RIPE NCC RPKI

(Resource Public Key Infrastructure)

Certification Practice Statement (CPS)

RIPE NCC

Document ID: ripe-520
Date: June 2011

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

Last updated December 2010

1. Introduction

As per Certification Policy (CP) [RFCxxxx]:

This Public Key Infrastructure (PKI) is designed to support validation of claims by current holders of Internet number resources (INRs), in accordance with the records of the organisations that act as Certification Authorities (CAs) in this PKI. The ability to verify such claims is essential to ensuring the unambiguous distribution of these resources.

The structure of the Resource PKI (RPKI) is congruent with the number resource allocation framework of the Internet. The IANA allocates Internet number resources to Regional Internet Registries (RIRs), among others, as well as for special purposes [RFC5736]. The RIRs, in turn, manage the allocation of number resources to End Users, Internet Service Providers (ISPs) and others.

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

- CA certificates for each organisation distributing INRs and for the INR holder
- End-entity (EE) certificates for organisations to validate digital signatures on RPKI-signed objects

In addition to the CP [RFCxxxx], relevant information about general PKI concepts may be found in RFC5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

1. 1. Overview

This CPS describes:
- Participants
- Distribution of the certificates and Certificate Revocation Lists (CRLs)
- How certificates are issued, managed and revoked
- Facility management (physical security, personnel, audit, etc.)
- Key management
- Audit procedures

The PKI encompasses several types of certificates:
- CA certificates for each organisation distributing INRs and INR holders
- End entity (EE) certificates for organisations to validate digital signatures on RPKI-signed objects

The Certification Practice Statement is for convenience and informational purposes only. The Terms and Conditions for the RIPE NCC Certification Service can be found at:
http://www.ripe.net/certification/legal/index.html

The RIPE NCC Certification Service Terms and Conditions prevail over the CPS and the CPS does not affect the interpretation of these Terms and Conditions.

1. 2. Document Name and Identification

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

1. 3. PKI Participants

As per CP [RFCxxxx]:

Note: 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

This CPS covers three types of CAs for the RPKI: one Offline CA for the RIPE NCC, one Online CA for the RIPE NCC, and a number of hosted member 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 allowing the RIPE NCC to act as a Trust Anchor in the RPKI. The Online CA allows the RIPE NCC to act as parent CA to RIPE NCC Contributors. This two layer approach provides a secure revocation and recovery capability in case the Online CA is compromised or becomes unavailable. The Offline CA issues certificates only to instances of

the Online CA. The CRLs issued by the Offline CA are used to revoke only a certificate issued to the Online CA. The Online CA is used to issue RPKI certificates to RIPE NCC Contributors, to whom Internet number resources have been distributed.

In addition the RIPE NCC offers a hosted CA service to RIPE NCC Contributors. These CAs are designated "hosted member CAs". The hosted member CAs are highly automated, taking care of the major part of the operational burden for RIPE NCC Contributors who want to act as CAs in the RPKI.

See also 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 or the Online 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 sign-on 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 Contributor) 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

All RIPE NCC Contributors can receive distributions of IP addresses and AS Numbers from the RIPE NCC Online CA and thus are subscribers in the PKI sense.

1. 3. 4. Relying parties

As per CP [RFCxxxx]:
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.

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 address space and/or AS Numbers. With regard to routing security, an initial goal of this PKI is to allow the holder of a set of address blocks to be able to declare, in a 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. CPS Administration

1. 5. 1. Organisation administering the document

Since this CPS describes the implementation of the Offline CA, Online CA and hosted member CAs maintained by the RIPE NCC, this CPS is also administered by the RIPE NCC. However, it should be noted that approval procedures described in section 1. 5. 3-4 apply.

Whenever the implementation is changed, this CPS will be modified and republished as a RIPE Document. When this happens this will be announced through the appropriate communication channels (such as the RIPE NCC's ncc-announce mailing list).

1. 5. 2. Contact person

The RPKI CPS point of contact is the RIPE NCC, Singel 258, 1016AB, Amsterdam, Netherlands.

1. 5. 3. Person determining CPS suitability for the policy

This document is reviewed on behalf of the RIPE community by the Certification Authority Task Force (CA-TF). It is expected that the role of the CA-TF will be transferred to an appropriate RIPE Working Group when the RPKI becomes established as a RIPE NCC service.

1. 5. 4. CPS approval procedures

A RIPE certification policy dealing with issues such as validity times, revocation, re-issuance and access to the services involved is currently being developed by the RIPE community. The implementation of the various CAs (Offline, Online and hosted member CAs) will reflect this policy.

This CPS is not subject to the RIPE Policy Development Process. It provides a detailed outline of the implementation of the RPKI by the RIPE NCC. The CPS is publicly available and when necessary, additional reporting mechanisms, such as mailing lists or presentations at RIPE Meetings, are used to communicate the contents. When the RIPE NCC RPKI implementation is found to be inconsistent with applicable policies the RIPE NCC is committed to update the implementation and this CPS.

