Rutinbeskrivning

BESLUTSDATUM:	2014-03-03
BESLUT AV:	Anders Nordlander
BEFATTNING:	Riskchef
ANSVARIG AVDELNING:	Stabsavdelningen
FÖRVALTNINGSANSVARIG:	Lars Andersson och Ulf Grahn
HANTERINGSKLASS	ÖPPEN
Senast granskad:	2023-11-28

SVERIGES RIKSBANK
SE-103 37 Stockholm
(Brunkebergstorg 11)

Tel +46 8 787 00 00
Fax +46 8 21 05 31
registratorn@riksbank.se
www.riksbank.se

DNR 2014-184-STA

Certifikatspolicy för Sveriges riksbank PKI

Sveriges riksbank utfärdar elektroniska certifikat för interna ändamål såväl som externa genom sin Public Key Infrastructure (PKI). Certifikaten används av användare, system och funktioner för autentisering, kryptering och digitala signaturer.

En certifikatpolicy beskriver hur detta görs, både tekniskt, organisatoriskt och administrativt. En förlitande part kan med hjälp av detta avgöra i vilken mån det är möjligt att lita på de certifikat som utfärdas av Sveriges riksbank och även i övrigt bedöma deras lämplighet för olika tillämpningar.

Detta styrande dokument är skrivet på engelska i syfte att fungera även i internationella sammanhang, exempelvis då en organisation utanför Sveriges gränser önskar upprätta förtroende för certifikat utfärdade av Sveriges riksbank PKI.

Sveriges Riksbank PKI Certificate Policy

Sveriges Riksbank issues electronic certificates for internal as well as external purposes through its Public Key Infrastructure (PKI). The certificates are used by users, systems and functions for authentication, encryption and digital signatures.

A certificate policy describes how this is done, technically, organizational and administrative. A relying party can with this help decide whether the certificates issued by Sveriges Riksbank are sufficiently trustworthy and otherwise appropriate for a particular application.

This policy is written in English for the purpose to function in an international context, for example when an organization from outside of Sweden wishes to establish trust in certificates issued by Sveriges Riksbank.

Table of Content

1 Introduction

1.1 Overview

This document sets out the Certificate Policies (CP) governing the certificates issued by the Certification Authorities of Sveriges Riksbank Public Key Infrastructure (RB-PKI)

The document follows the structure and recommendations laid out in RFC 3647[1]. For clarity, all sections in RFC 3647 have been included. Where nothing has been established for a particular section the phrase "No stipulation" will appear.

The Certificate Policies is complemented by a Certification Practice Statement in which the techniques and procedures that fulfil the demands in the CP are detailed. In cases where there is conflicting information between CP, CPS and other PKI documentation, information in this CP always takes precedence.

From the perspective of the X.509 v3 standard, a Certificate Policy is a set of rules that define the applicability or use of a certificate within a community of users, systems or specific class of applications that have a series of security requirements in common.

The certificates covered in these policies adhere to three different assurance levels:

> **Basic assurance** – non-personal certificates or personal certificates with a limited binding with the holder. Certificates can only guarantee that it is probable that the activities are actually carried out by the intended holder (subject).
>
> **Medium assurance** – personal certificates with a strong binding with the holder. Certificates guarantee that activities are carried out by the intended holder.
>
> **High assurance** – personal certificates with a very strong binding with the holder. Certificates guarantee that the holder could not deny carrying out the activities.

Note: High assurance certificates are not fully covered in the CP since no certificates of this type are currently being issued, but might be in future versions.

Certificates can be used for one (or several) of the following purposes:

> **Authentication** – the process of determining whether someone or something is, in fact, who or what it is declared to be.
>
> **Encryption** – the conversion of data into a form that cannot be easily understood by unauthorized people or systems.
>
> **Digital signature** – the binding between a collection of information and the signer that guarantees that the information has not been tampered with and that the signer is not able to repudiate the act.

Certificates can be issued to:

[1] Internet Engineering Task Force. Public Key Infrastructure Standards Working Group.
Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework (RFC 3647).

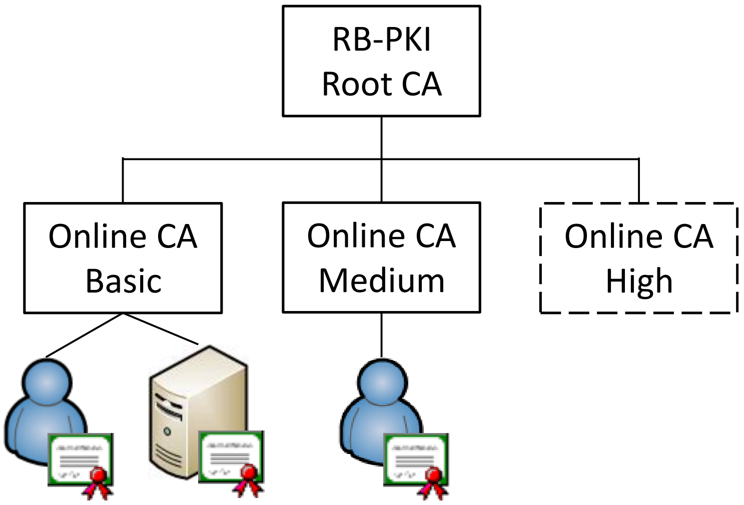
Users – physical persons from Riksbank staff, subcontractors, customers etc.

Systems – computers, services, applications etc.

Functions – organisational units, generic users, projects etc.

Medium and high assurance certificates can only be issued to users.

The general architecture of RB-PKI, in hierarchic terms, is as follows:



For further reading, it is assumed that the reader of this document is familiar with the concepts of certificates and public key infrastructure.

1.2 Document Name and Identification

This document replaces the previous CP version “Sveriges Riksbank Medium Assurance Certificates version v1.0” published at *http://www.riksbank.se/pki/*

Document name	Certificate Policies (CP) for Sveriges Riksbank
Document version	1.1g
Document status	Approved
Date of issue	2023-11-28
OID (Object Identifiers)	1.2.752.91.21.1.2.0: Certificate policies for Sveriges Riksbank (this document) 1.2.752.91.21.1.2.0.1.1: Certificate Policy for basic assurance certificates used for authentication. 1.2.752.91.21.1.2.0.1.2: Certificate Policy for basic assurance certificates used for encryption. 1.2.752.91.21.1.2.0.1.3: Certificate Policy for basic assurance certificates used for digital signature.

	1.2.752.91.21.1.2.0.2.1: Certificate Policy for medium assurance certificates used for authentication. 1.2.752.91.21.1.2.0.2.2: Certificate Policy for medium assurance certificates used for encryption. 1.2.752.91.21.1.2.0.2.3: Certificate Policy for medium assurance certificates used for digital signatures. 1.2.752.91.21.1.2.0.3.1: Certificate Policy for high assurance certificates used for authentication. (Not covered in this version) 1.2.752.91.21.1.2.0.3.2: Certificate Policy for high assurance certificates used for encryption. (Not covered in this version) 1.2.752.91.21.1.2.0.3.3: Certificate Policy for high assurance certificates used for digital signatures. (Not covered in this version)
CPS location	The CPS is published at Riksbank official website. Https://www.riksbank.se/pki
Related CPS	Certification Practice Statement of RB-PKI OID: **1.2.752.91.21.1.2.1**

1.3 PKI Participants

This section describes the types of entities that fill the roles of participants within RB-PKI.

1.3.1 Certification Authorities

The RB-PKI consists of two distinct levels of Certification Authorities:

- Root CA (offline)
- Issuing CAs

The Root CA certificate is self-signed and does not depend on the other CAs. The Root CA signs the certificates of the issuing CAs.

Issuing CA:s are responsible for creating and signing certificates for applicants and subscribers. Each issuing CA is responsible for issuing certificates of one specific trust level only (basic, medium or high).

Certification Authorities are also responsible for supplying information on the status of issued certificates by regularly publishing lists of revoked certificates (CRLs).

1.3.2 Registration Authority

The Registration Authority (RA) is responsible for the following tasks:

- registration and verification of the information contained in certificate applications,
- preparation and technical transmission of certificate and revocation requests to the CA,
- archiving requests.

It is also responsible for the secure transmission of private key activation data.

The RA may rely on a Delegated Registration Officer (RO) to carry out some or all information verification tasks. In this case, the RA makes sure that applications are complete, exact and carried out by a duly authorized Delegated RO.

