to the RIPE NCC Certification Service Terms and Conditions.

In the case of a hosted CA, the system will automatically create the certificate in the LIR Portal. The subscriber will need to accept the RIPE NCC Certification Service Terms and Conditions by clicking “I accept. Create my Certification Authority”. This way, the subscriber confirms that they have read, understood, and agree to be bound by these terms and conditions.

For non-hosted CA, the requester will need to upload the identity .xml file generated by their CA software.

4.2.1. Performing identification and authentication functions

See Section 3.2.3. for identification and authentication practice of certificate applicants.

4.2.2. Approval or rejection of certificate applications

The online CA will issue certificates to hosted CAs that are valid until to the end of the calendar year, plus a further six-month grace period to allow for renewal before the certificate expires.

All Provider Aggregatable (PA) resources registered to a RIPE NCC member at the time of issuance will be included in the certificate. All Provider Independent (PI) resources registered to the End User at the time of issuance will be included in the certificate.

Certificates cannot be issued when:

- The RIPE NCC member does not hold any Internet number resources
- Service level for a RIPE NCC member has been suspended (e.g. due to non-payment).

4.2.3. Time to process certificate applications

Certificates are generated automatically upon request by a RIPE NCC member or End User and processed immediately.

In case the automated process is not functional, a RIPE NCC member or End User can request a certificate manually, via a request form on the RIPE NCC website. These requests will be processed within one business day.

4.3. Certificate Issuance

4.3.1. CA actions during certificate issuance

The Offline CA will produce a response message that includes all publishable certificates and other objects after the certificate has been issued. This message can be physically transferred to the Production CA and the ACA, where it is published.

The Production CA and the ACA, as well as hosted CAs, make all subordinate certificates and objects available for publication. While the system will make a best effort to publish these materials as soon as possible, publication should happen no later than eight hours after issuance (as described in Section 2.3.)

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

For RIPE NCC member and End User CAs, there is no active notification to a subscriber about certificate issuance. The approved and published certificate is visible in the RPKI Dashboard in the LIR Portal and in the RIPE NCC-hosted repository.

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

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

4.4. Certificate Acceptance

4.4.1. Conduct constituting certificate acceptance

When a certificate is issued, the RIPE NCC CA will publish it in the repository.

After the Certificate is issued, the subscriber can see the updated number of issued certificates under “Certified Resources” in the RPKI Dashboard in the LIR Portal.

Certificate acceptance by the subscriber is not part of the process.

4.4.2. Publication of the certificate by the CA

Certificates will be published in the repository system within eight hours of being issued by any of the CAs covered by this CPS.

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

There are no entities other than the subscriber who are 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

The hosted CAs receive CA certificates from the Online CA. This means that these certificates could in principal be used to issue subordinate CA certificates. However, the hosted system does not provide this functionality. The hosted CA certificates will only be used (by the system) to issue EE certificates used for RPKI-signed objects (such as ROAs) and manifests. The private key associated with each of these certificates is used to sign subordinate (CA or EE) certificates and CRLs.

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:

- Verify that the certificate will be used for an appropriate purpose that is not prohibited or otherwise restricted by this CPS (see section 1.4.)
- Assess the status of the certificate and all CAs in the chain that issued certificates relevant to the certificate in question (terminating at the RIPE NCC Trust Anchor accepted by the Relying Party). If any of the certificates in this chain have been revoked or have expired, the relying party is solely responsible for determining 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, as defined by the RIPE NCC Certification Repository Terms and Conditions.

If a relying party determines that use of the certificate is appropriate, the relying party must utilise 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 [RFC 6487], which specifies the extended validation algorithm for RPKI certificates.

4.6. Certificate Renewal

Note that the hosted CAs do not issue CA certificates to subordinate CAs and there is no need for certificate renewal for EE certificates used for signed objects. However, hosted CAs are mentioned a few times in this section as children of the Production CA and the ACA.

4.6.1. Circumstances for certificate renewal

A certificate will be renewed for hosted CAs when new INRs are associated with a RIPE NCC member or End User, or a new validity period is applied (see Section 4.2.2).