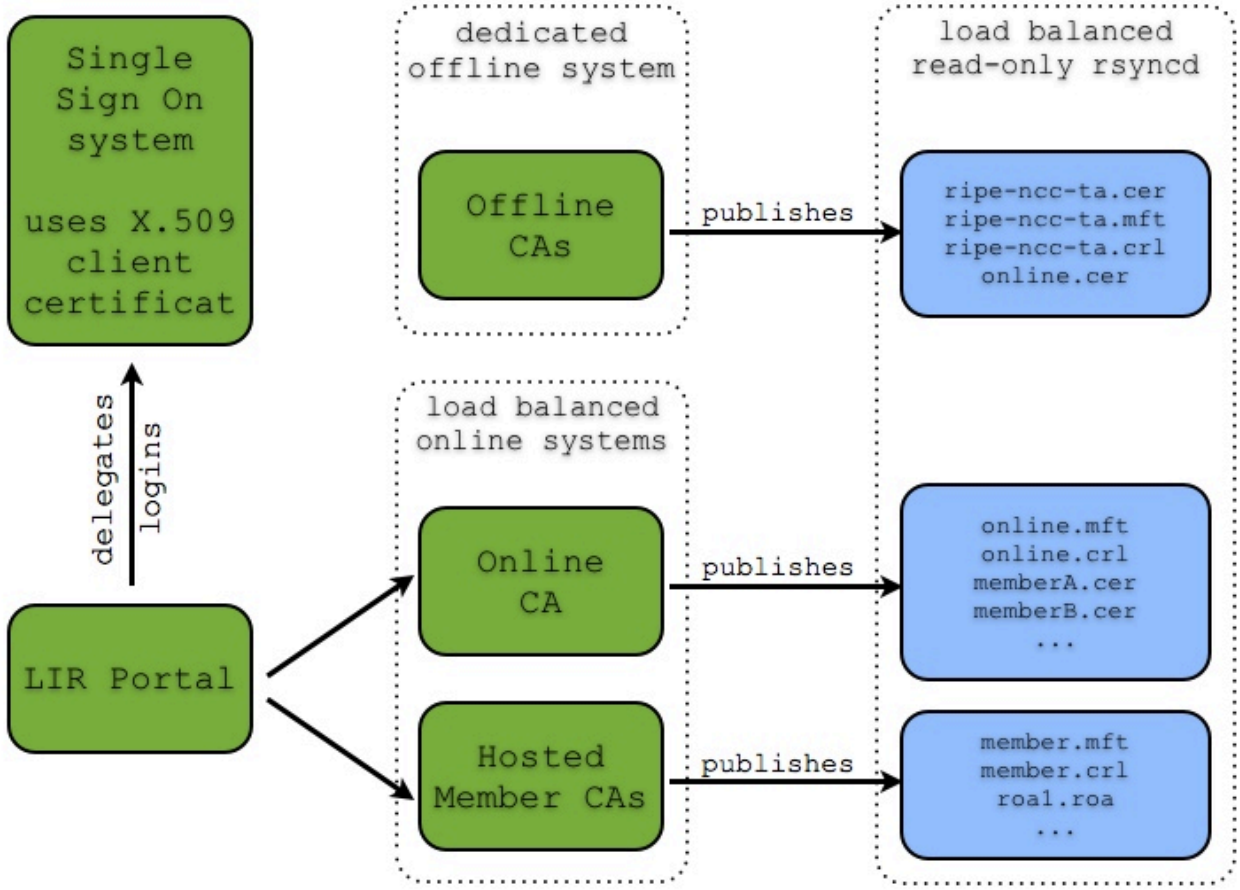
1. 6. Definitions and Acronyms

BPKI	Business PKI: A BPKI is used by the RIPE NCC to identify RIPE NCC Contributors to whom RPKI certificates can be issued.
CA	Certificate Authority. A CA is an entity that issues digital certificates for use by other parties. A CA may issue CA certificates to subordinate CAs. Thus a tree structure of CAs can be created, often dubbed Public Key Infrastructure (PKI). 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 [draft-TA-version4]. In the future this CA may become subordinate to a top level single Trust Anchor CA that will issue certificates to all RIRs.
Online CA	The RIPE NCC Online CA. This CA is used on a daily basis to issue certificates to subordinate hosted member CAs.
Hosted member CA	A hosted member CA that is technically hosted by the RIPE NCC as a RIPE NCC service in the LIR Portal.
CP	Certificate Policy for the Resource PKI (RPKI). See [RFCxxxx].
CPS	Certification Practice Statement. A CPS is a document that specifies the practices that a Certification Authority employs in issuing certificates.
ISP	Internet Service Provider. An ISP is an organisation managing and selling Internet services to other organisations.
LIR	Local Internet Registry. This is an organisation, typically a network service provider, that distributes IP addresses and AS Numbers to End Users and/or uses them in its own infrastructure. RIPE NCC Contributors are usually referred to as "LIRs".
LIR Portal	The public portal provided by the RIPE NCC to its members (LIRs) that allows them access to various RIPE NCC services, including the hosted member CA service. The portal is also used to access the RIPE NCC Online CA by specific users, as described later in this CPS.
RIPE NCC Contributor	A natural person or legal entity that has entered into the RIPE NCC Standard Service Agreement with the RIPE NCC.
RIR	Regional Internet Registry. An RIR is an organisation that manages the distribution and registration of IP address and AS Numbers within a particular region of the world. At present, there are five RIRs: ARIN (North America), RIPE NCC (Europe, the Middle East and parts of Central Asia), APNIC (Asia-Pacific), LACNIC (Latin America and Caribbean) and AfriNIC (Africa).
RP	Relying Party as defined in section 1. 3. 4.