1.3.3 Subscribers

The subscriber is the entity to whom the certificate is issued.

Certificates can be issued to users, systems or functions. Medium and high assurance certificates can only be issued to users.

All issued certificates must bind to an entity that is in possession of the private key that corresponds to the public key specified in the certificate.

1.3.4 Relying parties

Relying parties are organisations, persons or systems who, for the purpose of verifying the correctness of an identity or digital signature, trust certificates issued by Sveriges Riksbank.

1.3.5 Other participants

No stipulation.

1.4 Certificate Usage

1.4.1 Appropriate certificate use

The certificates, with their corresponding keys, could be used for authentication, signing and/or encryption purposes, depending on the corresponding keyUsage extension and OID attribute in the certificatePolicies extension.

1.4.2 Certificate Usage Constraints and Restrictions

Sveriges Riksbank may not be held liable in the event that a certificate is used for a purpose other than those referred to in the preceding paragraph.

1.4.3 CA key usage

For technical reasons the Riksbank Root CA and all Issuing CA in the organisation have the ability for document signing. But this ability is not allowed to be used for any reason as document signing always have to be verified to a physical subscriber.

1.5 Policy Administration

1.5.1 Organization administering the document

Chief Risk Officer, head of Risk Division, is the owner of this document and is responsible for approval of the CP.

The Risk Division, part of General Secretariat, is responsible for drafting, registering, maintaining, and updating the document.

Name	Chief Risk Officer
E-mail address	registratorn@riksbank.se
Phone	+46 8 787 00 00
Postal Address	Sveriges Riksbank Risk Division SE-103 35 Stockholm, Sweden

1.5.2 Contact Person

This CP is managed by the Risk Division of Sveriges Riksbank:

Name	Risk Division
E-mail address	pki@riksbank.se
Phone	+46 8 787 00 00
Postal Address	Sveriges Riksbank Riskenheten SE-103 35 Stockholm, Sweden

1.5.3 Person determining CPS suitability for the policy

The RB-PKI system owner determines CPS suitability for the policy. Head of IT of Sveriges Riksbank, or equivalent, is the system owner of the RB-PKI system.

1.5.4 CPS approval procedures

The CPS document shall be reviewed and endorsed by the CP owner.

■ The CPS document shall thereafter be submitted to the RB-PKI system owner for acceptance and accreditation.

1.6 Definitions and Acronyms

1.6.1 Definitions

Within the scope of this CP the following terms are used:

Term	Definition
Certificate Revocation List (CRL)	List of the serial numbers of unexpired certificates that have been revoked. The CRL is signed by the Certification Authority to ensure integrity and authenticity.
Certification Authority (CA)	The core component of the PKI, the Certification Authority is the entity that issues certificates to a community of holders and to other infrastructure components.
Certificate Policy (CP)	Set of rules that indicate the applicability of a certificate to a particular community or to applications with common security requirements.
Certification Practice Statement (CPS)	Set of practices that must be implemented to comply with the requirements of the CP.
Component	Platform operated by an entity, comprising at least a computer workstation, software and, as the case may be, cryptological capabilities, and playing an identified role in the operational implementation of at least one PKI function.
Key pair	Set comprising a public key and a private key that form an indissociable pair used by an asymmetric cryptographic algorithm.
Object Identifier (OID)	Unique identifier used to reference the CP with another organisation.
Organisation	Entity with which a holder is affiliated.
Private key	Confidential component of a key pair, known only to the owner and used solely by the owner to authenticate or to decrypt inbound data or to sign data authored by the owner.
Public key	Non-confidential component of a key pair that may be communicated to all members of a community. A public key may be used to encrypt data for the holder of the key pair. It may also be used to verify the holder's signature.
Public key certificate	Certain type of message (e.g. X. 509 v3) that is created and signed by a recognised Certification Authority, which guarantees the authenticity of the public key contained in the message. As a minimum, a certificate contains the holder's identifier and public key. The Certification Authority signs certificates using its own private key.
Public Key Cryptographic Standards (PKCS)	Set of cryptographic standards for public keys.
Public Key Infrastructure	Set of components, functions and procedures dedicated to the management of key pairs and certificates.

Registration Authority (RA)	Entity responsible for processing certificate applications and for certificate lifecycles.
Registration Officer (RO)	The certificate manager role of the PKI environment
Root Certification Authority	Certification Authority whose certificates are self-signed. The Root Certification Authority signs the certificates of Subordinate Certification Authorities.
RSA algorithm	Invented in 1978 by Ronald L. Rivest, Adi Shamir and Leonard M. Adleman, the RSA algorithm may be used to encrypt and/or sign (digital signature) information.
Subordinate Certification Authority	Certification Authority whose certificate is signed by the Root Certification Authority. A Subordinate Certification Authority signs holders' certificates.
RB-PKI	Certification Authorities of Sveriges Riksbank Public Key Infrastructure

1.6.2 Acronyms

Within the scope of this CP the following acronyms are used:

ARL	Authority Revocation List
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
HSM	Hardware Secure Module
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RO	Registration Officer

2 Publication and Repository Responsibilities

2.1 Responsibility for making information available

The RB-PKI System Owner is responsible for making published information available.

2.2 Published information

Information concerning the issuer and related documents shall be made available on the intranet and the external website of Sveriges Riksbank, according to the following table.

Published information	Published at (scope)
Certificate Policy (this document)	Sveriges Riksbank intranet (all versions) http://www.riksbank.se/pki (current version)
Certification Practice Statement	Sveriges Riksbank intranet (all versions) http://www.riksbank.se/pki (current version)
Certificate Revocation Lists	http://www.riksbank.se/pki/crl
Root CA certificate	http://www.riksbank.se/pki/crl
Issuing CAs certificates	http://www.riksbank.se/pki/crl

2.3 Time and frequency of publication

Published documentary information is updated after every amendment, within 24 hours of validation.

Root CA CRL
Issued CRL from root CA is published at least once every 50 weeks but normally biannual as part of routine operations.
High Assurance CRL
Not defined.
Medium Assurance CRL
Issued CRL from medium assurance CA is published every 48 hours or as part of revocation of a certificate.
Basic Assurance CRL
Issued CRL from basic assurance CA is published every 21 days or as part of revocation of a certificate.

New versions of CP and CPS are published within 5 days after approval.

2.4 Access controls on published information

Published documentary information, including policies, public keys and revocation lists, is available on a read-only basis for subscribers, relying parties and other participants. Only explicit, assigned personnel are authorized to update published documentary information. The distribution point is protected by strict access control.

The CPS details the procedures for assigning and managing these authorizations.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of name

The certificates issued by RB-PKI contain the common name of the subscriber (user, system or function). The naming of issued certificates shall follow the default of the X.509.v3 standard and shall, wherever possible, be compatible with RFC3280[2]:

- If the certificate is issued to a user, the person's name will be included in the CN field of the certificate.
- If the certificate is issued to a system, the DNS FQDN or the service invocation name of the system will be included in the certificate CN field.
- If the certificate is issued to a function, the name of the function will be included in the CN field of the certificate.

3.1.2 Need for names to be meaningful

The CNs of the issued certificate must be meaningful and are subject to the rules established in paragraph 3.1.1 of this certificate policy.

3.1.3 Anonymity or Pseudonymity of Subscribers

For certificates issued to users, anonymity is not allowed. Pseudonomity could be considered in special cases if deemed necessary.

3.1.4 Rules for interpreting various name formats

Sveriges Riksbank applies the following rules regarding the naming format of UPN[3] and mail address;

- All characters are defined by the English alphabet and no Swedish special characters are used in the naming format.
- The Swedish character Å is replaced by A
- The Swedish character Ä is replaced by A

[2] IETF Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[3] Universal Principle Name

- The Swedish character Ö is replaced by O

The naming convention rules are defined within the Active Directory and in the RA function.

3.1.5 Uniqueness of names

The Riksbank Directory Service ensures that all certificate owners have a unique email address in the system. The RB-PKI system for the generation of unique certificate serial numbers shall be designed in such a way that the same identification number cannot be generated twice in the system's entire lifetime.

- Naming of user certificates follows the same procedures used for the naming in the Riksbank directory service.
- Naming of system certificates follows the Riksbank default naming convention.
- Naming of function certificates follows the Riksbank standards for the naming of business functions.

3.1.6 Recognition, authentication, and the role of trademarks

No stipulation.