Note that if INRs are no longer associated with a RIPE NCC member or End user, the Production CA and the ACA will re-issue a new certificate – minus those Internet number resources – and revoke overclaiming certificates, as described in Section 4.9.

4.6.2. Who may request renewal

For hosted CAs, the renewal process is fully automated, which means that the subscriber cannot initiate renewal.

For the Production CA and the ACA, a RIPE NCC Engineer can request renewal from the Offline CA.

For the Offline CA, Internet number resources may have to be added to the self-signed certificate. A RIPE NCC Engineer may perform this action.

4.6.3. Processing certificate renewal requests

See 4.6.1.

For hosted CAs, the system will automatically request renewal of the CA certificate that lists all eligible INRs when new resources are received by a RIPE NCC member or End User, or a new validity period is applicable.

4.6.4. Notification of new certificate issuance to subscriber

See Section 4.3.2. (Notification to Subscriber by the CA of Issuance of Certificate).

4.6.5. Conduct constituting acceptance of a renewal certificate

See Section 4.4.1. (Conduct Constituting Certificate Acceptance).

4.6.6. Publication of the renewal certificate by the CA

The Offline CA, Production CA, and the ACA, will all publish renewed subordinate CA certificates within eight hours of issuance.

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

See Section 4.3.2. (Notification to Subscriber by the CA of Issuance of Certificate).

4.7. Certificate Re-Key

Hosted CAs do not issue CA certificates to subordinate CAs and there is no need for certificate re-key for EE certificates used for signed objects. However, hosted CAs are mentioned a few times in this section as children of the Online CA.

4.7.1. Circumstance for certificate re-key

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

- Confirmed/suspected compromise or loss of the associated private key
- Expiration of the cryptographic lifetime of the associated key pair

If a certificate is revoked to replace the resource extensions (see RFC 3779), the replacement certificate will incorporate the same public key (not a new key). If the re-key is based on a suspected compromise, then the previous certificate will be revoked.

Section 5.6 of [RFC 6484] notes that when a CA signs a certificate, the signing key should have a validity period which exceeds that of the certificate. This places additional constraints on when a CA should request a re-key.

4.7.2. Who may request certification of a new public key

For the RIPE NCC Hosted CA, Production CA, and the ACA, there is no scheduled manual key rollover. This can be initiated by a RIPE NCC Engineer in the event of an outage.

The RIPE NCC may also initiate a re-key based on a verified compromise report.

4.7.3. Processing certificate re-keying requests

The procedure in Section 4.2.2 applies here.

4.7.4. Notification of new certificate issuance to subscriber

See section 4.3.2.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

See section 4.4.1.

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

For all CAs covered by this CPS, a re-keyed certificate will be published in the repository system within eight hours of being issued by this CA.

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

See section 4.3.3.

4.8. Certificate Modification

4.8.1. Circumstance for certificate modification

Certificate modification is not applicable to the CAs described here. Renewal is used when new resources are being certified, or a new validity period is applicable (Section 4.6). Re-issuance and revocation is used when resources are no longer held by an entity (Section 4.9.).

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for revocation

Certificates must be revoked for several reasons:

- One or more listed INRs are no longer associated with the RIPE NCC member or End User
- As a last step when doing a planned re-key (clean up)
  As a last step when doing an unplanned re-key because a loss or compromise of the old key has come to light
- The RIPE NCC member violates the RIPE NCC Certification Service Terms and Conditions

A certificate may be revoked if a signed object needs to be invalidated.

4.9.2. Who can request revocation

For Hosted and Delegated CAs, revocation of their CA certificate can be performed automatically via the RPKI Dashboard in the LIR Portal, or when RIPE NCC staff have reason to believe the keys have been compromised. In this latter case, this would always be performed as the final step of an emergency key rollover for the hosted CA.

For Delegated CAs, the revocation request can be done via the RPKI Dashboard in the LIR Portal.

The other circumstances for revocation, most notably when ROA objects need to be invalidated because a user of the hosted CA changes the specification, are managed automatically by the system.

For the Production CA and the ACA, the RIPE NCC may manually request revocation of the old CA certificate as soon as a key rollover has been performed. Related events, most notably the revocation of the EE certificates used for manifests, are managed by the system.