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 [res-certificate-profile]. Certificates come in two flavors: Certificate Authority (CA) Certificates are used by Certificate 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 [RFCsignedobject]). Note the CAs described in this CPS do not currently issue any multi-use End Entity Certificates as described in [res-certificate-profile].
ROA	Route Origin Authorisation. This is a digitally signed object that identifies a network operator, identified by an AS Number, that is authorised to originate routes to a specified set of address blocks. See [RFCroa].
CRL	Certificate Revocation List as described in [res-certificate-profile].
Manifest	A signed object under the RPKI listing all subordinate signed objects and certificates for a CA certificate. See [RFCmanifest].



file	description
ripe-ncc-ta.cer	RIPE NCC Offline CA (Trust Anchor) Certificate.
ripe-ncc-ta.crl	The Certificate Revocation List (CRL) for the RIPE NCC Offline CA (Trust Anchor).
ripe-ncc-ta.mft	The Manifest object listing all subordinate objects and certificates signed by the RIPE NCC Offline CA (Trust Anchor).
online.cer	The Online CA certificate that is signed and published by the RIPE NCC Offline CA (Trust Anchor).
online.crl	The Certificate Revocation List (CRL) for the Online CA.
online.mft	The Manifest object listing all subordinate objects and certificates signed by the Online CA.
member.cer	The member CA certificate that is signed and published by the Online CA.
member.crl	The Certificate Revocation List (CRL) for the member CA.
member.mft	The Manifest object listing all subordinate objects and certificates signed by the member CA.
roa1.roa	A ROA RPKI-signed object for the member CA.

2. Publication And Repository Responsibilities

2. 1. Repositories

As per the CP [RFCxxxx], certificates, CRLs and RPKI-signed objects are made available to all network operators to download, to enable them to validate this data.

2. 2. Publication of Certification Information

RIPE NCC uploads the certificates, CRLs and RPKI-signed objects that it issues to a local repository system that operates as part of a world-wide distributed system of 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 [RFCtrustanchor], follows:

rsync://rpki.ripe.net/ta/ripe-ncc-ta.cer
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0URYSGqU
z2myBsOzeW1jQ6NsxNvlLMyhWknvnl8NiBCs/T/S2XuNKQNZ+wBZ
xIgPPV2pFBFeQAvoH/WK83HwA26V2siwm/MY2nKZ+Olw+wlpzlZ1
p3Ipj2eNcKrmit8BwBC8xImzuCGaV0jkRB0GZ0hoH6Ml03umLprR
sn6v0xOP0+l6Qc1ZHMFVFb385IQ7FQQTcVIxrdeMsoyJq9eMkE6D
oclHhF/NlSllXubASQ9KUWqJ0+Ot3QCXr4LXECMfkpkVR2TZT+v5
v658bHVs6ZxRD1b6Uk1uQKAyHUbn/tXvP8lrjAibGzVsXDT2L0x4
Edx+QdixPgOji3gBMyL2VwIDAQAB

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 member CAs

The hosted member 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 member CA and can be found in the hosted member CA certificate as described in [res-certificate-profile].

Note the repository structure is defined in [RFCrepos].

2. 3. Time or Frequency of Publication

A certificate will be published within 24 hours after issuance.

2. 4. Access Controls on Repositories

Write access to the repositories is limited to the systems running the Offline CA, Online CA and hosted member 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).

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 Offline CA, Online CA and hosted member 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 [RFC4387].

3. 1. 2. Need for names to be meaningful

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

Note: The name of the holder of an address block or AS Number is intended to not be "meaningful" in the conventional, human-readable sense, since certificates issued under this PKI are used for authorisation in support of applications that make use of attestations regarding INR holdings, not for identification.

3. 1. 3. Anonymity or pseudonymity of subscribers

Although subject names in certificates issued by this registry are not 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

The generated subject based on the public key hash, as described in 3.1.1, reduces the likelihood of accidental collisions to a negligible minimum.

3. 1. 6. Recognition, authentication, and role of trademarks

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

3. 2. Initial Identity Validation

3. 2. 1. Method to prove possession of private key

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

For the Online CA that acts as subscriber to the Offline CA, possession of the private keys is effected 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 and thus assures that the private key is appropriately associated with the public key in the certificates issued by each of these CAs

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

3. 2. 2. Authentication of organisation identity

The hosted Member CA is available only to RIPE NCC Contributors. The RIPE NCC has already established procedures to verify the identity of the RIPE NCC Contributors. These procedures are explained here:
http://www.ripe.net/info/faq/membership/newlir-setup.html#1

However it should be noted that certificates issued under this PKI do not attest to the identity of certificate holders. This is also reflected by the seemingly random subject names as described in 3.1.3.

For hosted member 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

The individuals who are authorised to operate the Offline CA are authenticated by possession of the necessary HSM key cards and via physical and procedural security access controls.

For hosted member CAs, individual identity is delegated to the RIPE NCC Contributor's LIR Portal "admin" user. Admin users must set up users for their LIR and associate them with the 'certification' role in order to grant individuals access to the certification section.

