Certificate Policy

Digital Signature
Medium Strength Soft Certificates

SwUPKI:
The Public Key Infrastructure for
Swedish Universities and University Colleges

Certificate Policy Name: SwUPKISoftSignCert–1
Object Identifier: {iso(1) member-body(2) se(752) stockholms universitet(43) swupki(2) policies(1) swupkisoftsigncert(1) swupkisoftsigncert-1(1)}

Revision history:

Version	Date	Comment
1.0	2001-02-08	Initial Release

Definitions

Activation data – Private data, other than keys, that are required when accessing cryptographic modules.

CA Certificate – A certificate for the public key of one CA (the **Subscriber CA**) issued by another CA (the **Issuer CA**).

CA System – The CMS and other systems used by a CA.

Certificate – The public key of a Subject, together with related information, digitally signed with the private key of the CA that issued the Certificate.

Certificate Management System (CMS) – The system used to issue and manage certificates.

Certificate Policy (CP) – A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

Certificate Revocation List (CRL) – A list maintained by a CA of the certificates that it has issued that are revoked before their natural expiration time.

Certification Authority (CA) – An entity that is trusted to associate a Subject with a public and a private key pair. The CA links the key pair to the Subject by issuing a certificate for the Subject containing the public key as data.

Certification path – An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification Practice Statement (CPS) – A statement of the practices a CA employs in issuing and managing certificates.

Certificate Status Service (CSS) – The service provided through a CRL repository or an OCSS is jointly called the Certificate Status Service (CSS).

Cross-certification – The process undertaken by CAs to establish a trust relationship, confirmed when each CA issues a certificate for the public key of the other CA. When two CAs are cross-certified, they have agreed to trust and rely on each other's public key certificates and keys as if they had issued them themselves.

Cryptographic module – The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms.

Digital signature – The result of a cryptographic transformation of a message using a private key. A person who has the message and the signature can determine
a) if the signature was created using the private key of the alleged Subject and
b) if the message has been altered since the signature was created.

End Entity – A Subscriber, Relying Party, or IT-system (that is not a CA or RA) that uses the keys and certificates created within a PKI.

Entity – An autonomous element within the PKI. This may be a CA, an RA or an End Entity.

Level One CA – The highest level CA within an Organisation. The Policy CA confirms that an Organisation is accepted as a member of the PKI by issuing a certificate for the public key of its Level One CA.

On-line Certificate Status Service (OCSS) – An on-line service that provides timely information regarding the revocation status of a certificate.

Private key – The private part of an asymmetric key pair used for public key encryption techniques. The private key is typically used for creating digital signatures or decrypting messages.

Policy CA – The CA, at the top of the PKI, assigned by the PMA to sign the CA-certificates of the Level One CAs of the PKI.

Policy Management Authority (PMA) – A PKI body responsible for setting, implementing, and administering policy decisions regarding CPs and CPSs throughout the PKI.

Public key – The public part of an asymmetric key pair used for public key encryption techniques. The public key is typically used for verifying digital signatures or to encrypt messages sent to the owner of the private key.

Public Key Infrastructure (PKI) – The entire set of organisations, practices, processes, server platforms, software, and workstations used for the purpose of administering policies, certificates and keys.

Registration Authority (RA) – An entity that from the CA has received the responsibility to identify and authenticate Subscribers and to verify their authority to act on behalf of the Subject. The RA does not sign or issue certificates.

Relying Party – A recipient of a certificate who acts in reliance on that certificate and/or a digital signature verified using that certificate.

Repository – A system for storing and distributing certificates or other information relevant to certificates.

Secret key – A key used in symmetric encryption where the sender and receiver of encrypted messages use the same secret key.

Set of provisions – A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a CP or CPS employing the approach described in this framework.

Sponsor – A Sponsor is an organisational unit or officer with the authority to nominate a person to be a Subscriber of certificates.

Subject – A certificate is assigned to a Subject. The Subject can be the Subscriber of the certificate or an organisational role or IT-system for whom the Subscriber is responsible and accountable.

Subscriber – The individual to which the public key certified in a certificate is attributable. Each Subscriber must have a Sponsor in the Organisation issuing the certificate.

List of Abbreviations

C	Country
CA	Certification Authority
CASO	Certification Authority Security Officer
CASA	Certification Authority System Administrator
CAO	Certification Authority Operator
CMS	Certificate Management System
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSS	Certificate Status Service
DC	Domain Component
DN	Distinguished Name
I&A	Identification and Authentication
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISO	International Organisation for Standardisation
ITU	International Telecommunications Union
O	Organisation
OU	Organisational Unit
OCSS	On-line Certificate Status System
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)
PMA	Policy Management Authority
RA	Registration Authority
RFC	Request for Comments
RSA	A specific Public key algorithm
SIS	Swedish institute of standards
SwUPKI	Swedish Universities' and University Colleges' Public Key Infrastructure
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

1 Introduction

A Certificate Policy (CP) is a "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements" [X509]. The purpose of a CP is to create the appropriate confidence in certificates issued by a Certificate Authority (CA) complying with the particular policy.

This CP is intended to have broad applicability across the different technical platforms and organisational structures of the members of the Public Key Infrastructure for Swedish universities and university colleges (SwUPKI). It is therefore focused on requirements that are not bound to specific technical solutions. The CP is complemented with a specific Certification Practice Statement (CPS) for each Certificate Authority (CA), which - in sufficient detail - outlines the technical, procedural and personnel policies and practices of the CA.

Users of this document may need to consult the CPS of the CA that has issued a particular certificate to obtain further details of precisely how the CP is implemented by the particular CA.

This CP is intended to comply with PKIX "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" [RFC2527]. Certificates and Certificate Revocation Lists of are intended to comply with PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [RFC2459].

1.1 Overview

This CP is a policy for SwUPKI in its issuance, management and use of certificates containing public keys for digital signatures. Keys for digital signatures are intended to be used in
signature verification,
authentication,
data integrity and
key agreement mechanisms.

The members of SwUPKI disclaim all liability for any use other than the intended, as identified by this CP, of certificates issued under this CP. Any dispute concerning key or certificate management under this policy are to be resolved by the parties concerned as stated in this policy.

Users of certificates issued by a CA under this CP are to consult the CA to obtain further details of the implementation of this CP. A CA operating under this CP is required to have a Certificate Practice Statement (CPS) that states the practices the CA employs in issuing and managing certificates.

This CP identifies specific roles, responsibilities and obligations for
the Policy Management Authority (PMA) supervising the PKI and responsible for registering, interpreting and maintaining this CP,
the Policy CA of SwUPKI,
CAs issuing certificates pursuant to this CP,
Registration Authorities (RAs) performing tasks assigned to them by the CA,
Sponsors nominating certificate Subjects and Subscribers,
Subscribers and
Relying Parties.