4.9.3. Procedure for revocation request

When one or more of the INRs listed in a certificate are no longer associated with a RIPE NCC member or End User, the Online CA will:

- Re-issue a new certificate that retains all other properties (minus the affected INRs)
- Publish the new certificate using the same publication point as before, thus replacing the old certificate
- Revoke any non-expired certificates held by the hosted CA that list the affected INRs, thus invalidating any signed objects (such as ROAs) that refer to these resources

For Delegated CAs, a new certificate not be issued automatically once the revocation request has been completed. This will have to be requested again via the LIR Portal.

4.9.4. Revocation request grace period

Any party or operators who can identify a need for revocation that is not already handled by the system are expected to notify the RIPE NCC as soon as possible.

4.9.5. Time within which CA must process the revocation request

The RIPE NCC will process a revocation request within eight hours of receipt and validation of the request.

4.9.6. Revocation checking requirement for relying parties

As per [RFC 6484], whenever a relying party validates a certificate, it is responsible for acquiring and checking the most recent, scheduled CRL from the issuer of the certificate

4.9.7. CRL issuance frequency

Each CRL contains a “Next Update” value, and a new CRL will be published at or before that time. The RIPE NCC will set the “Next Update” value when it issues a CRL to signal when the next scheduled CRL will be issued.

The CAs covered by this CPS use different values:

Offline CA:	3 months from the moment of issuance
CA:	24 hours from the moment of issuance
Hosted CAs:	24 hours from the moment of issuance
ACA	24 hours from the moment of issuance

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

It should be noted that the values listed here may be used by relying parties to determine the need to fetch an updated CRL.

4.9.8. Maximum latency for CRLs

A CRL will be published to the repository system within one hour of their generation.

4.10. Certificate Status Services

The RIPE NCC will only issue CRLs and does not support Online Certificate Status Protocol (OCSP) or the Server-Based Certificate Validation Protocol (SCVP).

5. Facility, Management and Operational Controls

5.1. Physical Controls

5.1.1. Site location and construction

For the Offline CA, operations are conducted within the physically-protected area of a data centre where the RIPE NCC is a tenant. This is located at:

Equinix AM3
Science Park 610
1098 XH Amsterdam
The Netherlands

For the Production CA and hosted CAs, core cryptographic operations are performed by virtual machines and their respective HSMs physically located in two different data centres in a load balanced (and fail-over) set up. The two data centres are:

Equinix AM3
Science Park 610
1098 XH Amsterdam
The Netherlands

Equinix AM5
Schepenbergweg 42
1105 AT Amsterdam
The Netherlands

5.1.2. Physical access

For both Equinix AM3 and AM5, IT staff may request access for themselves. IT management may request access for others. The server is physically located in one of four racks that are rented by the RIPE NCC. These racks are housed in a special suite that is dedicated to the RIPE NCC only.

5.1.3. Power and air conditioning

The server rooms are located on the first floor of the building, which is above sea level. Power to the data centres comes from the public grid, supported by internal back-up generator infrastructure. More information on the ISO standards applicable to Equinix AM3 and Equinix AM5 data centres is available.

5.1.4. Water exposures

The server rooms located at Equinix AM3 and Equinix AM5 are both located on the first floor of their building or higher, which is above sea level.

5.1.5. Fire prevention and protection

The server room at Equinix AM3 has two-stage fire detection system: Aspiration and VESDA, on a head-per-head basis. The server room at Equinix AM5 has VESDA and HI-FOG as water mist fire suppression and double knock fire activation.

5.1.6. Media storage

Whenever the Offline CA is operated, all data is backed up to a USB stick (and encrypted where needed). For the Online CA and hosted Cas, all data is stored (encrypted where needed) on a network filesystem that is mirrored between the Equinix AM3 and Equinix AM5 datacentres. In addition, this data is backed-up off-site nightly and across both data centres (see Section 5.1.8.).

5.1.7. Waste disposal

Key cards that are found to be broken will be destroyed. If a key card is lost, a new card set will be generated and all HSM keys will be migrated to this new set, to render the lost card useless.