3.2 Initial Identity Validation

A certificate creates a trust between the holder of a certificate and the public key in the issued certificate. The initial identity validation of the certificate holder provides the basis for the trust that is established between Sveriges Riksbank and the certificate holder.
This section describes how this information is collected and validated.

3.2.1 Means of proof of possession of the private key

For Medium assurance certificates, the private key is either generated by the CA or by the hardware token at the time of certificate issuance and thus there is no need for proof of possession.

For Basic assurance certificates, the private key is normally generated by the CA and thus there is no need for proof of possession.

If the private key is generated by the applicant, the certificate request must be signed with the private key as a proof of possession.

3.2.2 Authentication of Organization Identity

Certificates are issued only to holders that are associated with organizations that work with Sveriges Riksbank. Within Sveriges Riksbank, each business unit is responsible for the relationship between Sveriges Riksbank and these specified organizations.

3.2.3 Authentication of Individual Identity

Evidence of the subject's identity or requestor is checked against a physical person.

Identification and verification of the identity of the requester is done by the requester providing a passport or national identity card, or any other legal document accepted by the applicable national legislation to duly identify an individual.

For medium assurance certificates, the initial identification and verification is done when the card for physical access to the Riksbank premises is issued. This card is a dual-purpose card with a photo-id and the certificate will be issued only to an individual with such a valid card. All information concerning the individual identity will be stored in a central repository, the Riksbank Active Directory.

When external organizations as defined in 3.2.2 request a certificate, the identification and verification of the identity of the organization shall be carried out by the responsible business unit as part of the initial certificate request.

3.2.4 Non-Verified Subscriber Information

All certificate requesters will be validated.

3.2.5 Validation of Authority

No stipulation, given that the issue of certificates for entities is not considered.

3.2.6 Criteria for Interoperation

Sveriges Riksbank will examine contract inquiries and investigate the agreement and cooperation with external certificate issuers and submit them for approval by Sveriges Riksbank PKI system owner.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for routine Re-Key Requests

The authentication procedures for a re-key request are the same as for an initial certificate application, the provisions of section 3.2 apply.

3.3.2 Identification and Authentication for Re-Key After Revocation

Identity checks in connection with key updates after revocation shall be carried out following the same procedures as when applying for a new certificate.

3.4 Identification and Authentication for Revocation Requests

A request to revoke a CA certificate should always be addressed to the PKI System Owner. Requests for revocation shall include:

- The name of the CA that the revocation request is for
- A clear description of why revocation is requested

- Identity of the person requesting revocation

3.4.1 Revocation Request of the Root CA

If revocation of the Riksbank Root CA is requested, the incident management organization at the Riksbank shall be activated in accordance with its procedure.

3.4.2 Revocation Request for a subordinate CA

If revocation of a subordinate CA is requested, the incident management organization at the Riksbank shall be activated in accordance with its procedure.

3.4.3 Revocation Request of personal certificates

If revocation of a user certificate is requested, the revocation request must be approved by the certificate holder or it will be handled by the Riksbank incident management process.

3.4.4 Revocation request of system and function certificates

If revocation of a function or system certificate is requested, the revocation request must be approved by the certificate owner or a Riksbank security officer.

3.4.5 The decision on revocation

Decisions on revocation will be documented in writing. The written decision shall contain:

- Name and/or serial number of the certificate to be revoked
- Decision on revocation
- Grounds for revocation
- Signature of the certificate holder or it will be handled by the Riksbank incident management process.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

The generic principle is that subjects who are authorized to apply for a user, system or functional account, also is authorized to submit a certificate application for the account.

Medium assurance certificates

Application for medium assurance user certificates for employees at Sveriges riksbank is done automatically as part of the registration process in the HR system. This includes certificates for authentication, encryption and digital signatures. The line manager of the employee can later submit an application for Non-repudiation certificates as needed.

Application for medium assurance user certificates for external users, i.e. consultants, is done by the line manager who is responsible for the agreement with the external user. This is normally done through an automated process which also includes a user account and authorization to the Riksbank premises.

Basic assurance certificates

Application for basic assurance user certificates for employees is done by the line manager of the employee or, if the user is authorized to, by the user himself.

Application for basic assurance user certificates for external users, i.e. customers, is done by the business unit who is responsible for the customer agreement.

Application for functional certificates, i.e. shared mailbox, is done by the owner of the function.

Application for system certificates, i.e. web server certificate, is done by the system owner or anyone the system owner has delegated this task to.

Computers with an account in the Riksbank directory could autoenroll for system certificates.

4.1.2 Enrollment Process and Responsibilities

User certificates

Certificate requests for user certificates are made by the line manager as part of the user registration process. The certificate request is processed by the Riksbank Registration Officer after validation.

System certificates

Certificate requests for system certificates are made by the system owner or appointed delegate. The certificate request is processed by the Riksbank Registration Officer or equivalent after validation. On delivery of the certificate, an application signed by the system owner or appointed delegate needs to be supplied.

Computer objects in the Riksbank Active Directory could autoenroll for system certificates.

Function certificates

Certificate requests for functional certificates are made by the owner of the applicable object, i.e. the shared mailbox or organisational unit. The certificate request is processed by the Riksbank Registration Officer or equivalent after validation. On delivery of the certificate, an application signed by the system owner or appointed delegate needs to be supplied.

4.2 Certificate Application Processing

4.2.1 Performance of identification and authentication procedures

The validation of all certificate requests (except auto enrolled machine certificates) will require face-to-face authentication of the subscriber or using means which provide equivalent assurance to physical presence.

The Riksbank Registration Officer will perform the identification and authentication of the subscriber and will guarantee that all the information provided was correct at the time of registration. The identification and authentication process will be carried out as specified in section 3.2.3 of this CP.

For the issuance of Basic assurance certificates, online authentication with a valid Medium assurance user certificate is also acceptable, provided that the applicant is privileged to apply for the certificate in question.

4.2.2 Approval or rejection of certificate applications

Certificates will be issued once the Riksbank Registration Officer has completed the verifications necessary to validate the certificate application.

The Riksbank Registration Officer may refuse to issue a certificate to any applicant based exclusively on its own criteria and without leading to any liability whatsoever for any consequences that may arise from said refusal.

4.2.3 Time limit for processing the certificate applications

Each certificate request is processed within 5 working days.

Autoenrolled certificates are processed immediately.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

When the CA receives a certificate request, the signature of the RA is always validated before the certificate is issued.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

User certificates

All Medium assurance user certificates will be created while applicants are present at the Registration Officer office The certificate(s) will only be issued after the applicant has signed an agreement including terms and conditions for the use of the private and public keys. This agreement will be registered with the CA for as long as the certificate is valid, including renewed and/or recovered ones.

Applicants for Basic assurance user certificates will be advised of the availability of the certificates via e-mail by the Registration Officer.

■ *System certificates*

Applicants for a system certificate will be advised of the availability of the certificates via e-mail by the Registration Officer.

For auto enrolled machine certificates no notification will be sent out.

Function certificates

Applicants for a function certificate will be advised of the availability of the certificates via e-mail by the Registration Officer.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Use of the certificate private key is considered as a recognition and acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

User and function certificates are published in the Riksbank internal LDAP directory and on the Riksbank global address list for mail.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers may only use the private keys and the certificates for the uses authorized in this CP and in accordance with the 'Key Usage' and 'Extended Key Usage' fields of the certificate. Likewise, subscribers may only use the key pair and the certificates once they have accepted the terms and conditions of use established in the CPS and CP, and only for that which is stipulated therein.

If the terms and conditions are changed, these changes must be communicated to the subscriber and agreed.

Following certificate end-of-life or revocation, subscribers must discontinue use of their private keys.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties may only rely on the certificates as stipulated in this CP and in accordance with the 'Key Usage' field of the certificate.

Relying parties should perform public key operations as a condition for relying on a certificate and are advised to check the status of a certificate using the mechanisms established in the CPS and this CP. Likewise, they accept the obligations regarding the conditions of use set forth in these documents.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

Root CA and Issuing CA:s

When a certificate expires, an assessment must be done to clarify whether there is a need for re-keying or if the certificates can be renewed with the existing key-pair. The determining factor is the development on encryption technology and the possibilities to mathematically derive the private keys from the certificates.

All issued certificates

When a certificate expires, only encryption certificates will be renewed with the existing key-pair. All other certificates will be renewed with a new key-pair, see section 4.7

4.6.2 Who May Request Renewal

The renewal process for Medium assurance certificates will be initiated by the Subscriber via a formal application for renewal.