The policy shall be reflected in signed agreements between a CA and subscribers. A CA shall instruct Subscribers of their obligations, and of the intended use of certificates issued in compliance with this CP.

Certificates may only be issued under this policy following authentication of a Subscriber's identity and of the Subscriber's responsibility and accountability for the certificate Subject. Identification and authentication shall be in the manner set out in this policy.

The private key corresponding to the public key of a certificate of an End Entity may not be backed-up or otherwise stored by the CA.

A potential Subscriber shall give the CA consent to collect, for issuance of a certificate and otherwise for the agreement, necessary personal information about the Subscriber. Personal information collected by a CA and not included in the certificate may not be disclosed without consent of the Subscriber unless required by law.

The universities and university colleges of Sweden does not represent or warrant 100% availability of the CA services offered by SwUPKI under this policy. System maintenance, system repair or factors outside the control of the CA may affect such availability.

Issuance of a public key certificate under this policy does not imply that the Subject or Subscriber has any authority to conduct business transactions on behalf of the organisation operating the CA.

The laws of Sweden concerning the enforceability, construction, interpretation and validity of this CP will govern the CAs.

SwUPKI reserves the right not to enter into a cross-certification agreement with an external PKI or CA.

1.2 Identification

This CP is registered following the procedures specified in ISO/IEC and ITU standards and assigned a unique object identifier, which is carried in a standard extension field of an X.509 certificate. By inspecting this field, a Relying Party may be able to determine whether a particular certificate is suitable for the intended use.

Certificate Policy Name: SwUPKISoftSignCert–1
Object Identifier: {iso(1) member-body(2) se(752) stockholms universitet(43) swupki(2) policies(1) swupkisoftsigncert(1) swupkisoftsigncert-1(1)}

This policy is published at URL: http://www.swupki.su.se/CP

1.3 Community and Applicability

This policy is designed for use in SwUPKI. Only Swedish universities or university colleges accredited by the Swedish government and related organisations complying with this CP can be members of SwUPKI. “Organisation” is used to denote a member of SwUPKI.

1.3.1 Policy Management Authority (PMA)

One member of SwUPKI has the specific responsibility of being the Policy Management Authority of the PKI. The PMA is responsible for:
registering, interpreting and maintaining this CP,
appointing a member of SwUPKI to serve as the Policy CA for SwUPKI,
approving the CPSs of CAs in SwUPKI,
compliance inspections and general supervision of SwUPKI,
cross-certification with other PKIs and with CAs of other PKIs.

1.3.2 Certification Authorities (CAs)

Each Organisation in the PKI shall provide CA services operating in compliance with this CP. Such a CA is responsible for:
the creation and signing of certificates, binding Subscribers, PKI personnel and (where permitted) other CAs to the public signature verification keys attributable to them,
providing a Certificate Repository and a Certificate Status Service (CSS), see 1.3.4,
publishing a CPS that includes reference to this CP,
assigning duties to its RAs, and for
the compliance with this CP by the CA itself, its RAs and any subordinate CAs.

A CA may not assign the duty of issuing certificates to an RA.

While an Organisation in the PKI may use a contractor to provide (some of its) CA services, it remains responsible and accountable for the operation of its CA.

Cross-certification under this CP, with CAs external to SwUPKI, may only be done by the Policy CA after decision by the PMA, and shall comply with this CP and any additional requirements decided by the PMA.

1.3.3 Registration Authorities

Any Registration Authority (RA) operating in compliance with this CP is responsible for all duties assigned to it by the CA. An RA may perform duties on behalf of more than one CA, provided that in doing so it satisfies all the requirements of this CP. An RA may not issue certificates.

1.3.4 Repositories

A CA must ensure that there is a Certificate repository and a Certificate Status Service (CSS) associated with it. A CSS consists of a CRL repository and an optional Online Certificate Status Service (OCSS).

These repositories and services shall comply with current standards as stated in the CPS.

1.3.5 Sponsors

Each Organisation in SwUPKI is solely responsible for issuing the certificates it finds reasons to use in its business. The policy for delegating authority to nominate persons to become Subscribers of certificates will vary between members, but the delegations are given to what we call Sponsors.

A Sponsor is an organisational unit or officer with the authority to nominate a person to be a Subscriber of certificates. The Sponsor may suggest appropriate distinguished names for Subjects and is responsible for either supplying or confirming authentication and certificate attribute details to the CA or RA. The Sponsor is also responsible for informing the CA or RA if the sponsor relationship with the Subscriber terminates or changes such that certificates should be revoked.

The PMA is the sponsor of the Policy CA.

1.3.6 Subscribers

A CA may only issue certificates to Subscribers - individuals (employees, students, guests and others) - having a Sponsor within the CA's Organisation.

Eligibility for a certificate is at the sole discretion of the CA.

1.3.7 Subjects

A CA may only issue certificates where the Subject is the Subscriber, or is an organisational role or an IT-system provided that responsibility and accountability is attributable to the Subscriber.

1.3.8 Policy Applicability

The certificates contain public keys corresponding to private keys for digital signatures. Keys for digital signatures are intended to be used in verification, authentication, data integrity and key agreement mechanisms.

The certificates are thus intended to be used for example for verifying the identity of electronic mail correspondents or for remote access to a computer system, verifying the identity of persons or other legal entities, or for protecting the integrity of software and data.

The CP is relevant for authentication and the protection of integrity of business transactions within the approval limits of the organisations and such that the falsification of the transaction would cause only minor financial loss or require only administrative action for correction.

This limit is at the discretion of the Relying Party or the organisation of the Relying Party.

The applicability of certificates issued in compliance with this policy does not rely solely on this compliance but is critically dependent on involved IT-systems as indicated in section 2.1.2.3.

1.4 Contact Details

This Certificate Policy is registered by Stockholms universitet, SE 106 91 Stockholm, Sweden. Stockholms universitet is the PMA of this SwUPKI CP and is fully responsible for registration, maintenance, and interpretation of the policy. Questions concerning this policy should be addressed to:

SwUPKI, Enheten för IT och Media, Stockholms universitet, SE 106 91 Stockholm, Sweden or info@swupki.su.se.

As an alternative to the address above, potential members may address their inquiries and requests to request@swupki.su.se or access http://www.swupki.su.se/join.html.

2 General Provisions

This section contains provisions relating to the respective obligations of the PMA, CAs, RAs, Sponsors, Subscribers, and Relying Parties, and other issues pertaining to law and dispute resolution.

2.1 Obligations

When an Entity suspects private key compromise, it shall immediately notify the CA that issued the certificate.