Once the HSM is decommissioned, the device is destroyed by a designated third party.

There is no other waste that may contain sensitive data.

5.1.8. Off-site backup

The network filesystem, used to store the data from the CAs, is backed up every night to another fileserver. This second fileserver is also backed up every night to another backup server.

5.2. Procedural Controls

Below are the procedural security controls used for certificate management.

5.2.1. Trusted roles

For the Offline CA:

System Operator	Has access to the server. Ensures system is set up correctly. Can perform restore using quorum of Administrative Card Set used to protect the keys. See Section 6 for more details on card set controls used for the HSM. Has access to one out of ten key cards from the Operator Card Set (OCS) needed to operate the Offline CA. Three out of ten key operators must be present to provide a quorum for operations involving the offline CA.
CA Operator	There are ten CA Operators. Five of these also have access to one of five cards from the Administrative Card Set (ACS) that initialised the HSM. Three of these cards are needed for a restore operation (see Section 6.).

Engineer	Has access to the source code used to run the Offline CA. Is responsible for developing, testing and deploying new releases. The Engineer also has de-facto technical knowledge of the set-up and will therefore facilitate specific Offline CA operations, including: - Transferring outstanding request (certificate and/or revocation) from the Online CA to the Offline CA - Providing technical knowledge for operating the Offline CA - Transferring the response to the Online CA and making sure the response is properly processed

For the Online CA and ACA:

System Operator	Same as for Offline CA.
Engineer	Has access to the source code used to run the Online CA. Is responsible for developing, testing and deploying new releases. In addition, the Engineer can configure values used by the software, such as publication frequency.
CA Operator	Has access to the user interface. Can perform key re-key operations, revoke old keys, and has access to the system status page that allows switching on/off of the background services for the Online CA.
Security Officers	The Security Officers receive one of five cards making up the ACS for the HSMs used for the Online CA and hosted CAs. Three of these five cards are needed to perform a restore. There are five ACS Card Holders.

For the hosted CAs:

System Operator	Same as for Offline CA.
Engineer	Same as for Online CA.
CA Operator	Has access to the user interface. This system automates all cryptographic operations, such as creating and revoking EE certificates, publication, etc. The CA Operator can perform the following actions only: - Activate the hosted CA - Create/update/delete ROA configurations (the objects themselves are managed by the system)
RIPE NCC Operator	This role is available to all CA Operators for the Online CA. It allows access to all actions that a member CA Operator could perform. In addition, it allows re-key

	operations and revocation of old keys. The role also has access to the system status page that allows switching on/off of the background services for hosted CAs.

For the Delegated CA:

System Operator	Follows the procedure as defined internally by the RIPE NCC member or End User.
CA Operator	Follows the procedure as defined internally by the RIPE NCC member or End User.

5.2.2. Number of persons required per task

For all roles and CAs listed in the above section, only one person is required per task, except for CA operations for the Offline CA (here, three out of ten persons are required).

5.2.3. Identification and authentication for each role

For the Offline CA:

System Operator	Access to the server running the Offline CA is limited to RIPE NCC IT staff. Since the system does not accept any incoming network traffic, this requires the IT staff to have access to the server room to log in (see Section 5.1.2.).
CA Operator	Has no account on the server but will be asked by the Engineer to present their key card and enter their pass phrase for authentication and authorisation of the operation.
Engineer	Engineers can login to the UNIX account that is used to run the Offline CA software.

For the Production CA and ACA:

System Operator	Access to the server running the Production CA and the ACA is limited to RIPE NCC IT staff. For some operations, IT staff need access to the server room to log in (see Section 5.1.2.).
Engineer	Engineers have access to the UNIX account that is used to run the software.
CA Operator	The CA operator uses the RIPE NCC admin interface to log in. The login process requires that a username, password, and SSL certificate are presented and valid.

For the hosted CAs:

System Operator	Access to the server running the Production CA and the ACA is limited to RIPE NCC IT staff. For some operations, IT staff needs access to the server room (see section 5. 1. 2) to log in.
Engineer	The Engineers have access to the UNIX account that is used to run the software.
CA Operator	The CA operator uses the RIPE NCC single sign-on system to log in to the user interface. The login process requires a username and a password. The CA Operator must also have either an “Admin” or “Regular” role in the LIR Portal. In case of End Users, the log in credentials for the LIR Portal must be associated with the maintainer of the respective organisation in the RIPE Database.