The admin user's identity can be (re-)established using the admin password reset procedure:
https://lirportal.ripe.net/lirportal/activation/activation_request.html

The reset procedure involves two halves of a code that are sent via two separate paths, email and fax, that need to be combined in order to reset the "admin" account's password.

For the Online CA, the same mechanism is used as described for hosted member CA users. It should be noted, however, that these users require an additional role that can not be set through the public user management interface.

3. 2. 4. Non-verified subscriber information

No non-verified subscriber data is included in certificates issued under this certificate policy.

3. 2. 5. Validation of authority

Access to the Offline CA is restricted to a Developer that has access to the Unix account on the server. In addition, the HSM key cards are protected by pass phrases known only to the individual CA Operators (see section 5. 2. 3 for a description of the CA Operator role).

Access to the Online CA is restricted to CA Operators using the LIR Portal to log in and having an additional role enabled by the administrators of the single sign-on system (this role can not be set by others).

Access to the hosted member CA is restricted to users of the LIR Portal that have the "certification" role enabled by the "admin" user for their registry.

3. 2. 6. Criteria for interoperation

The RPKI is not intended to interoperate with any other PKI at this stage.

The function of the Online CA will be extended in the future to interoperate with the other four RIRs and RIPE NCC Contributors operating their own CAs.

3. 3. Identification and Authentication for Re-Key Requests

3. 3. 1. Identification and authentication for routine re-key

For the Offline CA and Online CA the same identification and authentication mechanisms apply as described in section 3. 2. 3.

For hosted member 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 member CA is older than five years.

The key roll over algorithm is described in [RFCkeyroll].

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 [RFCkeyroll], after a new key has been activated.

In our 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 Online CA. CA Operators for the Online CA can also revoke old keys for specific hosted member CAs. Identification and authentication for these roles has been described in section 3. 2. 3.

The RIPE NCC implementation may change following discussion of the key rollover standard, as the standard is currently unclear about whether revocation of the old key should be done immediately. Current belief is that there is no reason (security or operational) why old keys should not be automatically revoked after a successful re-key, so that may well be implemented in the near future.

3. 4. Identification and Authentication for Revocation Request

For hosted member CAs it should be noted that user actions in the interface may result in revocation of EE certificates used for objects (such as ROAs) that should be invalidated.

4. Certificate Life-Cycle Operational Requirements

4. 1. Certificate Application

4. 1. 1. Who can submit a certificate application

Any RIPE NCC Contributor may request a certificate.

4. 1. 2. Enrolment process and responsibilities

For the Offline CA a Developer can configure and initialise the CA on a server controlled by the RIPE NCC (see section 5. 2. 1 for a description of the Developer role).

For the Online CA a Developer can install and initialise the application. When this has been done a CA Operator can log in and initialise the Online CA.

For hosted member CAs: RIPE NCC Contributors may use a hosted member CA hosted by the RIPE NCC as part of the RIPE NCC LIR portal. In order to activate the hosted member CA an "admin" user must log in and grant the "certification" role to a normal user. This user must then log in and ensure that a client certificate has been generated for them (or generate one if this is missing). The user that has the "certification" role will then be able to click through on a link labeled "Certification". This link will take the user to a page where they must explicitly opt in to the hosted member CA service - they do this by clicking "Yes, I want to activate my hosted member CA". After activation, a mostly automated hosted member CA will be created. Authentication and authorisation for further automated processes should be considered transitive from the moment that user opted-in and activated the hosted member CA, as described here.

4. 2. Certificate Application Processing

For hosted member CAs an initial CA certificate is requested automatically by the system when the authorised user chooses to opt in to the service.

4. 2. 1. Performing identification and authentication functions

See section 3. 2. 3.

4. 2. 2. Approval of certificate applications

The online CA will issue certificates to hosted member CAs with a validity time to the end of the calendar year, plus a six months grace period to allow for renewal before the certificate expires.

All Provider Aggregatable (PA) resources registered to the RIPE NCC Contributor at the time of issuance will be included in the certificate.

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

4. 2. 3. Time to process certificate applications

The RIPE NCC will issue a certificate attesting to resource allocations within one business day of approval of the certificate application.

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 Online CA, where it is published.

The Online CA and hosted member CAs make all subordinate certificates and objects available for publication. In practice, the system will make a best effort to publish these materials as soon as possible, but as described in section 2. 3, publication should happen within no more than 24 hours of issuance.

4. 3. 2. Notification to subscriber by the CA of issuance of certificate

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

4. 3. 3. Notification of certificate issuance by the CA to other entities

Publication of a certificate in the repository operated by 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

A subscriber is presumed to have accepted a certificate issued by any of the Certificate Authorities covered by this CPS and published in the RIPE NCC repository unless the subscriber contacts the RIPE NCC.

4. 4. 2. Publication of the certificate by the CA

Certificates will be published in the repository system within one business day of being issued by any of the CAs covered by this CPS.

4. 5. Key Pair and Certificate Usage

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

4. 5. 1. Subscriber private key and certificate usage

The hosted member 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 member CA certificates will only be used (by the system) to issue EE certificates used for RPKI-signed objects (such as ROAs) and manifests.