2.1.1 PMA Obligations

The PMA is the member of SwUPKI who is responsible for the supervision of SwUPKI. The PMA shall register, interpret and maintain this CP. It shall appoint one member to serve as the Policy CA. Before the Policy CA starts its operation, the PMA shall approve its CPS and give further instructions to ensure that the Policy CA operates in compliance with this CP and the intentions of the SwUPKI. The PMA shall make compliance inspections of the Policy CA in accordance with this CP.

The PMA accepts organisations as members of SwUPKI, and thus is the Sponsor of CAs subordinate to the Policy CA. Before accepting an organisation as a member of the SwUPKI, the PMA shall approve the CPS of the potential member.

The PMA shall ensure that compliance inspections are carried out to determine whether the performance of the CAs in SwUPKI meet the standards established in their CPSs and satisfy the requirements of this CP.

The PMA shall decide whether SwUPKI, through its Policy CA, shall attempt to cross-certify with other PKIs or CAs of other PKIs. The PMA shall include in such a decision any requirements, in addition to compliance with this CP, for cross-certification.

2.1.2 CA Obligations

A CA shall operate in accordance with its CPS, this CP, and the laws of Sweden when managing keys and issuing certificates to RAs, other CAs and Subscribers under this CP. The CA shall ensure that all RAs operating on its behalf shall comply with the relevant provisions of this CP concerning the operation of RAs. If no RAs are appointed, the RA obligations, as stated in 2.2, are obligations of the CA. A CA may not assign the duty of issuing certificates to an RA. The CA will take all reasonable measures to ensure that Subscribers and Relying Parties are aware of their respective rights and obligations with respect to the operation and management of any keys, certificates or End Entity hardware and software used in connection with the PKI.

A CA must provide notice of limitations of liability. Such notice must, at a minimum, be provided in the `userNotice` field of the certificate as defined by PKIX ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile” [RFC2459]. Because of space limitations within a certificate, such notice must be limited to the following: “Limited Liability. See http://www.swupki.su.se/CP”.

A CA must:
issue a CPS that is approved by the PMA and that, in sufficient detail, outlines the technical, procedural and personnel policies and practices of the CA and that meets the requirements of all the CPs supported by the CA;
maintain a CA Repository;
have in place mechanisms and procedures to ensure that its RAs and Subscribers are aware of, and agree to abide with, the stipulations in this CP that apply to them; and
establish that any subordinate CA complies with the CP that is mutually recognised.

CA personnel associated with PKI roles must be individually accountable for actions they perform. “Individually accountable” means that the CA and RA practices must ensure that there is evidence that attributes an action to the person performing the action.

In addition, the Policy CA must:
structure its CPS so that proposed common practices for the PKI as a whole are easily identified and referred to in the CPSs of subordinate CAs;
through compliance inspection, verify to cross-certifying CAs that it complies with this CP;

document any negotiated enhancements and assurances of the operational procedures, restrictions on the usage of the cross-certificate, validity period for the cross-certificate, liability issues, etc, in an agreement with the cross-certified CA; and
make any applicable disclaimers available to the Subscribers of both CAs.

CAs may, but are not required to, provide additional undertakings.

2.1.2.1 Notification of Certificate Issuance and Revocation

A CA must offer a CSS to Subscribers and Relying Parties in accordance with 4.4. A CA must notify a Subscriber when a certificate whose Subject is attributable to the Subscriber, is issued or revoked.

2.1.2.2 Accuracy of Representations

When an Issuing CA publishes a certificate in its repository, it certifies that it has issued a certificate to a Subscriber that has entered into a Subscriber Agreement with the CA. It also certifies that the information stated in the certificate was verified in accordance with this CP. The publication of the certificate in a repository, to which a Relying Party has access, constitutes notice of such verification.

2.1.2.3 Subscriber Agreement

A CA shall provide to each Subscriber notice of the rights and obligations the Subscriber under this CP. Such notice shall be in the form of a Subscriber Agreement and shall include
the obligations of the Subscriber concerning key protection;
procedures for communication between the Subscriber and the CA or RA, including communication of changes in service delivery or changes to this policy;
procedures for dealing with suspected key compromise, certificate or key renewal, CA termination, and dispute resolution; and
a description of the obligation of a Relying Party with respect to use, verification and validation of certificates.

The agreement shall also advise the Subscriber that the kind of applications intended to be used with the certificates and services of the PKI must, as a minimum, meet the following requirements. They must:
correctly generate, protect, transfer and use the public and private keys;
be capable of performing the appropriate certificate validity and verification checking;
report appropriate information and warnings to the Relying Party;
be operated in accordance with the IT Security Policy of the Organisation.

Finally, the Subscriber shall, in the agreement, give the CA consent to collect, for the issuance of a certificate and otherwise for the agreement, necessary personal information about the Subscriber. Personal information collected by a CA and not included in the certificate may not be disclosed without consent of the Subscriber unless required by law.

2.1.2.4 Certificate Expiration, Revocation and Renewal

A CA must ensure that any procedures for the expiration, revocation and renewal of a certificate will conform to the relevant provisions of this CP; and
be expressly stated in the Subscriber Agreement, and any other applicable document outlining the terms and conditions of the certificate use.

2.1.2.5 Protection of CA's Private Keys

Each person involved in CA duties must ensure that its certificate signing private keys and activation data are protected in accordance with 4, 5 and 6.

2.1.2.6 Restrictions on CA's Private Key Use

A CA must ensure that its certificate signing private key is used only to sign certificates, CRLs and entries in an OCSS. If a CA undertakes to act in accordance with other policies, using the same private key or issuing identity, these shall be identified in the CPS.

2.1.3 RA Obligations

Each RA is appointed by the CA to perform some of the duties of the CA. The RA must, in operating on the behalf of the CA, comply with the relevant provisions of this CP and the CPS of the CA.

A RA is responsible for bringing to the attention of Subscribers all relevant information regarding the rights and obligations of the CA, RA and Subscriber contained in
this CP,
the Subscriber Agreement, and
any other relevant document outlining the terms and conditions of certificate use.

Records of all actions carried out in performance of RA duties must identify the individual who performed the particular duty.
RAs must not issue certificates.

There is no requirement for an RA to notify a Subscriber of the issuance or revocation of a certificate.

When an RA submits Subscriber information to a CA, it must certify to the CA that it has
verified that the Subscriber has a Sponsor within the Organisation,
authenticated the identity of that Subscriber in accordance with 3 and 4,
verified the authority of that Subscriber to receive a certificate for the particular Subject,
verified that the Subscriber possesses the private key corresponding to the public key to be included in the certificate.

Each person involved in RA duties must ensure that private keys and activation data used to access and operate RA applications are protected in accordance with 4, 5 and 6.

Private keys used by RA personnel to access and operate RA applications must not be used for any other purpose.

2.1.4 Sponsor Obligations

The Sponsor decides whom to nominate as a Subscriber of certificates. The Sponsor is also responsible for informing the CA or RA if the relationship between the Organisation and the Subscriber terminates or changes such that certificates should be revoked.