Renewal of a Basic assurance certificate can be requested by the subscriber or the Registration officer.

4.6.3 Processing Certificate Renewal Requests

Medium Assurance Certificates

The processing of certificate renewal requests is conducted in accordance with the provisions of section 4.3. The provisions of section 3.3.1 govern the procedures for identification and authentication for certificate renewal.

Basic Assurance Certificates

User encryption certificates could be renewed by the RA in two ways:

- Automatically before the certificate expires and delivered to the user account in the Riksbank directory service.
- On request by the subscriber, given that the subscriber is authenticated with, or the request is signed with, a valid Medium Assurance certificate

All other certificate types will be renewed with a new key-pair (re-key)

4.6.4 Notification of New Certificate Issuance to Subscriber

The provisions of section 4.3.2 apply.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The provisions of section 4.4.1 apply.

4.6.6 Publication of the Renewal Certificate by the CA

The provisions of section 4.4.2 apply.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 Certificate Re-key

4.7.1 Circumstances for Certificate Re-Key

Root CA and Issuing CA:s

Depending on the development on encryption technology and the possibilities to mathematically derive the private keys from the certificates, an assessment must be done to clarify whether there is a need for re-keying or if the certificates can be renewed with the existing key-pair.

If a CA certificate is revoked, a new certificate based on a new key-pair must be issued.

All issued certificates

When a certificate expires, a new certificate based on a new key-pair will be issued. The exception is user certificates used for encryption where the certificate will be renewed with the existing key-pair.

When a certificate is revoked, a new certificate based on a new key-pair must be issued.

4.7.2 Who May Request Certification of a New Public Key

The provisions of section 4.6.2 apply.

4.7.3 Processing Certificate Re-Keying Requests

The provisions of section 4.6.3 apply.

4.7.4 Notification of New Certificate Issuance to Subscriber

The provisions of section 4.3.2 apply.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

The provisions of section 4.4.1 apply.

4.7.6 Publication of the Re-Keyed Certificate by the CA

The provisions of section 4.4.2 apply.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

Certificates must not be modified. In case of changes, the old certificate must be revoked and a new certificate must be requested.

4.8.1 Circumstances for certificate modification

No stipulation.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

A certificate shall be revoked:

- If there is a suspicion that the private key has been compromised.
- In case of loss of private keys on the key-bearing equipment.
- If the certificate holder requests that their certificate should be revoked.

The certificate issuer has the right to revoke certificates without informing the certificate subscriber:

- If the certificate holder neglects his obligations as described in this document and this involves a fundamental breach of contract.

- In case of the certificate holders death.
- When the certificate issuer is unable to contact the certificate holder within a reasonable timeframe.

Once the certificate is revoked, it must not be reinstated.

4.9.2 Who Can Request Revocation

Anyone who has reason to do so according to section 4.9.1 may request the revocation of a certificate.

4.9.3 Procedure for Revocation Request

The certificate issuer shall ensure that procedures and requirements for the revocation of certificates are documented in the Certification Practice Statement (CPS). All revocation requests and all implemented measures for revocation request must be documented along with the reason for revocation. The Riksbank Registration officer performs the requested revocation after approval according to section 3.4.

4.9.4 Revocation Request Grace Period

The revocation request must be done as soon as, and no longer than 24 hours after, the certificate holder or any other PKI participant is made aware of any of the circumstances listed in 4.9.1.

4.9.5 Time Within Which CA Must Process the Revocation Request

Revocation of Medium assurance certificates

The revocation service is operational 24 hours a day, 365 days a year. Information about revocation shall be published in the certificate revocation list as soon as possible; the certificate revocation list shall be published no later than one (1) hour after the revocation request.

Sveriges Riksbank revokes the certificate as soon as it has approved the revocation request.

Revocation of Basic assurance certificates

The revocation service shall, if possible, be operational 24 hours a day, 365 days a year. Information about revocation shall be published in the revocation list as soon as possible; the certificate revocation list shall be published no later than 24 hours after the revocation request.

Sveriges Riksbank revokes the certificate as soon as it has approved the revocation request.

4.9.6 Revocation Checking Requirement for Relying Parties

The provisions of section 4.5.2 apply.

4.9.7 CRL Issuance Frequency

For Medium assurance CA

The revocation list must be updated if a revocation is performed, 24 hours a day, 365 days a year. A new CRL will be issued at least every 48 hours even if no new information has emerged since the last release.

Revocation status information shall include information on the status of certificate until the certificate expires

For Basic assurance CA

The revocation list must be updated if a revocation is performed, 24 hours a day, 365 days a year. A new certificate revocation list will be issued at least every 21 days even if no new information has emerged since the last release.

Revocation status information shall include information on the status of certificate at least until the certificate expires

4.9.8 Maximum Latency for CRLs

CRLs and ARLs are published no later than 1 hour after they are generated.

4.9.9 On-Line Revocation/Status Checking Availability

If the Riksbank publishes online CRL checks via the OCSP protocol, the access point will be available 24 hours a day, 365 days per year. The access point will be published in the issued certificate.

4.9.10 On-Line Revocation Checking Requirements

The provisions of section 4.5.2 apply.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements re-Key Compromise

Should a private key become compromised, the certificate so affected shall immediately be revoked. Should the private key of a Riksbank CA become compromised, all certificates issued by the Riksbank CA shall be revoked.

4.9.13 Circumstances for Suspension

Suspension of certificates are not allowed in Sveriges riksbank PKI.

4.9.14 Who Can Request Suspension

Suspension of certificates are not allowed in Sveriges riksbank PKI.

4.9.15 Procedure for Suspension Request

Suspension of certificates are not allowed in Sveriges riksbank PKI.

4.9.16 Limits on Suspension Period

Suspension of certificates are not allowed in Sveriges riksbank PKI.

4.10 Certificate Status Services

The provisions of section 4.9.9 apply.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

No stipulation.

4.10.3 Operational Features

No stipulation.

4.11 End of Subscription

If relations between the holder and the CA are terminated before the validity period of the certificate expires, the Registration Officer will revoke the holder's certificate if so deemed necessary.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The key recovery service for Riksbank PKI encryption certificates (and the associated private key) will be available only for encryption certificates. For these certificates, the Certification Authority will send a copy of any user encryption key pair to the key archive, so as to allow key recovery in case of cryptographic token loss or replacement.

Routines for key escrow and recovery are described in the CPS

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 Facility, management and operational controls

5.1 Physical Controls

5.1.1 Site location and construction

The Riksbank CA systems must be placed in one of the Riksbank-approved data centres. The facility housing the CA system key elements must be located in a heavily-protected area. The data centre shall be locked and alarmed. The jurisdiction of the computer room shall be restricted so that only persons authorized to administer the system placed in the data centre and guarded personnel have jurisdiction in the data centre. Permissions for access must be checked at least once a year by the RB-PKI system owner.

5.1.2 Physical Access

The Riksbank Issuing CA-systems components in the data centres that are directly connected to the dedicated network segment shall be placed in individual access-protected cabinets or enclosures. Cabinets or enclosures shall be individually secured with alarms to prevent unannounced access to the certificate system. Access to the Riksbank PKI system shall be controlled, using "4 eye" principal among authorized CA personnel.

An access log of physical access to the CA system and its components shall be kept. The system owner shall be responsible for drawing up a list of authorized personnel.

Physical access to the root-CA that is never connected to the network or normally placed in the computer room must be in accordance with specially-arranged and documented procedures.

5.1.3 Power and air conditioning

The power supply shall be arranged so that the Riksbank PKI systems, with its surrounding systems, shall function in normal operation in accordance with the requirements that are set for availability. Ventilation and climate control shall be designed so that the recommended climate values from the supplier are followed and so that availability is not affected.

5.1.4 Water exposures

The Riksbank PKI systems shall be fully protected from exposure to liquid. Water pipes of a type other than those intended for climate control or fire protection shall not be present in the data centre.

5.1.5 Fire Prevention and Protection

The Data centre must be equipped with functions for automatic extinguishing systems and sensors for smoke and fire. Doors and walls shall be designed for a minimum fire rating of EI60.

5.1.6 Media Storage

Media containing software and documentation of the Riksbank PKI systems must be kept in two copies in two geographically-separate, fire-protected areas separated from the data centre.

5.1.7 Waste Disposal

Computer media used for the storage of information such as encryption keys, activation data or files from the CA system must be destroyed according to the Riksbank guidelines for protection of information.