For the Delegated CA:

System Operator	Follows the procedure as defined internally by the RIPE NCC Member or End User.
CA Operator	Follows the procedure as defined internally by the RIPE NCC Member or End User.

5.2.4. Roles requiring separation of duties

The CA Operator role for the Offline CA is performed by RIPE NCC staff from various departments. The people fulfilling these roles have no other roles in the CAs operated by the RIPE NCC.

5.3. Personnel Controls

Below are the personnel security controls employed for individuals associated with certificate management.

5.3.1. Qualifications, experience and clearance requirements

Staff members are assigned to the roles mentioned in section 5. 2. 1 only if supervisory personnel deem them to be sufficiently trustworthy and only after they have undergone in-house training for the role.

5.3.2. Background check procedures

All RIPE NCC staff undergo normal employment reference checks.

5.3.3. Training requirements

The RIPE NCC provides its staff with training upon assignment to a System Operator, CA operator or an Engineer role. It also arranges on-the-job training as needed to perform their job responsibilities competently.

5.3.4. Retraining frequency and requirements

The RIPE NCC provides its staff with re-training as needed to continue performing their job responsibilities competently.

5.3.5. Job rotation frequency and sequence

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

5.3.6. Sanctions for unauthorised actions

It has been established that if a RIPE NCC staff member performs activities inconsistent with the organisation's RPKI policies and procedures, appropriate disciplinary action will be taken.

5.3.7. Independent contractor requirements

Independent contractors and consultants may be part of the development team but cannot constitute more than 50% of the total team.

Contractors who are required to perform any maintenance functions on CA severs or cryptographic modules must be accompanied and directly supervised by RIPE NCC staff at all times when in sensitive areas.

5.3.8. Documentation supplied to personnel

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

5.4. Audit Logging Procedures

Below is the description of how RIPE NCC implements audit logging.

5.4.1. Types of events recorded

For the Offline CA, no audit logging is implemented.

Audit records are generated for operations performed by the CA Operators for the Production CA, ACA and hosted CAs. These records include the date, time, responsible user and summary content data relating to the event. Records are stored in a database and are visible through the user interface.

The physical access control system maintains separate logs for access to the areas housing sensitive CA equipment.

Auditable events include, but are not limited to, the following:

- Access to CA computing equipment (e.g. log-in, log-out)
- 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

5.4.2. Frequency of processing log

Logs will be reviewed during general audits or after a suspected incident.

5.4.3. Retention period for audit log

Audit records for the Production CA and the ACA, as well as hosted CAs, are included in the nightly database back-up and retained off-site for a minimum of two years.

5.4.4. Protection of audit log

At the moment, no additional measures are taken to protect the audit logs, as compared to normal back-up procedures.

5.4.5. Audit log backup procedures

See Section 5.4.3.

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

5.4.7. Notification to event-causing subject [OMITTED]

5.4.8. Vulnerability assessments

The RIPE NCC uses a third party to perform periodic vulnerability assessments of computer and network systems and of software that is developed in house to operate the CAs covered by this CPS. These reports are provided to the RIPE NCC Security Officer and the RIPE NCC Managing Director.

5.5. Records Archival [OMITTED]

5.6. Key Changeover

The Offline CA acts as a Trust Anchor. If necessary, the RIPE NCC can issue a new key pair for the Trust Anchor and issue a new Trust Anchor Locator (TAL) and make this publicly available. For the Production CA, the ACA, and the hosted CA, key pair changes are not performed on a scheduled basis. If a key-roll is required, a procedure as described in [RFC6489] will be followed.

Initiating the re-key is a manual action initiated by a Production CA and the ACA Operator via the user interface.

5.7. Compromise and Disaster Recovery

In the event of a key-pair compromise, a key-rollover can be performed on demand for Production CA, ACA and Hosted CA.

As part of disaster recovery, backups are used.