2.1.5 Subscriber Obligations

Any information required by the CA or RA in connection with a certificate application must be complete and accurate.

Every Subscriber must enter into a Subscriber Agreement, which outlines the obligations of the Subscriber stating the terms and conditions of use of issued certificates, including permitted applications and purposes.

The Subscriber must fulfil its obligations as stated in the Subscriber Agreement.

Subscribers must protect their private keys (personal private keys and private keys for Subjects attributable to them) in accordance with 6.2, and must take all reasonable measures to prevent their loss, disclosure, modification, or unauthorised use.

The Subscriber shall use the private keys of Subjects attributable to the Subscriber only for the purposes identified in the CP.

When a Subscriber suspects private key compromise, the Subscriber must immediately notify the CA that issued the certificate in a manner specified by that CA.

2.1.6 Relying Party Obligations

Before using a certificate, a Relying Party must ensure that:
the PKI can be trusted;
the certificate is appropriate for the intended use;
the certificate was issued as a valid SwUPKI certificate, by using the certification path validation procedure specified in X.509 and PKIX ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile” [RFC2459];
the certificate is valid by consulting the CSS as stated in 4.4.8.; and

the application software can process the content of the certificate and its extensions in accordance with this CP and the PKIX ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile” [RFC2459].

2.1.7 Repository Obligations

The CA is responsible for maintaining a CA Repository. The Repository shall be available for a high proportion of every 24-hour period. Certificates and CSS must be available to Relying Parties in accordance with the requirements stated in 2.6 and 4.4.7.

2.2 Liability

2.2.1 Liability

By signing a certificate containing a policy identifier, which indicates the use of this policy, a CA only ensures, to all who reasonably relies (see 2.1.4) on the information contained in the certificate, that its certification and repository services, issuance and revocation of certificates, and issuance of CRLs is in accordance with this CP. It will also take reasonable efforts to ensure that all RAs and Subscribers will follow the requirements of this policy when dealing with any certificates containing this policy’s OID or the associated keys.

2.2.2 Disclaimers of Warranties and Obligations

The CA and its Organisation disclaim all liability for any use other than the intended, as identified by this CP, of certificates issued under this CP. Any dispute concerning key or certificate management under this policy are to be resolved by the parties concerned as stated in this policy.

Certificates issued in compliance with this CP and containing this policy’s OID are only relevant for authentication and the protection of integrity of business transactions within the approval limits of the organisations and such that the falsification of the transaction would cause only minor financial loss or require only administrative action for correction. This limit is at the discretion of the Relying Party or the organisation of the Relying Party.

The members of SwUPKI do not represent or warrant 100% availability of the CA services offered by SwUPKI under this policy. System maintenance, system repair or factors outside the control of the CA may affect such availability.

The Organisation of the CA and its employees makes no representations, warranties or conditions, express or implied other than as expressly stated in this CP or its CPS.

The CA assumes no liability whatsoever in relation to the use of SwUPKI certificates or associated public/private key pairs in relation to cross-certified CAs and their relying parties.

2.3 Financial Responsibility

An Organisation or CA in SwUPKI that uses a contractor to provide (some of) its CA services must require that any contractor it uses provides satisfactory evidence of financial responsibility and waiver of any legislative immunity, if applicable.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

A CA must ensure that the laws of Sweden concerning the enforceability, construction, interpretation and validity of this Certificate Policy will govern any agreements.

2.4.2 Severability, Survival, Merger, Notice

A CA must ensure that any agreements by that CA will contain appropriate provisions governing severability, survival, merger or notice.

2.4.3 Dispute Resolution Procedures

Any dispute related to key and certificate management with an organisation or individual outside of the SwUPKI should be resolved using an appropriate dispute settlement mechanism. A dispute with a non-governmental organisation should be resolved by negotiation if possible. A dispute not settled by negotiation should be resolved either by arbitration in accordance with the Rules for Expedited Arbitrations of the Arbitration Institute of the Stockholm Chamber of Commerce or in accordance with the Rules of the Arbitration Institute of the Stockholm Chamber of Commerce.

A dispute related to key and certificate management between Organisations in SwUPKI should be resolved by negotiation if possible. A dispute not settled by negotiation should be resolved by the PMA or, where appropriate, through a mediator or arbitrator(s) appointed by the PMA.

A dispute related to key and certificate management within an Organisation shall be resolved by the appropriate organisational authority in conjunction with the Issuing CA.

Each CA must ensure that any agreement it enters into provides appropriate dispute resolution procedures.

2.5 Fees

No fees, other than those covering reasonable media reproduction and distribution costs, may be charged for supplying on-line or physical media copies of this CP or for supplying on-line copies of a CPS supporting this certificate policy.

2.6 Publication and Repository

A CA must use a CA Web Site for publishing CA documents and a CA Repository for publishing certificates and CRLs. As a complement to publishing CRLs in the CA Repository, an OCSS may optionally be offered. These services or parts thereof, may be operated by a separate organisation on behalf of the CA.

A CA must:
include the URL of the CA Web Site within any certificate it issues;
ensure the publication of its CP and its CPSs referencing this policy, digitally signed by an authorised representative of the CA, on the CA Web Site, the location of which must be indicated in compliance with 8.2;
ensure that the CP and the CPSs are publicly available on the CA Web Site;
provide a full text version of the CPS when necessary for the purposes of any audit, inspection, accreditation or cross-certification;
promptly upon issuance publish CA certificates and other certificates (after Subscriber consent) in the CA Repository;
publish the address and other relevant access information for its CSS on the CA Web Site;
publish signed CRLs in the CA repository and update the optional OCSS according to 4.4.7;
ensure that there are no access restrictions on checking certificate status in the optional OCSS;
ensure that CRLs, CA-certificates and other published certificates are publicly available in the CA Repository; and
ensure that access controls are configured so that only authorised CA personnel can modify the CA Web Site, CA Repository and CSS.

The CA shall provide relevant information about issued certificates when necessary to aid in dispute resolution concerning digital signatures.

Personal information collected by a CA and not included in the certificate may not be disclosed without consent of the Subscriber unless required by law.

2.7 Compliance Inspection

A compliance inspection determines whether the performance of a CA meets the standards established in its CPS and satisfies the requirements of the CPs it supports.

The PMA is responsible for the supervision of SwUPKI and is responsible for compliance inspections of the CAs of the PKI in accordance with this CP. The PMA shall yearly publish a compliance report for SwUPKI.

2.7.1 Frequency of Entity Compliance Inspection

A CA issuing certificates pursuant to this CP must establish, to the satisfaction of any CA it is subordinate to, that it fully complies with the requirements of this policy. This shall be done
before the CA it is subordinate to issues the CA-certificate
as a minimum every two years thereafter.