5.1.8 Off-Site Backup

Reserve facilities must maintain a physical security equivalent to that of the ordinary plant.

5.2 Procedural Controls

5.2.1 Trusted Roles

The Riksbank guidelines and rules for information protection require that there must be an ownership and management structure for each information system. The following roles shall be mandatory for the certificate system:

Description	Liability
System owner	The System owner officially owns the Riksbank PKI systems and is ultimately responsible for its operation, safety, efficiency and relation to other systems and activities.
System manager	The system manager is appointed by the system owner to delegate tasks and implement changes according to the system owner. The system manager is responsible for developing and continuously monitoring the effectiveness of procedures, methods and channels of information for the management of the CA system. The system manager is also responsible for investigate and plan, and also assess impacts, costs and consequences of actions taken within and outside the system for change and development.
CA operator	The system operator appointed by the system owner and system manager who delegates tasks to him for decision. The system operator shall, on behalf of the system administrator, compile information, investigate and plan, and also assess impacts, costs and consequences of actions taken within and outside the system for change and development.
Operator	The operator appointed by the system owner and system manager to implement changes according to the system owner and system manager. The operator is responsible for ensuring that all the detailed operational arrangements for the CA system are performed to the system-owner agreed level.

Description	Liability
CA Auditor	The auditor is appointed by the systems owner and is responsible for: (a) Reviewing, maintaining, and archiving audit logs; and (b) Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CP and CPS.
Registration Officer	The Registration Officer is appointed by the system owner and is responsible for all certificate management procedures and operations .
Security Officer	The role Security Officer is handled by the person in Sveriges riksbank that have the "IT security Officer". This role is appointed by the head of IT at Sveriges riksbank.

5.2.2 Number of Persons Required per Task

Two CA operators are required per task, for the work on the basic and medium CA, in the Riksbank PKI systems for the following tasks:

- Riksbank CA private key generation
- Riksbank CA private key activation
- Riksbank CA Private Key Backup

All individuals must serve in a trusted role as defined in Section 5.2.1.

For accessing and operating the Riksbank PKI root CA the following minimum roles need to be present; The Riksbank PKI system manager and the Riksbank PKI system CA auditor.

5.2.3 Identification and Authentication for Each Role

Physical access to the Riksbank PKI systems requires at least two persons. All work carried out on the Riksbank PKI systems must be performed by each trusted role. Each trusted role shall have jurisdiction and access to those parts of the system according to his specified role and tasks. The Riksbank PKI systems roles are documented with a description of duties, responsibilities and authority, se section 5.2.1.

5.2.4 Roles Requiring Separation of Duties

The Riksbank approved personnel and individuals may only occupy one trusted Riksbank PKI system role to ensure separation of duties.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Security clearance and controls are carried out with respect to suitability for different tasks for the staff with a trusted role within the Riksbank PKI systems. Checks must be carried out in accordance with the Riksbank guidelines for personnel protection and rules for safe employment. Staff with a trusted role in the Riksbank PKI systems must possess well-documented skills in accordance with each role assigned.

5.3.2 Background Check Procedures

A security clearance shall be performed for those who hold roles with access to the Riksbank PKI system.

5.3.3 Training Requirements

The holders of all defined PKI system trusted roles according to paragraph 5.2.1 must have relevant and comprehensive training for the task.

5.3.4 Retraining Frequency and Requirements

All staff in trusted roles should be offered relevant training on updates and changes to the Riksbank PKI system, or at set intervals defined on the three-year cycles.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The system owner shall immediately replace staff when misconduct is suspected. When needed, disciplinary actions could be carried out according to Riksbank standard procedures.

5.3.7 Independent Contractor Requirements

All of the requirements of section 5.3 - 5.3.5 shall also apply to contracted staff. Penalties for unauthorized acts by contracted staff shall be determined in a separate agreement with the contractor.

5.3.8 Documentation Supplied to Personnel

The Riksbank has established the following records for their staff:

- Riksbank Certificate Policy
- Riksbank Certification Practice Statements.
- Operational documentation
- Process documentation
- Installation documentation
- Routine descriptions

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Logging shall be performed to such an extent and level of execution that it has a protective effect against unauthorized activities and to create confidence in the Riksbank PKI systems.

- The following events will be logged in the Riksbank PKI systems and related underlying systems, such as underlying operating systems, protective systems and communications equipment;

  - events that can cause an adverse impact on the CA systems, and reliability and security derived in confidentiality, integrity, availability and traceability
  - events that are of a security logging character
  - events that may cause a direct and negative impact on the logical access protection of the system
  - events that occur when physically accessing the CA systems and accessing repositories for logs and keys
  - events that affect the availability and interruption of the PKI systems.
  - events that measures uptime, e.g. start and stop
  - events related to the certificate management, account generation, retirement of accounts, the revocation of certificates and the issuance of the revocation list (CRL)
  - Change management events

All Riksbank PKI systems and subcomponents shall be protected with functions for alarm / incident response to infringements for the logical access protection.

5.4.2 Frequency of Processing Log

Logs should be checked and analysed with such frequency that it is possible to ensure that trust in the Riksbank PKI systems' reliability and safety is not compromised. The frequency of log checking should also detect unauthorized access immediately. The system shall include functions for scanning and automatic control in real time, and for the correlation and escalation of events.

In addition to this, a full inspection and analysis shall be carried out at least once (1) per week to detect any irregular activities. An analysis of this involves checking that the log is accurate and carrying out a concise review of all logged events and a detailed investigation of suspected improper events.

Serious events that require immediate action shall be reported and handled in accordance with the Riksbank regulations. Other events in the form of irregularities will be compiled and explained in a report communicated to the system owner as soon as possible. A compilation of all the events that caused the suspicion or resulted in irregularities shall be notified to the system owner for the Riksbank PKI system on a quarterly basis.

5.4.3 Retention Period for Audit Log

Logs described under section 5.4.1 shall be maintained in the PKI system for at least six (6) months and then archived according to Section 5.5.

5.4.4 Protection of Audit Log

Access to the audit logs are restricted in such a way that no personal holding a PKI role (except the CA auditor role) can manipulate information within the logs. Two copies of the log must be stored in physically-secured areas, in physically-separate locations. The logs must be stored in such a way that, when irregularities are suspected, the logs can be accessed and made readable for review during the specified retention period.

5.4.5 Audit Collection System (Internal vs. External)

Automatically-generated logs from the Riksbank PKI system according to 5.4.1 shall be written to separate logging systems outside the Riksbank PKI system in a safe and reliable manner in accordance with Section 5.4.4.

5.4.6 Notification to Event-Causing Subject

Certificate subscribers and relying parties will be informed in the contracts about the logging of events in the Riksbank PKI system, and about the purpose of this logging. No notification is made individually to the certificate subscriber that caused the event.

5.4.7 Vulnerability Assessments

No stipulation.

5.5 Records Archival

The Registration Authority and the CAs archive data in an effort to ensure service continuity, auditability and non-repudiation of transactions.

The Registration Authority and the CAs take the necessary measures to ensure that these archives are available, reusable, integrity-protected, and subject to strict operational and destruction-protection rules.

5.5.1 Types of Records Archived

The following types of information shall be archived:

- Certificate applications
- Agreement with the certificate subscribers
- Agreements with relying parties
- Documentation regarding the revocation of certificates
- Governing documents regarding the Riksbank PKI system
- Documentation relating to staff in administrative roles of the certificate system, security, personnel changes, etc.
- Record of completed audits (audits)
- Logs in accordance with 5.4.1

5.5.2 Retention Period for Archive

Information in accordance with 5.5.1 shall be retained for at least five (5) years.

5.5.3 Protection of Archive

Archived information shall be protected from unauthorized access, modification or deletion. The archive itself is only physically and logically accessible to authorized personnel. Archived information should be stored in such an environment and on such media that the readability requirement is met throughout the estimated time period for the storage.

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time-Stamping of Records

No stipulation.

5.5.6 Archive Collection System (Internal or External)

The Riksbank archiving system is internal.

5.5.7 Procedures to Obtain and Verify Archive Information

Archived information shall be stored in such way that in case of serious suspicion of irregularities it can be produced and made readable for review during the specified retention period. Archived information must be verified for readability and accuracy at least every 24 months by performing sampling for readability and accuracy. The extent of sampling should be such that the readability and accuracy can be assumed to be good in all stored information.