4. 5. 2. Relying party public key and certificate usage

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

Before any act of reliance, relying parties MUST independently (1) verify that the certificate will be used for an appropriate purpose that is not prohibited or otherwise restricted by this CPS (see section 1. 5), and (2) assess the status of the certificate and all the CAs in the chain (terminating at the RIPE NCC Trust Anchor) that issued the certificates relevant to the certificate in question. If any of the certificates in the certificate chain have been revoked, 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.

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 [RFCyyyy], which specifies the extended validation algorithm for RPKI certificates.

4. 6. Certificate Renewal

Note that the hosted member 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 member CAs are mentioned a few times in this section as children of the Online CA.

4. 6. 1. Circumstance for certificate renewal

For hosted member CAs: When new Internet number resources are associated with a RIPE NCC Contributor or a new validity time is applicable (see section 4. 2. 2) a certificate will be renewed.

Note that in case Internet number resources are no longer associated with a RIPE NCC Contributor the Online CA 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 member CAs, requests for renewal are fully automated.

For the Online CA, RIPE NCC staff with the Online CA Administrator role can request renewal from the Offline CA.

For the Offline CA, Internet number resources may have to be added to the self-signed certificate. RIPE NCC staff with the appropriate role may perform this action.

4. 6. 3. Processing certificate renewal requests

The same stipulations listed in section 4. 2. 2 apply here.

4. 6. 4. Notification of new certificate issuance to subscriber

See section 4. 3. 2.

4. 6. 5. Conduct constituting acceptance of a renewal certificate

See section 4. 4. 1.

4. 6. 6. Publication of the renewal certificate by the CA

Both the Offline CA and Online CA will publish renewed subordinate CA certificates within one business day of issuance.

4. 6. 7. Notification of certificate issuance by the CA to other entities

See section 4. 3. 2.

4. 7. Certificate Re-Key

Note that the hosted member 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 member CAs are mentioned a few times in this section as children of the Online CA.

4. 7. 1. Circumstance for certificate re-key

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

1. Knowledge or suspicion of compromise or loss of the associated private key, or
2. Expiration of the cryptographic lifetime of the associated key pair

If a certificate is revoked to replace the resource extensions (see [res-certificate-profile], 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

For hosted member CAs, an automated key roll over is performed when the key has been in use for five years. Authentication and authorisation for this is considered transitive from opt in (see section 4. 1. 2).

For the RIPE NCC Online CA, a manual key rollover is planned to be performed every five years. This manual rollover can be initiated by RIPE NCC staff in the Online CA Administrator role.

4. 7. 3. Processing certificate re-keying requests

The same stipulations listed in section 4. 2. 2 apply 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 Certificate Authorities covered by this CPS, a re-keyed certificate will be published in the repository system within one business day of being issued by this CA.

4. 7. 7. Notification of certificate issuance by the CA to other entities

See section 4. 3. 3.

4. 8. Certificate Modification

4. 8. 1. Circumstance for certificate modification

Certificate modification is not applicable to the CAs described here. Renewal is used when new resources are to be certified, or a new validity time is applicable, as described in section 4. 6. Re-issuance and revocation is used when resources are no longer held by an entity, as described in section 4. 9.

4. 9. Certificate Revocation and Suspension

4. 9. 1. Circumstances for revocation

Certificates can be revoked for several reasons:

- A signed object needs to be invalidated
- One or more listed Internet number resources are no longer associated with the RIPE NCC Contributor
- As the last steps when doing a planned re-key (clean up)
- As the last steps when doing an unplanned re-key because a loss or compromise of the old key has come to light

4. 9. 2. Who can request revocation

For the hosted member CAs, revocation of their CA certificate can be performed by RIPE NCC staff on request or when RIPE NCC staff have reason to believe the keys are compromised. In the latter case this will always be performed as the final step of an emergency key rollover for the hosted member CA. The other circumstances for revocation, most notably when ROA objects need to be invalidated because a user of the hosted member CA changes the specification, are managed automatically by the system.

For the Online CA, 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 Internet number resources listed in a certificate are no longer associated with a RIPE NCC Contributor, the Online CA will:

- Re-issue a new certificate, minus the lost Internet number resources, but maintaining all other properties
- 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 member CA that list the lost Internet number resources, thus invalidating any signed objects (such as ROAs) that refer to these Internet number resources.

4. 9. 4. Revocation request grace period

Any party that is able to identify the need for revocation that is not already handled by the system and operators is expected to notify the RIPE NCC within one business day.

4. 9. 5. Time within which CA must process the revocation request

The RIPE NCC will process a revocation request within one business day of receipt and validation of the 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 that relying party validates a certificate.

4. 9. 7. CRL issuance frequency

Each CRL will carry a nextScheduledUpdate value and a new CRL will be published at or before that time. The RIPE NCC will set the nextScheduledUpdate 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
Online CA:	24 hours from the moment of issuance
Hosted member CAs:	24 hours from the moment of issuance

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

It should be noted that the values listed here may be used by relying parties to determine the need to fetch an updated CRL. In particular this means that a possible revocation by the Offline CA may go unnoticed for three months - this should not be a problem since the production keys are protected by an HSM. A revoked ROA for a hosted member CA may not be noticed for 24 hours. The values here should be regarded as a compromise between various aspects, including the operational burden of re-signing (for Offline CA), time needed to be able to do an emergency restore, efficiency of caching in the global RPKI, propagation time of revocation in the global RPKI.