The PMA, at its discretion, may at any time request the Organisation operating the CA to have a compliance inspection carried out by an external inspector approved by the PMA.

A CA must report annually to the PMA whether they have complied with the requirements of this policy at all times during the period in question. The CA must also provide to the PMA reasons why the CA has not complied with its CP at all times and state any periods of non-compliance.

2.7.2 Identity/Qualifications of CA Inspector

Any person or entity, external to the organisations of the PKI, seeking to perform a compliance inspection must possess significant experience with PKI and cryptographic technologies as well as the operation of relevant PKI software.

2.7.3 Inspector's Relationship to Inspected CA

When a compliance inspector belongs to one of the organisations of the PKI, the inspector must not be affiliated with the inspected CA.

2.7.4 Topics Covered by Inspection

The compliance inspection must follow the inspection guidelines instituted by PMA. This will include inspecting whether:
the CPS outlines - in sufficient detail - the technical, procedural and personnel policies and practices of the CA;
the CPS meets the requirements of all the CPs supported by the CA;
the CA implements and complies with the CPS; and
each RA implements and complies with the CPS.

2.7.5 Actions Taken as a Result of Inspection

The CA must submit the inspection results to the PMA, and to the CA that issued its CA-certificate.

If irregularities are found, the CA must also submit a report of any action the CA will take in response to the inspection report. When a CA fails to take appropriate action in response to the inspection report, the PMA or the CA that issued its CA-certificate may:
indicate the irregularities, but allow the CA to continue operations until the next programmed inspection; or
allow the CA to continue operations for a maximum of thirty days pending correction of any problems prior to revocation; or
revoke the certificate of the CA.

Any decision regarding which of these actions to take will be based on the severity of the irregularities and on previous response to problems.

2.7.6 Communication of Results

CAs sub-ordinate to or cross-certified with the Policy CA must submit the inspection results to the PMA. The method and detail of notification of inspection results to CAs cross-certified with the SwUPKI Policy CA must be defined in the cross-certification agreement between the two parties.

2.8 Confidentiality of Information

CA Certificates, CRLs, OCSS entries, and personal or corporate information appearing on them and in public directories are not considered sensitive. Other certificates and personal or corporate information held by a CA or an RA (e.g. registration and revocation information, logged events, correspondence between the Subscriber

and the CA or RA) are considered sensitive and must not be disclosed without the prior consent of the Subscriber, unless required by law.

The private key of each Subject is to be held only by its Subscriber and must be kept confidential by them. Any disclosure by the Subscriber is at the Subscriber's own risk.

Inspection information is to be considered sensitive and must not be disclosed to anyone for any purpose other than inspection purposes or when required by law.

Information pertaining to the CA's management of a Subject's certificate may only be disclosed to the Subscriber, the Sponsor or when required by law.

Any requests for the disclosure of information must be signed and delivered to the CA.

2.9 Intellectual Property Rights

No stipulation.

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

Each Subject must have a clearly distinguishable and unique (within the CA) X.501 Distinguished Name (DN) in the certificate `subjectName` field in accordance with PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [RFC2459]. Each Subject may have alternative names in the `subjectAltName` extension field in accordance with [RFC2459], see 7.1.2. The DN must be in the form of a X.501 UTF8String and must not be blank.

The CPS shall state whether an alternative name of a particular form shall be included in the certificate.

3.1.2 Need for Names to Be Meaningful

The contents of each certificate `subjectName` and `issuerName` fields must be attributable to the authenticated name of the Subject and Issuer. It is recommended that the `organizationName` component should be included in the DN and that it should be the official name of the Organisation.

3.1.3 Rules for Interpreting Various Name Forms

No stipulation.

3.1.4 Uniqueness of Names

DNs must be unique among all Entities of a CA. For each Entity, additional numbers or letters may be appended to the `commonName` to ensure the uniqueness of the DN. The capability of Unique Identifier fields to differentiate Subscribers with identical names will not be supported.

3.1.5 Name Claim Dispute Resolution Procedure

The CA reserves the right to make all decisions regarding Entity names in all issued certificates.

3.1.6 Recognition, Authentication and Role of Trademarks in Identification and Authentication

No stipulation.

3.1.7 Method to Prove Possession of Private Key

Before a certificate is issued, the Issuing CA and a potential Subscriber shall confirm their respective identities through a method that proves the possession of their respective private keys.

The proof of possession method shall comply with current standards as stated in the CPS.

3.1.8 Authentication of the Identity of an Organisation, an Organisational Role or an IT-system

The identity of an organisation, an organisational role or an IT-system to be the Subject must be authenticated through one of the following means. The CA or RA:
must examine documentation providing evidence of the existence of the prospective Subject;
must verify the identity and authority of the Subscriber to act on behalf of the prospective Subject; and
may utilise previously shared information between the Subscriber and the CA and RA, if the CA has previously established the identity of the prospective Subject, and there have been no changes in the information presented.

The CA or RA must keep a record of the type and details of identification used.

3.1.9 Authentication of Individual Identity

The identity of an individual to be the Subscriber must be authenticated through one of the following means:

the CA or RA will compare the identity of the prospective Subscriber with a valid, certified and commonly recognised picture-type identification card such as a Swedish SIS-identity card; or
if the prospective Subscriber does not possess a picture-type identification as stated above, this can be replaced with a government paper certifying the existence of the claimed identity (e.g. ”personbevis” in Sweden) in combination with an independent individual of full age, whose identity is authenticated as described above, and who certifies that the prospective Subscriber has the claimed identity; or
if the CA has previously established the identity of the prospective Subscriber, and there have been no changes in the information presented, then the CA or RA and the prospective Subscriber may utilise this previously shared information;
if the application for a person to be a Subscriber is made by another individual, the CA, an RA or a Sponsor who is coordinating the establishment of an organisational network, the CA or RA must verify the identity and authority of this entity to act on behalf of the prospective Subscriber.

The CA or RA must keep a record of the type and details of identification used.

3.2 Authentication for Routine Renewal of Certificates

The request for renewal of a certificate may only be made by the Subscriber. The CA must authenticate a request for renewal, and the Subscriber must authenticate the subsequent response. This may be done by an on-line method as described in the CPS. A Subscriber requesting renewal of a certificate may authenticate the request using the keys corresponding to its valid certificate. When the certificate has expired the request for renewal must be authenticated in the same manner as the initial application of a certificate.

3.3 Authentication for Renewal of Certificates after Revocation

When the information contained in a certificate has changed or there is a known or suspected compromise of the private key, a CA must authenticate a request for renewal in the same way as an initial request. The CA or the RA must verify any change of the information contained in a certificate before the certificate is issued.

3.4 Authentication of Revocation Request

A CA or RA must authenticate a request for revocation of a certificate. A CA must establish and make publicly available in its CPS the process by which it addresses such requests and the means by which it will establish the validity of a request.