For the Trust Anchor, in case of key-pair compromise a key-rollover will be performed and a new Trust Anchor Locator (TAL) will be published.

5.8. CA or RA Termination

The RIPE NCC has been granted sole authority by the Internet Assigned Numbers Authority (IANA) to manage the allocation of IP address space and AS Numbers in its service region, which includes Europe, the Middle East and parts of Central Asia. The RIPE NCC has established the RPKI for its region consistent with this authority. There are no provisions for termination and transition of the CA function to another entity.

6. Technical Security Controls

This section describes the security controls used by the RIPE NCC.

6.1. Key Pair Generation and Installation

6.1.1. Key pair generation

For the RIPE NCC RPKI and hosted CAs operated by the RIPE NCC, key pairs are generated using a hardware cryptographic module. The module used for this purpose is certified as complying with FIPS 140-2 level 3. The module employed for this process is nShield Connect 6000.

6.1.2. Private key delivery to subscriber

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

6.1.3. Public key delivery to certificate issuer

For the Offline CA, transfer of certificate sign requests and/or revocation requests that include the ACA public key hash are done using XML files on a USB stick, because the Offline CA server is not connected to a network.

The hosted CA, the ACA, and the production CA are all managed by the same software. Therefore, the ACA has direct access to the production CA public keys.

The Production CA, in turn, has direct access to the hosted CA public keys. For this reason, no key delivery is involved.

6.1.4. CA public key delivery to relying parties

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

The Offline CA is intended to be used as a Trust Anchor by relying parties. The Trust Anchor Locator [RFC 6490] is described in Section 2.2.

The RIPE NCC will publish this Trust Anchor Locator at:
https://www.ripe.net/manage-ips-and-asns/resource-management/certification/ripe-ncc-rpki-trust-anchor-structure

It may also publish this via other mechanisms, such as printed material, RIPE Meeting presentations or training courses.

6.1.5. Key sizes

The key sizes used in this PKI are as specified in [RFC 7935].

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 7935].
The nCipher HSMs used by the CAs covered by this CPS were certified as complying with FIPS 140-2 level 3. Though the details of the key generation implementation used by these modules are not known by the RIPE NCC, the RIPE NCC trusts that this certification implies that key generation and quality checking by the modules is sufficiently safe.

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

The key usage extension bit values employed in RPKI certificates are specified in [RFC 6487].

The key usage extension bit values are consistent with [RFC 6818]. For the RIPE NCC RPKI CA certificates, the keyCertSign and cRLSign bits are set TRUE. All other bits (including digitalSignature) are set FALSE, and the extension is marked critical.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards and controls

The Offline CA is operated under FIPS 140-2 level 3, requiring three out of ten operator keys to be presented for key pair generation and signing operations.

The ACA, the production CA, and hosted CAs employ a cryptographic module evaluated under FIPS 140-2 level 3 [FIPS]. However, because these systems need to be running 24/7 and need to be able to perform key generation and signing operations without human intervention, they are operated under FIPS 140-2 level 2 to allow unattended operation.

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

As described in Section 6.2.1, three out of ten CA Operators are required to operate the Offline CA. For the ACA, Production CA and hosted CA, no multi-person control is used during normal operation.

6.2.3. Private key escrow

No private key escrow procedures are required for this PKI.

6.2.4. Private key backup

For all CAs covered by this CPS, the private keys are stored in the database that feeds the HSM using Advanced Encryption Standard (AES) encryption with a key that is protected by a three-out-of-five Administrative Card Set.

For the Offline CA, the encrypted private key is stored in the local file system by the HSM, using Advanced Encryption Standard (AES).

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 encrypted private keys and other information described in Section 6.2.4. may be restored to another HSM. In order to do this, a system administrator must have access to a quorum of the Administrative Card Set (ACS); in this case three-out-of-five cards are needed.

Also note that this mechanism allows multiple HSMs to share the same internal key and encrypted managed keys stored on a network file system. This allows for the load balancing and fail-over set-up that is used for the ACA, the production CA, and hosted CAs.

6.2.7. Private key storage on cryptographic module

The private keys for all CAs covered by this CPS may be temporarily stored in the cryptographic module and will be protected from unauthorised use in accordance with the [FIPS 140-2] requirements applicable to the module.