4. 9. 8. Maximum latency for CRLs

A CRL will be posted to the repository system within one hour of issuance.

4. 9. 9. On-line revocation/status checking availability [OMITTED]

4. 9. 10. On-line revocation checking requirements [OMITTED]

4. 9. 11. Other forms of revocation advertisements available [OMITTED]

4. 9. 12. Special requirements re key compromise [OMITTED]

4. 9. 13. Circumstances for suspension [OMITTED]

4. 9. 14. Who can request suspension [OMITTED]

4. 9. 15. Procedure for suspension request [OMITTED]

4. 9. 16. Limits on suspension period [OMITTED]

4. 10. Certificate Status Services

These CAs do not support Online Certificate Status Protocol (OCSP), but rather use Certificate Revocation Lists (CRLs).

4. 10. 1. Operational characteristics [OMITTED]

4. 10. 2. Service availability [OMITTED]

4. 10. 3. Optional features [OMITTED]

4. 11. End of Subscription [OMITTED]

4. 12. Key Escrow and Recovery [OMITTED]

4. 12. 1. Key escrow and recovery policy and practices [OMITTED]

4. 12. 2. Session key encapsulation and recovery policy and practices [OMITTED]

5. Facility, Management and Operational Controls

5. 1. Physical Controls

5. 1. 1. Site location and construction

For the Offline CA, operations are conducted within a physically protected area of an office building in which the RIPE NCC is a tenant. This building is located at:

Singel 258
1016AB Amsterdam
The Netherlands

The RIPE NCC space within this facility includes offices and meeting spaces and two machine rooms.

For the Production CA and hosted member CAs, core cryptographic operations are performed by two machines physically located in two different data centers in a load balanced (and fail over) set up.

The two data centers are:

Nikhef:
Science Park 105
1098XG Amsterdam
The Netherlands

Telecity 2:
Kuiperbergweg 13
1101AE Amsterdam
The Netherlands

5. 1. 2. Physical access

For the Offline CA, physical access is restricted to the RIPE NCC's IT staff and senior managers. The access system relies on personal smart cards. Access to areas is logged every moment of the day on our access system, this data is mirrored at the same moment to another server, located in another building. CCTV is in operation and recordings are kept for one week.

For Nikhef, physical IT staff may request access for themselves. IT management may request access for others. Access is logged by the reception and the electronic access system. The server is physically located in one of five racks rented by the RIPE NCC. The racks are kept locked and have their own key set. They are located in a machine room that includes rack space rented by third parties.

For Telecity2, IT staff may request access for themselves. IT management may request access for others. The server is physically located in one of four racks rented by the RIPE NCC. The racks are housed in a special suite, dedicated to the RIPE NCC only. Only Telecity2 staff can open the suite for us and access is logged by the reception.

5. 1. 3. Power and air conditioning

The offline CA server is located in an air conditioned server room in the RIPE NCC office building. At the moment of writing we do not monitor power, but we are running a project to overcome this. It should be noted that power outages are not expected to have an impact on this CA since it is kept offline when not in use.

For Nikhef, power consumption and air conditioning are monitored by the provider. Should power consumption exceed the maximum allowance, the RIPE NCC will receive an invoice, but power will not be cut. Nikhef has an uninterruptible power supply (UPS) to overcome immediate power failures, and a generator with enough fuel to cover for arrival of more fuel and/or fixing the power failure.

For Telecity2, power consumption and air conditioning are monitored by the provider. Should power consumption exceed the maximum allowance, the RIPE NCC will receive an invoice, but power will not be cut. Telecity2 has a UPS to overcome immediate power failures, and a generator with enough fuel to cover for arrival of more fuel and/or fixing the power failure.

5. 1. 4. Water exposures

The RIPE NCC server room used by the Offline CA is located on the second floor of the office building. This is above sea level.

The server room located at Nikhef is located on the first floor of their building. This is above sea level.

The server room located at Telecity2 is located on the first floor of their building.

5. 1. 5. Fire prevention and protection

The RIPE NCC server room used by the Offline CA has fire extinguishing equipment that is sufficient for any fire in the server rooms. The server rooms are monitored by our security company, and in case of fire they will contact the fire brigade of Amsterdam.

5. 1. 6. Media storage

Whenever the Offline CA is operated, all data is backed up (encrypted where needed) to a network filesystem that is mirrored between the Nikhef and Telecity2 datacenters. In addition this data is backed up off-site nightly (see section 5. 1. 8).

For the Online CA and hosted member CAs all data is stored (encrypted where needed) on a network filesystem that is mirrored between the Nikhef and Telecity2 datacenters. In addition this data is backed-up off-site nightly (see section 5. 1. 8).

5. 1. 7. Waste disposal

When servers reach their end of life, the hard disks are physically destroyed by RIPE NCC staff.

Key cards will be destroyed if they are found to be broken. If a key card is lost a new card set will be generated and all HSM keys will be migrated to the new card set in order to ensure that the lost card is rendered useless.

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, located in Ede, the Netherlands. The distance between this site and Amsterdam is approximately 70km. Ede is above sea level.