Requests for revocation of certificates must be logged.

4 Operational Requirements

This section specifies the requirements imposed upon issuing CA, subject CAs, RAs, or end entities with respect to various operational activities.

4.1 Application for a Certificate

A CA must ensure that all procedures and requirements with respect to an application for a certificate are set out in the CPS. Bulk applications on behalf of Subscribers are accepted only from Sponsors.

An application for a certificate where a person is the prospective Subject and Subscriber, may be made by the person or by another individual or organisation authorised to act on behalf of the prospective Subscriber. The application may also be made by the CA, an RA, or by a Sponsor coordinating the establishment of an organisational network.

An application for a certificate, where an organisation, organisational role or IT-system is the prospective Subject, may be made by a prospective Subscriber if the signature of the prospective Subject is attributable to the prospective Subscriber for the purposes of accountability and responsibility.

A CA must ensure that each application be accompanied by:
proof of the identity of the Subscriber according to 3.1.8 or 3.1.9;
when the applicant is not the Subscriber, proof of authorisation to act on behalf of the Subscriber;
when the applicant is not the Subject, proof of authorisation that the signature of the Subject is attributable to the Subscriber for the purposes of accountability and responsibility;
proof of authorisation for any requested certificate attributes;
a signed Subscriber Agreement according to 2.1.2.3;
a public signature verification key possessed by the Subscriber, according to 3.1.7.

The decision of whether to issue a certificate is at the sole discretion of the CA.

4.1.1 Application for a Cross-Certificate

The Policy CA shall identify all procedures and requirements with respect to an application for a cross-certificate in its cross-certification procedures.

The Policy CA must ensure that, in addition to what is stated in 4.1, a request for cross-certification with SwUPKI from a CA also must be accompanied by:
its CP and CPS;
an external compliance inspection report validating that the CA satisfies the requirements of its CP;
the public signature verification key generated by the CA.

The decision of whether to issue a cross-certificate is at the sole discretion of the Policy CA.

4.2 Certificate Issuance

The issuance of a certificate by a CA indicates a complete and final approval of the certificate application by the CA.

4.3 Certificate Acceptance

A CA must ensure that the Subscriber acknowledges acceptance of a certificate and accepts the obligations as articulated in the Subscriber Agreement.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Revocation

A CA must revoke a certificate:
when any of the information in the certificate changes;

upon suspected or known compromise of the private key.

The CA may, at its discretion, revoke a certificate when a Subscriber or a Subject fails to comply with obligations set out in this CP, the CPS, the Subscriber Agreement, or any applicable law.

When a CA is cross-certified with or sub-ordinate to the Policy CA, the Policy CA must revoke its CA-certificate:
when any of the information in the certificate changes;
upon suspected or known compromise of the private key.

The PMA may, at its discretion, instruct an issuing CA to revoke a CA-certificate when a certified CA fails to comply with obligations set out in this CP, its CPS, the Subscriber agreement or any applicable law.

Upon request from the Subscriber, the issuing CA shall revoke the certificate.

4.4.2 Who Can Request Revocation

The revocation of a certificate may only be requested by:
the Subscriber in whose name the certificate was issued;
the Sponsor;
personnel of the CA or its associated RAs.

The revocation of a CA-certificate may only be requested by:
the CA on whose behalf the CA-certificate was issued;
the personnel operating the CA issuing the CA-certificate;
the PMA.

4.4.3 Procedure for Revocation Request

A CA must ensure that all additional procedures and requirements with respect to revocation are set out in the CPS. An authenticated revocation request, and any resulting actions taken by the CA, must be recorded and retained. When a certificate is revoked, full justification for the revocation must also be documented.

When a certificate is revoked, the subscriber shall be informed and the revocation shall be published in the CSS.

4.4.4 Revocation Request Grace Period

Any action taken as a result of a request for revocation of a certificate must be initiated without delay as specified in the CPS.

4.4.5 Circumstances for Suspension

The SwUPKI does not support certificate suspension.

4.4.6 On-line Revocation/Status Checking Availability

The CSS may offer an On-line Certificate Status Service (OCSS) as a complement to the CRL. The availability of an OCSS shall be stated in the CPS.

4.4.7 CSS Publishing Frequency

A CA must ensure that it issues an up to date CRL and that it updates the optional OCSS as specified in the CPS. A CA must also ensure that it publishes the updated CRL without delay in the CA repository to ensure that the most recent CRL is available to Relying Parties. When a certificate is revoked due to key compromise, the CSS must be updated without delay.

4.4.8 CSS Checking Requirements

A Relying Party must, before their use, check the status of all certificates in the certificate validation chain against the current CRLs or through the OCSS. A Relying Party must also verify the authenticity and integrity of CRLs and the OCSS responses.

4.4.9 Special Requirements Regarding Key Compromise

See 4.8.3 and 4.8.2 for requirements in the event of revocation upon a compromise, or suspected compromise, of a private key.

4.5 System Security Audit Procedures

The security audit procedures in this section are valid for all CA-system components influencing the outcome of issuing processes for certificates issued in compliance with this CP and their corresponding CSS, CA-certificates and cross-certificates.

4.5.1 Types of Event Recorded

A CA shall record in audit log files, electronic or manual, all events relating to the security of the CA-system. All logs should contain the date and time of the event, and the identity of the entity which caused the event.

A CA should also collect and consolidate, either electronically or manually, security information generated outside the CA-system.

The parts of the CA-system that us network connected should use a reliable source for time synchronisation.

A CA must ensure that the CPS specifies what information is logged.

To facilitate decision-making, all agreements and communication relating to CA-services should be collected and consolidated, either electronically or manually, in a single location.

4.5.2 Frequency of Processing Audit Log

A CA must ensure that CA personnel as specified in the CPS periodically review its audit logs and that all significant events are explained in an audit log summary. Such reviews include verifying that the log has not been tampered with and brief inspections of all log entries, with a more thorough investigation of any alerts or irregularities in the logs.

Actions taken following these reviews must be documented.

4.5.3 Retention Period for Audit Log

A CA must retain recent audit logs on-site easily accessible for inspection and subsequently retain them in the manner described in 4.6.

4.5.4 Protection of Audit Log

The electronic audit log system must include mechanisms to time-stamp entries and to protect the log files from unauthorised viewing, modification, and deletion.

Manual audit information must be protected from unauthorised viewing, modification and destruction.

4.5.5 Audit Log Backup Procedures

Audit logs and audit summaries must be backed up or copied if in manual form.

4.5.6 Audit Collection System

A CA must identify its audit collection systems in the CPS.

4.5.7 Notification to Event-Causing Subject

When an event is logged by the audit collection system, no notice need be given to the individual, organisation or IT-system that caused the event.

4.5.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. The CA must ensure that a vulnerability assessment is performed, reviewed and revised following an examination of these monitored events.