5.6 Key Changeover

The Riksbank CA cannot generate a certificate whose end date comes after the expiry date of the corresponding CA certificate. The validity period of the CA certificate must therefore extend beyond that of the certificates that it signs.

The Riksbank CPS details the applicable procedures in the event of a CA key changeover.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The system owner shall ensure that the plans, emergency procedures, procedures and practices are such that the objectives of the Riksbank business continuity requirements are met by maintaining the reliability level of the Riksbank PKI system.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

The Riksbank PKI issuing CA platform is mirrored in a remote site that reflects its primary facility, so that if any software or data is damaged, it can be restored from backup. In the event of disaster, the work to restore the system for business will start as quickly as possible, with the provision that the recovery of the system revocation function shall take precedence over all other activities.

Following a disaster the CA shall, where practical, take steps to avoid repetition of a disaster.

5.7.3 Entity Private Key Compromise Procedures

The system owner for the CA system shall ensure that there is a written plan for what steps the organization, certificate subscribers and relying parties will take in the event of a compromise.

The Certificate Authority shall take the following steps if it is suspected that the issuing keys are compromised:

- Revoke all CA certificates related to the compromised CA.
- Invoke the incident manager procedures and convene an incident management organization consisting of at least the system owner of the certificate system.
- Inform all certificate subscribers and relying parties with which the Riksbank has contractual or other established relationships.

The issuer shall ensure that the revocation information is available for the CA certificates until the revoked certificates expire.

In the event that the parent CA key (Root CA) is compromised, the issuer shall immediately discontinue service to revocation checking. This means that certificates are not accepted by the relying party responsible for supervising the blacklist.

5.7.4 Business Continuity Capabilities After a Disaster

See Chapter 5.7.2

5.8 CA or RA Termination

One or more PKI components may terminate operations or be transferred to another entity.

Termination of operations shall be defined as the end of operations of a PKI component with an impact on the validity of certificates issued prior to the cessation in question.

Transfer of activities shall be defined as the end of operations of a PKI component with no impact on the validity of certificates issued prior to the transfer and the resumption of operations organised by the CA in conjunction with the new entity.

A decision to terminate may only be taken by the issuer in the form of the system owner of the certificate system, provided that all the departments of the Riksbank have been informed at least three months before the decision is taken.

When the decision is made to terminate a CA, the following steps must be taken;

- The decision on cessation must be recorded
- All certificate subscribers and relying parties shall be informed of the decision

- Plans and procedures must be developed to ensure that encrypted data can be restored and that all signatures can be verified at least five (5) years after termination of service
- All procedures and actions performed for the CA cessation shall be documented and archived
- Archived information under paragraph 5.5 shall be made available under these conditions during the time period specified in paragraph 5.5
- All private keys must be destroyed.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Root CA

The key pair for the Root CA is generated inside the HSM pursuant to the CC EAL4+ specification and FIPS 140-2 level 3.

Issuing CA:s

The key pair for an Issuing CA is generated inside a HSM pursuant to the CC EAL4+ specification and FIPS 140-2 level 3.

Medium assurance certificates:

- Certificates with key escrow. The key pair will be generated by the Riksbank Issuing CA, using a cryptographic module pursuant to the FIPS 140-2 level 3 specifications.
- Certificates without key escrow. The key pair will be generated inside the cryptographic token pursuant to the CC EAL4+ specification or equivalent.

Basic assurance certificates:

- All Basic assurance certificates, where the private key will be generated by the Riksbank PKI Online CA, will be using a cryptographic module pursuant to the FIPS 140-2 level 3 specifications.
- If the key pair is generated outside the issuing CA, the requestor is responsible for the integrity and confidentiality of the private key.

6.1.2 Private Key Delivery to Subscriber

If subscribers for system certificates or the individual sponsors of such systems, generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

■ *Medium assurance certificates:*

- Certificates with key escrow. The private key will be delivered in a manner that guarantees integrity and confidentiality.
- Certificates without key escrow. The private key will be generated in the certificate subscriber's hardware module so there will be no need for delivery.

Basic assurance certificates:

A certificate subscriber's private encryption / signing key will be delivered in a manner that guarantees integrity and confidentiality.

6.1.3 Public Key Delivery to Certificate Issuer

Subscriber public keys are delivered to the CA for signing purposes in a manner that guarantees integrity, confidentiality and origin.

6.1.4 CA Public Key Delivery to Relying Parties

The Riksbank root CA and Issuing CA public keys is available at https://www.riksbank.se/pki. The website is TLS protected with a public certificate from a trusted issuer, Sectigo, formerly ComodoCA.

6.1.5 Key Sizes

The Root CA uses a 4096 bit RSA key.

Subordinate CAs use a 2048 bit RSA key.

Medium assurance certificates use an RSA key with a length equal to or greater than 2048 bits.

Basic assurance certificates use an RSA key with a length equal to or greater than 1024 bits.

These data will be revised to reflect changes in technology and/or legislation.

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The use of a CA private key and associated certificate is restricted to signing certificates and CRLs/ARLs, all other use is strictly forbidden The CA private key must only be used within the physically secure premises.

The use of holder private keys is restricted to the service described in this CP.

For issued certificates, the Key Usage Field must follow the restrictions defined in the following table:

	Authentication	Encryption	Digital signature

Medium assurance certificates	digitalSignature: 1 nonRepudiation: 0 keyCertSign: 0 cRLSign: 0	keyEncipherment: 1 nonRepudiation: 0 keyCertSign: 0 cRLSign: 0	nonRepudiation: 1 all other keyUsage: 0
Basic assurance certificates	digitalSignature: 1 nonRepudiation: 0 keyCertSign: 0 cRLSign: 0	keyEncipherment: 1 nonRepudiation: 0 keyCertSign: 0 cRLSign: 0	digitalSignature: 1 nonRepudiation: 0 keyCertSign: 0 cRLSign: 0

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Root and issuing CAs:

Riksbank CA keys will be protected by a security module certified to the CC EAL4+ specification and FIPS 140-2 level 3.

Medium assurance certificates:

Subscribers' private keys will be protected in a hardware module/token certified to the CC EAL4+ specification and FIPS 140-2 Level 2.

Basic assurance certificates:

No requirement for a hardware security module.

6.2.2 Private Key (n out of m) Multi-Person Control

Access to the Riksbank PKI system CA private keys in the security module requires two different trusted roles of two physically-distinct persons.

6.2.3 Private Key Escrow

Only private encryption keys issued to a user by a medium assurance CA can be escrowed.

Private keys will not be escrowed outside the CA.

6.2.4 Private Key Backup

Root CA certificate

Root CA private keys will be protected in a hardware module/token certified to FIPS 140-2 Level 3 and are backed up according to a defined PKI operating procedure.

The private keys are backed up with strong encryption and stored on two physically separated sites. Two different operators need to be present in the protected area with their respective admin smart card to restore the private keys.

■ *Issuing CA certificates*

Issuing CA private keys will be protected in a hardware module/token certified to the CC EAL4+ specification and FIPS 140-2 Level 3 and are backed up according to the normal Riksbank PKI issuing backup routine.

The private keys are backed up with strong encryption and stored on two physically separated sites still within the protected areas. Two different operators need to be present in the protected area with their respective admin smart card to restore the private keys.

Medium assurance certificates

When key escrow service is requested, the encryption private keys are subject to key backup as described in section 4.12.1 Key archive and recovery practices and policies.

For encryption certificates, a backup copy of the private key will be kept in the CA for as long as the Riksbank PKI is operational.

The private key backup could only be used in the following four scenarios:

- The certificate holder needs a temporary certificate, i.e. when a smart card is left at home
- The certificate holder needs a replacement smart card in case the original smart card is lost or damaged
- The certificate holder needs a copy of the certificate for the use in another device
- The certificate holder is not present due to discharge, illness or death.

The private key backup must only be recovered on the same key bearing equipment as the original key, i.e. smart card.

Recovery of a private key from backup is subject to a 4-eyes-principle where two different individuals are responsible for key retrieval and recovery respectively.

Basic assurance certificates

Normally, no backup of basic assurance certificates private keys are performed. The subscribers of certificates will have to keep the PKCS#12 file and corresponding protection password as a backup copy.

In case of a need for key backup services for basic assurance certificates, the same procedures as for medium assurance certificates should apply.

6.2.5 Private Key Archival

Medium assurance certificates

For encryption certificates, an archive copy of the private key will be kept in the CA for as long as the PKI is in use.