Long term storage is done by storing the keys on a disk in an encrypted form, as described above.

6.2.8. Method of activating private key

For the Offline CA, activating the keys requires that three-out-of-five Operator cards are presented by individual senior staff, as described in Section 6.2.1.

For the ACA, Production CA, and hosted CAs, the private keys can be used by all processes with access to the nShield Connect 6000.

6.2.9. Method of deactivating private key

The Offline CA keys are de-activated as soon as processing is finished. Subsequent operation will require re-activation as described above. In addition, the server is physically turned off when not in use. As soon as processing is done, the server is backed up and shut down again.

The cryptographic modules for the RIPE NCC ACA, Production CA, and hosted CAs will operate in an unattended mode, on a 24/7 basis.

6.2.10. Method of destroying private key

Keys are not stored long-term inside the hardware security modules used by the CAs covered by this CPS. The HSMs store the keys in encrypted form. Keys are deleted when they are no longer in use. Since they were encrypted in the first place, no additional action is taken to zero the bytes or purge them from long term back-up.

6.2.11. Cryptographic module rating

The cryptographic module(s) used by all CAs covered by this CPS are certified under FIPS 140-2, at level 3 [FIPS].

For the ACA, the production CA, and hosted CAs, these modules are operated at FIPS-140-2 level 2, to allow for automatic processing.

6.3. Other Aspects of Key Pair Management

6.3.1. Public key archival

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

6.3.2. Certificate operational periods and key pair usage periods

For the Offline CA that is intended to be used as a Trust Anchor by relying parties, the RIPE NCC is committed to support the same key pair for at least five years. This may change if a new RFC is implemented that affects this process, or if the keys are compromised, which makes the CA unable to support the same key pair.

For the ACA, production CA, and hosted CAs, there is no intended validity period.

6.4. Activation Data

6.4.1. Activation data generation and installation

For the Offline CAs, the three-out-of-five Administrative Card Set (ACS) and the three-out-of-ten Operator Card Set (OCS) were generated following the procedures described in the HSM manual. The cards were distributed among five-of-the-ten Offline CA Operators described in Section 5.1.2.

For the ACA, production CA, and the hosted CAs, the three-out-of-five Administrative Card Set was generated following the procedures described in the HSM manual. The cards were distributed between the five Offline CA Operators described in Section 5.1.2.

6.4.2. Activation data protection

See section 6.2.8.

6.4.3. Other aspects of activation data

None.

6.5. Computer Security Controls

The Offline CA is kept offline when not in use. It is only switched on when in use and is never connected to any network. All data (requests, responses, backups) are transferred using empty USB sticks.

The ACA, Production CA, and hosted CAs are operated on machines in the RIPE NCC internal service VLAN. The user interface is made available through a firewall that load balances requests to two different back-end proxy servers.

6.6. Life Cycle Technical Controls

6.6.1. System development controls

The software for all CAs covered by this CPS was developed in-house by the RIPE NCC, working with external consultants. Unit test and succeeding functional tests were required for all components. All software is developed and maintained under a revision control system (git) and releases are tagged. Continuous integration is triggered for each commit and release, which ensures that any possible broken tests come to light before a release is made final.

Code is subject to a review during development. The RIPE NCC Software Development department uses bug and issue tracking software for all development. Prior to deployment to the production service, code is versioned and deployed to a standalone platform for integration tests. The same packages used for these integration tests are then deployed to the production service, provided that no problems are found.

6.6.2. Security management controls

The RIPE NCC uses the same access policy for the servers used to run the Offline CA, the ACA, the Production CA, and hosted CAs; only staff from the responsible departments have SSH access. SSH access is limited to the RIPE NCC office and VPN networks. Access to the systems is logged.

In addition, it should be noted that the Offline CA server is physically switched off when not in use.

6.6.3. Life cycle security controls

Section 6.6.1 contains a description of the software life cycle, including testing prior to release. Deployment of new software releases is on demand, with planned roll-back, and post-deployment testing of service.