4.6 Records archival

Certificates, and CSS data generated by the CA, must be retained for at least one year after the expiration of the key material. Audit information as detailed in 4.5, Subscriber Agreements and any inspection, audit, application, identification, authentication, acceptance and revocation information should be retained for at least seven years.

CA signing keys must be backed up by the CA and must be protected as prescribed in 6.2.

A second copy of all material retained or backed up must be stored in a location other than the CA site and must be protected by either physical security alone, or a combination of physical and cryptographic protection. Any such secondary site must provide adequate protection from environmental threats such as temperature, humidity and magnetism.

A CA should periodically verify the integrity of the backups. Material stored off-site must be periodically verified for data integrity.

In addition to the above, information retained or backed up by a CA may be subject to the law “Arkivlagen”.

The CA shall ensure availability of the archive and that archived information is stored in a readable format during its retention period, even if the CA’s operations are interrupted, suspended or terminated.

In the event that CA services are to be interrupted, suspended or terminated, the CA shall send notification to all subscribers to ensure the continued availability of the archive. All requests for access to archived information shall be sent to the CA or to the entity identified by the CA before terminating its service.

Further details of relevance concerning records archival shall be given in the CPS.

4.7 Key Changeover

A Subscriber, the CA, or the RA may initiate the key changeover process. Automated key changeover is permitted. A CA must ensure that the details of this process are indicated in its CPS.

Subscribers without valid keys must be re-authenticated by the CA or RA in the same manner as the initial registration.

When a Subscriber’s certificate has been revoked as a result of non-compliance, the CA must verify that any reasons for non-compliance have been addressed to its satisfaction before certificate re-issuance.

Keys may not be renewed using an expired digital signature key.

New Policy CA keys shall be generated and a new self signed CA certificate shall be issued at least three months before the expiration of the old private CA key.

After generation of Policy CA keys, the Policy CA shall cross-certify according to the following:
the Policy CA service representing the new private key shall issue one certificate for the old public Policy CA key signed with the new private Policy CA key and
the Policy CA service representing the old private Policy CA key shall issue one certificate for the new public Policy CA key signed with the old private Policy CA key.

4.8 Compromise and Disaster Recovery

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

A CA must establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data. When a repository is not under the control of the CA, the CA must ensure that any agreement with the repository provides that business continuity procedures be established and documented by the repository.

4.8.2 Entity Public Certificate Is Revoked

In the event of the need for revocation of a CA’s certificate, the CA must as described in the CPS, notify:
the PMA;
all of its subordinate CAs;

all CAs with whom it is cross-certified;
all of its RAs;
all Subscribers.

The CA must also:
publish the certificate serial number in the CSS;
revoke all CA-certificates signed with the revoked certificate.

After addressing the factors that led to revocation, the CA may:
generate a new CA signing key pair;
re-issue certificates to all Subjects and ensure all CSS entries are signed using the new key.

In the event of the need for revocation of any other Entity's certificate, see 4.4.

4.8.3 Entity Key Is Compromised

In the event of the compromise of a CA's private key a CA must:
request revocation of CA-certificates issued to the CA;
revoke all certificates issued using that key; and
provide appropriate notice (see 4.8.2).

After addressing the factors that led to key compromise, the CA may:
generate a new CA signing key pair;
request a new CA certificate; and
after receiving its new certificate, re-issue certificates to all Entities and ensure all CSS entries are signed using the new key.

In the event of the compromise, or suspected compromise, of any other Entity's private key, the Entity must notify the CA immediately.

4.8.4 Secure Facility after a Natural or Other Type of Disaster

A CA must establish a disaster recovery plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. When a repository is not under the control of the CA, the CA must ensure that any agreement with the repository provides that a disaster recovery plan be established and documented by the repository.

4.9 CA Termination

Termination of a CA is regarded as the situation when all service associated with a logical CA is terminated permanently. This is not the case when the service is transferred from one organisation to another, or when the CA-service is passed over from an old CA-key to a new CA-key.

In the event that a CA ceases operation, it must notify its Subscribers immediately upon the termination of operations and arrange for the continued retention of the CA's keys and information. It must also notify all its sub-ordinate CAs, all CAs with whom it is cross-certified, and it must terminate the CSS.

In the event of a change in management of a CA's operations, the CA must notify all Entities for which it has issued certificates and CAs with whom it has cross-certified.

In the event of a transfer of a CA's operations to another CA operating at a lower level of assurance, the certificates issued by the CA whose operations are being transferred must be revoked through a CRL signed by that CA prior to the transfer, and terminate the CSS.

The CA archives should be retained in the manner and for the time indicated in 4.6.

5 Physical, Procedural and Personnel Security

5.1 Physical Security Controls

5.1.1 & 5.1.2 Site Location, Construction and Physical Access

The CA site contains the hardware and software of the CA, including the CA workstation and any external cryptographic hardware module or token. The CA site shall satisfy:
physical security controls to control access to the CA site is implemented;
the CA site is manually or electronically monitored for intrusion at all times;
access to the CA site is limited to authorised personnel listed on an access list and to authorised and properly escorted and supervised visitors;
a site access log shall be kept and inspected periodically; and
all removable media and paper containing sensitive plain text information such as keys for signing certificates and CRLs shall be stored in a secure container or safe.

The CPS shall include a description of the CA site.

The duties of an RA may vary. If an RA acts only as an information verifier/forwarder, it is sufficient to ensure that the records of subscriber registration requests and tokens used to gain access to the RA workstation are stored in a secure container or safe. The hardware workstation and software may be kept in a regular office environment.

If an RA is permitted to submit on-line requests in a session with the CA, the CA shall ensure that the operation of the RA site provides appropriate security protection of the cryptographic module and the RA Administrator's private key. The CA must conduct a threat and risk assessment. For example, the cryptographic module and the RA Administrator's private key could be stored in a secure container or safe.

Where activation data is recorded, it must be stored in a security container accessible only to authorised personnel.

A CA must ensure that facilities used for off-site back-up, have the same level of security as the primary CA site.

5.2 Procedural Controls

5.2.1 Trusted Roles

5.2.1.1 CA Trusted Roles

A CA must ensure a separation of duties for critical CA functions to prevent one person from maliciously using the CA system without detection.

A CA should provide for a minimum of three distinct CA personnel roles, distinguishing between day-to-day operation and administration of the CA system and the management and audit of those operations. Different arrangements of separation of duties may be acceptable, provided the resilience to insider attack is at least as strong as with the recommended model and provided the roles are described in the CPS.

CA Security Officer (CASO) role includes:
assigning security privileges and access controls of CA Operators and System Administrators
commencement and cessation of CA services;
review of the audit log to detect CA Operators' compliance with system security policy;
personally conduct or supervise an annual inventory of the CA's records.