- When key archive service is requested by the Riksbank, the encryption private keys are subject to key archive as described in section 4.12.1 Key archive and recovery practices and policies.

Basic assurance certificates

Normally, the Riksbank PKI system will not keep any archive of the private key associated to basic assurance certificates.

In case of a need for key archive services for basic assurance certificates, the same procedures as for medium assurance certificates should apply.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The transfer of a private key into or from a cryptographic module is subject to a secret-sharing scheme.

The transfer procedures used ensure the confidentiality and integrity of the private key. Details are provided in the CPS.

6.2.7 Private Key Storage on Cryptographic Module

Medium assurance certificates

Private keys of authentication, signature and encryption certificates without key escrow are created on the cryptographic token and stored there. Private keys of encryption certificates with key escrow are generated by the CA's cryptographic module and afterwards stored in the CA's database and in cryptographic token.

Basic assurance certificates

No stipulation

6.2.8 Method of Activating Private Key

Root CA certificate

Activation of Root CA private keys in cryptographic modules is controlled via activation data. Activation requires two different trusted roles of two physically-distinct persons holding each a personal activation card that's needed to activate the CA private key.

Issuing CA certificates

Activation of Issuing CA private keys in cryptographic modules is controlled via activation data. Activation requires two different trusted roles of two physically-distinct persons holding each a personal activation card that's needed to activate the CA private key.

Medium assurance certificates

Private keys are stored in a cryptographic token protected with a PIN code that is required to activate the keys.

Basic assurance certificates

Private keys are delivered in a PKCS#12 file, protected by a password. The password is required to activate the private key.

6.2.9 Method of Deactivating Private Key

CA private key

CA private keys in a cryptographic module are automatically deactivated if the module environment changes, e.g. the module is stopped or disconnected or the operator is disconnected.

Medium assurance certificates

Private keys can be deactivated by removing the card from the reader. Some computer applications also provide deactivation following a time-out period.

Basic assurance certificates

No stipulation.

6.2.10 Method of Destroying Private Key

CA private key

CA private keys in a cryptographic module can be destroyed by resetting the HSM module.

Medium assurance certificates

Private keys can be destroyed by physically destroying the smartcard and by deleting the key in the CA database.

Basic assurance certificates

The certificate holder is responsible for destroying the private key. The private key can be destroyed by deleting the certificate with the corresponding private key from the key stores in question and deleting all copies of the PKCS#12-file.

6.2.11 Cryptographic Module Rating

The cryptographic modules used by the RB-PKI Authorities comply with the FIPS 140-2 Level 3 standard.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archive

Public keys are archived as part of the archival process for the corresponding certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

All certificates and their linked key pairs have a maximum lifetime as specified in the table below, although the Online CA may establish a shorter period at the time of their issue.

Issuer and certificates	Certificate lifespan
Root CA certificate	240 months
Issuing CA certificates	120 months
Issued certificates	36 months
Temporary certificates	7 days

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Root CA private key

A passphrase or PIN, in addition to the token, is required to operate cryptographic modules that comply with FIPS 140 level 3.

The passphrase is random generated and consist of a minimum of 12 characters. The different operator cards have different passphrases.

Issuing CA private key

If activation data is used (see section 6.2.8), the passphrase is random generated and consist of a minimum of 8 characters.

Medium assurance certificates

Activation data shall have an appropriate level of strength for the key pair or data to be protected, and shall be transmitted to the certificate holder in a method and manner that is different from that used to transmit the cryptographic module.

The PIN will be generated in such a way that only the certificate holder has knowledge of it. The PIN validation process only accepts maximum three incorrect attempts before locking the device.

- The PIN can be changed by the certificate holder. The PUK will only be handled by the RA system using special procedures and never be viewed in plain text.

Basic assurance certificates

Activation data shall have an appropriate level of strength for the key pair or data to be protected, and shall be transmitted to the certificate holder in a method and manner that is different from that used to transmit the cryptographic module.

The Basic assurance certificate PKCS#12 file is delivered in a pfx format and includes the full certificate chain. The pfx file is protected with an eight characters random generated password. The certificate file and password are separately sent to the certificate subscriber.

6.4.2 Activation Data Protection

CA certificates

Cryptographic module passphrases used to activate any Riksbank CA private keys are stored in a locked safe at a secured site. The activation data protection mechanism shall also include a facility to temporarily suspend access to or terminate the operation of the Riksbank CA hardware and software, after five (5) failed login attempts. The protection mechanism for other activation data shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts.

Medium assurance certificates

Hardware modules use PIN to activate the keys. The hardware modules are configured to prevent more than three (3) failed attempts to enter the PIN by locking further attempts to enter the correct PIN.

To unlock the hardware module the personal unlocking key (PUK) needs to be implemented. The PUK are unique for each hardware module and handled securely.

The PUK is used to unlock the hardware module and is handled by the RA function.

Basic assurance certificates

The certificate holder is responsible for the protection and secure storage of the PKCS#12 file password.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The CA system must meet the following requirements, either through the operating system or as a combination of operating system, CA application, physical protection and manual procedures:

- Access control system shall identify operators on an individual level.
- All information stored in the certificate system is classified as "RB Confidential" and shall be protected against unauthorized access.
- Private Keys, passwords and other activation data is classified as "RB Strictly Confidential" and must be stored in encrypted form.
- All communications to and from the CA application which is classified as "RB Confidential" or "RB Strictly Confidential" must be encrypted.
- An operating system that is used as a platform for the CA system and surrounding systems shall be installed and maintained according to the Riksbank guidelines and instructions for each platform.
- The integrity of CA systems and information shall be protected against viruses, malicious and unauthorized software.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

The Riksbank will ensure that PKI systems are developed and implemented in strict compliance with the Riksbank security policy.

6.6.2 Security Management Controls

The Riksbank PKI System owner will ensure that any system change are recorded in the audit logs and follows the Riksbank change management procedures.

6.6.3 Life-cycle security controls

No stipulation.

6.7 Network Security Controls

The logical network protection for the PKI system computers and associated systems used for communication will be in accordance with the Riksbank guidelines and regulations. The logical protection is strong and in addition to ordinary security measures include the following,

- CA system is operated on its own separate network segments.
- Network segments are protected by a firewall.
- IDS will monitor the CA-system network segment in order to detect malicious or unauthorized network traffic.
- Only those network protocols required for operation of the CA systems will be allowed on the network segment.

- All communication to and from the CA application which is classified as RB Confidential or higher must be encrypted.

6.8 Time-Stamping

No stipulation.

7 Certificate and CRL Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

Certificates for subscribers issued by the Riksbank PKI CA use the X.509 version 3 (X.509 v3) standards.

7.1.2 Certificate extensions

The Riksbank follows RFC 3280 regarding valid certificate extensions. The Riksbank Root CA is bound to the Riksbank assigned OID series.

The Riksbank CA certificates will not contain private critical extensions.

7.1.3 Algorithm Object Identifiers

No stipulation.

7.1.4 Name Forms

Certificates issued by the Riksbank PKI contain the X.500 distinguished name of the certificate issuer and that of the subject in the issuer name and subject name fields, respectively.

7.1.5 Name Constraints

See section 3.1.1.

7.1.6 Certificate Policy Object Identifier

The OID of this document; 1.2.752.91.21.1.2.0

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

The Riksbank PKI platform issues CRL as X.509 v2 CRL or higher.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.3 OCSP Profile

If used, the profile for the OCSP requests received and OCSP responses issued by the Riksbank OCSP Responder conforms to the standards as described in [RFC2560].

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP Extensions

No stipulation.

8 Compliance Audit and Other Assessment

8.1 Frequency and Circumstances of Assessment

8.1.1 Internal review

The review shall be performed annually by an internal review following the Riksbank standard procedures.

8.1.2 External review

External reviews shall be performed by an external party with a maximum interval of three (3) year.

8.2 Identity/Qualifications of Assessor

8.2.1 Internal review

Internal reviews shall be performed by an individual with the necessary expertise and understanding of PKI technology, information technology and the tools relating to it. The individual shall also have experience in the field of IT security audits.

8.2.2 External review

External reviews must be performed by an individual with the same qualifications as the internal reviewer and have received training in IT auditing and be certified by CISA (Certified Information Systems Auditor) or other comparable certification.

8.3 Assessor's Relationship to Assessed Entity

8.3.1 Internal review

Internal reviewer should be independent of the system owner and its operational and management organization.