5. 2. Procedural Controls

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.
CA Operator	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. There are ten CA Operators. Five of the CA operators 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).
Developer	Has access to the source code used to run the Offline CA. Is responsible for developing, testing and deploying new releases. In addition, the Developer 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:

System Operator	Same as for Offline CA.
Developer	Has access to the source code used to run the Online CA. Is responsible for developing, testing and deploying new releases. In addition the Developer 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.
ACS Card holder	The ACS Card Holder receives one of five cards making up the ACS for the HSMs used for the Online CA and hosted member CAs. Three of these five cards are needed to perform a restore. There are five ACS Card Holders.

For the hosted member CAs:

System Operator	Same as for Offline CA.
Developer	Same as for Online CA.
CA Operator	Has access to the user interface. The 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 member 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 member CAs.

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	Root 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 that the IT staff have access to the server room (see section 5. 1. 2) in order to log in.
CA Operator	Has no account on the server, but will be asked by the Developer to present their key card and enter their passphrase for authentication and authorisation of the operation.
Developer	The Developers can login to the Unix account that is used to run the Offline CA software.

For the Production CA:

System Operator	Same as for Offline CA.
Developer	The Developers 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 that a username, password and client certificate are presented. In addition, the CA Operator must be a member of a specific group that is not available to public users of the LIR Portal.

For the hosted member CAs:

System Operator	Same as for Online CA.
Developer	Same as for Online CA.
CA Operator	The CA operator uses the RIPE NCC single sign-on system to log in to the user interface. The login process requires that a username, password and client certificate are presented. In addition the CA Operator must be made a member of the "certification" group by the "admin" user for their LIR in the LIR Portal.

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

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 CA staff with training upon assignment to a CA role as well as on-the-job training as needed to perform their job responsibilities competently.

5. 3. 4. Retraining frequency and requirements

The RIPE NCC provides its CA 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 enforced job rotation among staff fulfilling trusted CA roles.

5. 3. 6. Sanctions for unauthorised actions

If RIPE NCC staff are determined to have performed activities inconsistent with RIPE NCC RPKI policies and procedures, appropriate disciplinary action will be taken.

5. 3. 7. Independent contractor requirements

No independent contractor or consultant is used to perform any of the roles for the CAs covered by this document. Contractors who are required to perform any maintenance functions on CA severs or cryptographic modules must be escorted and directly supervised by RIPE NCC staff at all times when in sensitive areas.

Independent contractors and consultants may be part of the development team, but never constituting more than 50% of the total team.

5. 3. 8. Documentation supplied to personnel

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

5. 4. Audit Logging Procedures

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 Online CA and hosted member CAs. Audit 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 separately maintains logs for access to the areas housing sensitive CA equipment.

5. 4. 2. Frequency of processing log

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

5. 4. 3. Retention period for audit log

Audit records for the Online CA and hosted member 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. This process is currently under review, and may change in the near future.

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 employs an outside firm to perform periodic vulnerability assessments for computer and network systems and the software that was 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. Key Changeover

The Offline CA currently acts as a Trust Anchor. An emergency key rollover has been practiced for the current set-up.

The Online CA key pair changes on a scheduled basis. The algorithm used is described in [RFCkeyroll]. Initiating the re-key is a manual action initiated by a Online CA Operator via the user interface.

The hosted member CAs perform an automated re-key using the algorithm described in [RFCkeyroll]. This happens whenever a key has been in use for five years.

5. 6. CA or RA Termination

The RIPE NCC has been granted sole authority by the Internet Assigned Numbers Authority (IANA) to manage allocation of IP address space and AS Number resources in the RIPE NCC 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 member CAs operated by 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 hardware cryptographic module employed for this process is the nCipher nShield9000e.

6. 1. 2. Private key delivery to subscriber

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

6. 1. 3. Public key delivery to certificate issuer

For the Offline CA, a custom mechanism has been developed to transfer certificate sign requests and/or revocation requests that include the Online CA public key hash. Since the Offline CA server is not connected to a network, the transfer is done using XML files on a USB stick (a.k.a. sneaker net).

The hosted member CAs and Online CA are managed by the same software. Therefore the Online CA has direct access to the member public keys and no key delivery is involved.

6. 1. 4. CA public key delivery to relying parties

For the Online CA and hosted member CAs, 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) to the repository.

The Offline CA is intended to be used as a Trust Anchor by relying parties. Its Trust Anchor Locator [RFCtrustanchor] is described in section 2. 2. The RIPE NCC will publish this Trust Anchor Locator at:
http://www.ripe.net/certification/validation

It may also publish this via other mechanisms, such as printed material, RIPE Meeting presentations or in Member Updates.

6. 1. 5. Key sizes

As per [RFCalgokeysize], the CAs covered by this CPS use a 2048-bit RSA key for all keys, including the keys used for EE certificates.

6. 1. 6. Public key parameters generation and quality checking

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 are consistent with [RFC5280]. 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 Online CA and hosted member 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 Online CA and hosted member CAs 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 on disk by the HSM using Advanced Encryption Standard (AES) encryption with a key that is protected by a 3-out-of-5 Administrative Card Set.