Host operating systems are maintained to current patch levels, and CERT (Computer Emergency Response Team) and other security advisories are tracked for relevant vulnerabilities.

Hosts and network infrastructure are physically maintained and replaced in a duty cycle averaging four years. Onsite maintenance contracts cover normal business hours support for this hardware.

6.7. Network Security Controls

The vLAN used for the servers that host the CAs covered by this CPS is protected by router Access Control Lists (ACLs) and/or by firewall rules. This applies both to incoming and outgoing traffic from/to other vLANs, and the same applies for the Internet at large.

Sensitive data is protected by at least one of TLS or SSL with client and server certificates, and with SSH version 2 with 1024-bit keys, or better.

6.8. Time-stamping

The RPKI does not make use of time-stamping.

7. Certificate and CRL Profiles

See [RFC 6487].

8. Compliance audit and Other Assessments

The RIPE NCC employs third parties to perform periodic vulnerability and compliance assessments for computer and network systems, including those that are part of the RPKI CA.

8.1. Frequency or Circumstances of Assessment

Assessments are initiated upon request of the Information Security Officer, Business Owner (Service Manager) or RIPE NCC Senior Management.

Vulnerability assessment is performed every two years; CPS is reviewed every two years; compliance assessment every three years and the procedural assessment is done every three years.

8.2. Identity/Qualifications of Assessors

All third parties engaged to perform the assessment are entities specialising in IT security assessment.

8.3. Assessors' Relationship to Assessed Entity

All third parties engaged to perform assessments are paid contractors, preferably with no other relationships with the RIPE NCC.

8.4. Topics Covered by Assessment

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

The procedural assessment covers a variety of topics including (but not limited to): logging and auditing, network security, configuration management and key signing ceremonies.

The compliance assessment covers a variety of topics including (but not limited to): the cryptographic compliance with the current applicable RFCs.

CPS assessment covers review of the current version of the text including implementation of the findings of the above-mentioned assessments.

8.5. Actions Taken as a Result of Deficiency

The RIPE NCC Security Officer and Business Owner (Service Manager) will review all recommendations made by the external assessors and advise on remedial actions as appropriate.

8.6. Communication of Results

External vulnerability reports are provided to all relevant stakeholders within the RIPE NCC including (but not limited to): the Business Owner, Information Security Officer and Senior Management. When deemed necessary, this information may also be shared with external stakeholders.

9. References

[RFC5280] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008.

[RFC6818] P. Yee, “Updates to the internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, January 2013

[RFC6484] Seo, K., Watro, R., Kong, D., and Kent, S. , "Certificate Policy (CP) for the Resource Public Key Infrastructure (RPKI), February 2012

[RFC6487] Huston, G., Loomans, R., Michaelson, G., "A Profile for X.509 PKIX Resource Certificates", February 2012

[RFC7318] Newton, A, Huston, G, “Policy Qualifiers in Resource Public Key Infrastructure (RPKI) Certificates” July 2014

[RFC6481] Huston, G., Loomans, R., Michaelson, G., "A Profile for Resource Certificate Repository Structure", February 2012

[RFC6482] Lepinski, M., Kent, S., Kong, D., "A Profile for Route Origin Authorizations (ROAs)", February 2012

[RFC6488] Lepinski, M., Chi, A., Kent, S., "Signed Object Template for the Resource Public Key Infrastructure (RPKI)”, February 2012

[RFC6486] Austein, R., Huston, G., Kent, S., Lipinski, M., "Manifests for the Resource Public Key Infrastructure (RPKI)”, February 2012

[RFC6489] Huston, G., Michealson, G., Kent, S., "Certification Authority (CA) Key Rollover in the Resource Public Key Infrastructure (RPKI)” , February 2012

[RFC6490] Huston, G., Weiler, S., Michealson, G., Kent, S., "Resource Public Key Infrastructure (RPKI) Trust Anchor Locator", February 2012

[RFC6485] Huston, G., “The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure (RPKI)”, February 2012

[RFC4387] P. Gutmann, Ed., "Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP", February 2006.

[RFC6492] G. Houston, R. Loomans, B. Ellacott, R. Austein, "A Protocol for Provisioning Resource Certificates”, February 2012

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

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