8.3.2 External review

External reviewer must be independent from the Riksbank.

8.4 Topics Covered by Assessment

The following minimum conditions shall be examined:

- That the Certification Practice Statement (CPS) meets the requirements of this document.
- That the Riksbank PKI certificate system has been implemented and is compliant with the technical requirements, personnel requirements and procedures described in this document and CPS.
- That the Riksbank PKI certificate system reaches the level of assurance set out in this document and other governing documents and that rules that establish security and reliability of the certificate type ”Basic Assurance” and "Medium Assurance" are in place.

8.5 Actions Taken as a Result of Deficiency

In the event that any deficiencies are found upon examination, the system owner is responsible for urgently carrying out a risk assessment aimed at describing the impact on the reliability of the PKI system and the effects of the deficiencies during the time they existed and then for deciding on measures to restore the PKI system to the accuracy set out in this document. The system owner shall report events that may have or have had an impact on security in accordance with the Riksbank regulations for incident management.

8.6 Communication of Results

The results of all reviews will be communicated to the system owner. Other participants are not entitled to have access to the review findings. The Riksbank may, at its sole discretion, publish a summary of the results of the review on the same web server where the CP exists.

9 Other Business and Legal Matters

9.1 Fees

No charges or fees occur unless a separate agreement is reached between the respective parties governing such matters.

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information fees

No stipulation.

9.1.4 Fees for other services, such as policy information

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Sveriges riksbank shall maintain sufficient insurances in respect of its performance under this CP through Kammarkollegiet (The Legal, Financial and Administrative Services Agency) in accordance with ordinance on governmental agencies´ risk management (förordningen (1995:1300) om statliga myndigheters riskhantering).

9.2.2 Other Assets

Sveriges riksbank processing centre and accountable issuers shall have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to subscribers and relying parties.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

All information that is collected, generated, transmitted or maintained by the issuer is classified in accordance with the Sveriges Riksbank regulation "Classification and management of the Riksbank's information"

- If a request for disclosure of public documents is received, a usual confidentiality assessment will be carried out under the Secrecy Act before any information is disclosed.

9.3.2 Information Not Within the Scope of Confidential Information

The following information are classified as open:

- All public certificates excluding administrative certificates and the CA system's internal certificates.
- Revocation lists issued by the issuer.
- This document (CP).
- Sveriges riksbank Certificate Practice Statement (CPS)

If a request for disclosure of public documents is received, a usual confidentiality assessment will be carried out under the Secrecy Act before any information is disclosed.

9.3.3 Responsibility to Protect Confidential Information

The categories of information deemed to be "Confidential Information".

- Private keys, CA's, RA's, Directories, (or OCSP Responders), must be kept strictly confidential. Each party is responsible for keeping their own private key confidential, after the certificate was issued.
- All PKI documents, except this document (CP) and Sveriges riksbank Certificate Practice Statement (CPS).
- Results of audits.

9.4 Privacy of Personal Information

The Riksbank CA does not collect any confidential or proprietary information. Except in cases where the CA or RA archive copies of identification documents to validate the identity of an individual relying parties.

Riksbank guarantees that this personal information will not be used for any other purpose

All registration and use of personal data on individual certificate subscribers will be done in accordance with the General Data Protection Regulation (GDPR) as implemented through Swedish legislation.

9.4.1 Privacy Plan

No stipulation.

9.4.2 Information Treated as Private

See section 9.3.1

9.4.3 Information Not Deemed Private

See section 9.3.2

9.4.4 Responsibility to Protect Private Information

See section 9.3.3

9.4.5 Notice and Consent to Use Private Information

No stipulation.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

No stipulation.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

The Riksbank PKI does not claim any intellectual property rights on issued certificates. Parts of this document are inspired by or even copied (in no particular order) from the ESCB-PKI, Banque de France Certification Authority, CERN PKI and may indirectly derive from documents they draw from. Anybody may freely copy from any version of the Riksbank Certificate Policy provided they include an acknowledgment of the source.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The Riksbank, acting in its capacity as an issuer of certificates, shall in accordance with this document and the Riksbank guidelines and rules:

- Create certificates upon request using the data obtained from RA.
- Ensure that the system owner of the certificate system publishes a certification practice statement (CPS) and follows this CP.
- Protect the issuer's own private keys in a safe manner.
- Provide information in accordance with this document.
- Have agreements with the certificate subscribers.
- Maintain this document.
- Revoke certificates and issue revocation lists in accordance with this document.

- Publish a public certificate for the CA so that certificate subscribers and relying parties can easily verify the validity and accuracy of certification revocation lists.
- Only register personal data on individual certificate subscribers in accordance with the General Data Protection Regulation (GDPR) as implemented through Swedish legislation
- To perform all tasks in accordance with Swedish legislation.

9.6.2 RA Representations and Warranties

The Registration Authority (RA) shall undertake to comply with the requirements of this document and the CPS and commit to undertake the following duties:

- Registration, verification and administration of applications for certificates and keys.
- Registration and management of certificates and keys with associated hardware.
- Generation of encryption keys in a designated media.
- Identification of users before issuing certificates with associated hardware.
- Receive notification of the revocation of certificates and cards, and request revocation.

9.6.3 Subscriber Representations and Warranties

Certificate subscribers shall enter into an agreement with the Riksbank, which describes the conditions for using the supplied keys and certificates.

The certificate subscriber's responsibilities are;

- To ensure that the information in the application and the issued certificate is correct.
- To immediately notify the issuer if the application information is changed.
- To not use certificates and keys after the expiry date or after the certificate has been revoked.
- To comply with other rules and handling instructions contained in the agreement.

The certificate holder is required to;

- Immediately report the loss of the private key
- Consider the private key a secret document and protect it thereafter
- Select the PIN in accordance with instructions
- Protect the PIN so that no unauthorized persons have access to it and to never keep the PIN in the same place as the private key
- Never leave the private key unattended in an "unlocked" mode
- To comply with other rules and handling instructions contained in the agreement

■ 9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

No stipulation.

9.8 Limitations of Liability

The Riksbank CA accepts no liability for damages incurred by a relying party accepting one of its certificates, or by a subscriber whose valid certificate is refused or whose revoked certificate is unduly accepted by a relying party. It also accepts no liability for damages arising from the non-issuance of a requested certificate, or for the revocation of a certificate initiated by the CA or the appropriate RA acting in conformance with this CP.

9.9 Indemnities

The Riksbank CA will not pay indemnities for damages arising from the use or rejection of certificates it issues. End entities shall indemnify and hold harmless the Riksbank CA and all appropriate RAs operating under this CP against all claims and settlements resulting from fraudulent information provided with the certificate application, and the use and acceptance of a certificate which violates the provisions of this CP document.

9.10 Term and Termination

9.10.1 Term

This CP shall remain in effect at least until the expiry of the last certificate issued under the CP or until an updated version is published.

9.10.2 Termination

This CP remains effective until it is superseded by a newer version.

9.10.3 Effect of Termination and Survival

This CP shall be published at least 5 years after the last issued certificate expires.

9.11 Individual Notices and Communications with Participants

In the event of a change of any sort to the technical composition of the PKI, the CA undertakes to conduct an impact assessment on the level of quality and security of CA and component functions.

9.12 Amendments

9.12.1 Procedure for Amendment

Certificate subscribers and relying parties will not be notified in advance if the CP document is changed. When changes are made, the system owner will be notified before the new CP document is published on the specified site as defined in Section 2.3. Changes are published on the same website.

9.12.2 Notification Mechanism and Period

See section 9.12.1

9.12.3 Circumstances Under Which OID Must be Changed

Substantial changes shall cause the OID to be changed. The decision is made by the Riksbank PKI System manager and submitted to the system owner for approval.

9.13 Dispute Resolution Procedures

Any disputes shall be settled by a Swedish court.

9.14 Governing Law

Swedish law applies.

9.15 Compliance with Applicable Law

All activities relating to the request, issuance, use or acceptance of a Riksbank CA certificate must comply with Swedish law. Activities initiated from or destined for another country than Sweden must also comply with that country's law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CP document supersedes any prior agreements, written or oral, between the parties covered by this present document.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should a clause of the present CP/CPS document become void because it conflicts with the governing law (see 9.14) or because it has been declared invalid or unenforceable by a court or other law-enforcing entity, this clause shall become void (and should be replaced as soon as possible by a conforming clause), but the remainder of this document shall remain in force.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

No stipulation.

■ 9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.