For the Offline CA, the files containing the encrypted private key and other necessary information are copied to fileshare that is duplicated between the Nikhef and Telecity2 data centres after every operation. These files are backed up off-site on a nightly basis to a remote site located in Ede, the Netherlands, 70 km from Amsterdam.

For the Online CA and hosted member CAs, all encrypted private keys and other necessary information are stored on a fileshare that is duplicated between the Nikhef and Telecity2 data centers after every operation. These files are backed up off-site on a nightly basis to a remote site located in Ede, the Netherlands, 70 km from Amsterdam.

6. 2. 5. Private key archival

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

6. 2. 6. Private key transfer into or from a cryptographic module

The 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 Online CA and member CAs.

6. 2. 7. Private key storage on cryptographic module

The private keys for all CAs covered by this CPS may be temporarily stored inside 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 to disk in 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 Online CA and hosted member CAs, the private keys can be used by all processes that run on the physical servers that host the nCipher nShield9000e PCI cards.

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 is shut down again.

The cryptographic modules for the RIPE NCC RPKI CA and hosted member 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 on disk in encrypted form. When keys are no longer in use they are deleted from disk. 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 Online CA and hosted member 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 after 1 Jan 2011.

For the Online CA and hosted member CAs, key pairs have an intended validity interval of five years.

6. 4. Activation Data

6. 4. 1. Activation data generation and installation

For the Offline CAs, the 3/5 Administrative Card Set (ACS) and the 3/10 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 Online CA and the hosted member CAs, the 3/5 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

6. 5. 1. Specific computer security technical requirement

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 otherwise empty USB sticks.

The Online CA and hosted member 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. These will delegate requests for the "certification" section only to the back-end machines.

6. 5. 2. Computer security rating [OMITTED]

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 together with external consultants. The RIPE NCC software development follows an "agile" methodology that includes test-driven development. Unit test coverage of at least 75% and succeeding functional tests were required for all components. All software is developed and maintained under a revision control system (subversion) and releases are tagged. Continuous integration is triggered for each commit and each release and ensures that any possible broken tests come to light before a release is made final. Code is subject to a code review during development. The RIPE NCC software development uses bug and issue tracking software for all software 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 deployed to the production service, provided that no problems were found.

6. 6. 2. Security management controls

The RIPE NCC uses the same access policy for the servers used to run the Offline CA and the Online and member 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.

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

6. 6. 3. Life cycle security controls

See section 6. 6. 1 for a description of the software life cycle, including testing prior to release. Deployment of new software releases is scheduled, with planned back-out, and post-deployment testing of service.

Host operating systems are maintained to current patch levels, and CERT and other security advisories are tracked for relevant vulnerabilities.

Hosts and network infrastructure are physically maintained and replaced in 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. We do not currently have a dedicated vLAN for these servers, though we plan to look into this in the near future.

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. Extra care is taken for private data: PGP encryption is mandatory.

6. 8. Time-Stamping

The RPKI operated by the RIPE NCC does not make use of or provide a Time Stamping Authority as defined by RFC3161.

7. Certificate and CRL Profiles [OMITTED]

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

8. Compliance Audit and Other Assessments

The RIPE NCC employs an outside firm to perform periodic vulnerability 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 at the behest of the Information Security Officer, Business Owner (Service Manager) or RIPE NCC Senior Management.

8. 2. Identity/Qualifications of Assessor

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

8. 3. Assessor's Relationship to Assessed Entity

The outside firm engaged to perform the assessment is a paid contractor with no other relationships to 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, logging and auditing, network security, and configuration management.

8. 5. Actions Taken as a Result of Deficiency

The RIPE NCC Security Officer reviews all recommendations made by the external assessor and will advise on remedial actions as appropriate.

8. 6. Communication of Results

The 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.

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.

[RFCxxxx] Seo, K., Watro, R., Kong, D., and Kent, S. , "Certificate Policy for the Internet IP Address and AS Number PKI", work in progress, July 2007.

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

[RFCrepos] Huston, G., Loomans, R., Michaelson, G., "A Profile for Resource Certificate Repository Structure", work in progress, May 2010.

[RFCroa] Lepinski, M., Kent, S., Kong, D., "A Profile for Route Origin Authorizations (ROAs)", work in progress, November 2010.

[RFCsignedobject] Lepinski, M., Chi, A., Kent, S., "Signed Object Template for the Resource Public Key Infrastructure", work in progress, October, 2010

[RFCmanifest] Austein, R., Huston, G., Kent, S., Lipinski, M., "Manifests for the Resource Public Key Infrastructure", work in progress, November 2010

[RFCkeyroll] Huston, G., Michealson, G., Kent, S., "CA Key Rollover in the RPKI", December 2010

[RFCtrustanchor] Huston, G., Weiler, S., Michealson, G., Kent, S., "Resource Certificate PKI (RPKI) Trust Anchor Locator", work in progress, November 2010

[RFCalgokeysize] Huston, G., "A Profile for Algorithms and Key Sizes for use in the Resource Public Key Infrastructure", work in progress, November 2010

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

[res-certificate-profile] Huston, G., Loomans, R., Michaelson, G., "A Profile for X.509 PKIX Resource Certificates".

[up/down] G. Houston, R. Loomis, B. Ellacott, R. Austien, "A Protocol for Provisioning Resource Certificates,"

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

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

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