CA Operator (CAO) role includes:
configuring CA security policies;
verification of audit logs;
verification of CP and CPS compliance;
creation, renewal or revocation of certificates;

generating, distributing, and otherwise managing CRLs and OCSS;

CA System Administrator (CASA) role includes:
configuration and maintenance of the CA system hardware and software;
creating emergency system restart media to recover from catastrophic system loss;
performing system backups, software upgrades and recovery, including the secure storage and distribution of the backups and upgrades to an off-site location.

Only these personnel should have access to the hardware and software that controls the CA operation.

5.2.1.2 RA Trusted Roles

A CA must ensure that RA personnel understand their responsibility for the identification and authentication of prospective Subscribers and perform the following functions:
acceptance of requests for certificates, certificate change, and revocation;
authentication of an applicant's identity and authorisations;
transmission of applicant information to the CA;
provision of authorisation codes for on-line key exchange and certificate creation.

A CA may permit all duties for RA functions to be performed by one individual.

5.2.2 Number of Persons Required per Task

A CA must ensure that no single individual may gain access to Subscriber private keys stored by the CA. At minimum two individuals, preferably using a split-knowledge technique, such as twin passwords, must perform any key recovery operation.

Multi-user control is also required for CA key generation as outlined in 6.2.2.

An individual operating alone may perform all other duties associated with CA roles. A CA must ensure that any verification process it employs provides for oversight of all activities performed by privileged CA role holders.

For a CA, different individuals shall fill each of the three roles described above and at least one individual shall be appointed per task.

5.2.3 Identification and Authentication for Each Role

All CA personnel must have their identity and authorisation verified before they are:
included in the access list for the CA site;
included in the access list for physical access to the CA system;
given a certificate for the performance of their CA role;
given an account on the CA system.

Each of these certificates and accounts (with the exception of CA signing certificates) must:
be directly attributable to an individual;
not be shared;
be restricted to actions authorised for that role through the use of CA software, operating system and procedural controls.

CA operations must be secured, using mechanisms such as token-based strong authentication and encryption, when accessed across a shared network.

5.3 Personnel Security Controls

A CA must ensure that all personnel performing duties with respect to the operation of a CA or RA must:
be appointed in writing;
be bound by contract or statute to the terms and conditions of the position they are to fill;
have received comprehensive training with respect to the duties they are to perform;
be bound by statute or contract not to disclose sensitive CA security-relevant information or Subscriber information; and
not be assigned duties that may cause a conflict of interest with their CA or RA duties.

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

The CAO role, which involves creating and managing certificate and key information, is a critical role for the security. The individual assuming the CAO role should be of unquestionable loyalty, trustworthiness and integrity, and should have demonstrated a security consciousness and awareness in his or her daily activities.

All CA personnel in sensitive positions, including, at least, all CAO, and CASO roles, shall not as far known have been previously relieved of a past assignment for reasons of negligence or non-performance of duties.

CA organisations may also specify special requirements. Such requirements shall be stated in the applicable CPS.

5.3.2 Training Requirements

A CA must ensure that all personnel performing duties with respect to the operation of a CA or RA must receive comprehensive training in:
the CA/RA security principles and mechanisms;
all PKI software versions in use on the CA system;
all PKI duties they are expected to perform; and
disaster recovery and business continuity procedures.

5.3.3 Retraining Frequency and Requirements

The requirements of 5.3.2 must be kept current to accommodate changes in the CA system. Refresher training must be conducted as required.

5.3.4 Contracting Personnel Requirements

CA must ensure that contractor access to the CA site is in accordance with 5.1.1.

5.3.5 Documentation Supplied to Personnel

A CA must make available to its CA and RA personnel, the CPs it supports, its CPS, and any specific statutes, policies or contracts relevant to their position.

6 Technical Security Controls

This section contains provisions of the public/private key pair management policy for CAs, RAs and end entities, and the corresponding technical controls.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Each prospective Subscriber must generate its own key pair for a cryptographic algorithm. Approved cryptographic algorithms are listed in 7.1.3.

6.1.2 Private Key Delivery to Entity

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

The public signature verification key must be delivered to the CA, either via an on-line transaction in accordance with the PKIX "Internet X.509 Public Key Infrastructure Certificate Management Protocols" [RFC2510], or via an equally secure manner stated in the CPS.

6.1.4 CA Public Key Delivery to Users

The certificate containing a CA's public signature verification key shall be available from the issuing CA's Repository.

6.1.5 Key Sizes

A CA must ensure that each certified public key is of the type and length stated in 6.3.2.

6.1.6 Public Key Parameters Generation

Stipulations, if any, shall be specified in the CPS.

6.1.7 Parameter Quality Checking

Stipulations, if any, shall be specified in the CPS

6.1.8 Hardware/Software Key Generation

Stipulations, if any, shall be specified in the CPS.

6.1.9 Key Usage Purposes (As per X.509 v3 field)

Only CA signing keys may be used for signing certificates and CRLs, and the CA signing keys shall only be used for signing certificates and CRLs.

End Entity signing keys may be used for authentication, non-repudiation and message integrity. They may also be used for session key establishment.

The certificate `KeyUsage` field is used in accordance with PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [RFC2459]. The values of the `KeyUsage` field are specified in 7.1.2.

6.2 Private Key Protection

6.2.1 Policy CA Private Signing Key

Two persons must participate or be present in the generation of the Policy CA's private signing key.

The Policy CA must protect its private signing key from disclosure. When not active, the private key must be stored in encrypted form to protect it from unauthorised use. The activation data for the private key may be in

the form of a password. Two persons must participate or be present to activate the Policy CA's private signing key.

Private keys must not be escrowed. See 4.6 for archival of Policy CA private keys.

There have to be means for recovering the Policy CA's private signing key in case of system disaster. The Policy CA's private signing key shall be backed up for this purpose in a way that provides at least the same level of protection in all situations as stipulated for the regular active private signing key used in the CMS.

These procedures used shall be described in the CPS.

6.2.2 CA Private Signing Key

Two persons must participate or be present in the generation of a CA's private signing key.

The CA must protect its private signing key from disclosure. When not active, the private key must be stored in encrypted form to protect it from unauthorised use. The activation data for the private key may be in the form of a password. Two persons must participate or be present to activate a CA's private signing key.

Private keys must not be escrowed. See 4.6 for archival of CA private keys.

There have to be means for recovering a CA's private signing key in case of system disaster. The CA's private signing key shall be backed up for this purpose in a way that provides at least the same level of protection in all situations as stipulated for the regular active private signing key used in the CMS.

These procedures used shall be described in the CPS.

6.2.3 End Entity Private Signing Key

The Subscriber must protect its private keys from disclosure. When not active, the private key must be stored in encrypted form to protect it from unauthorised use. The activation data for the private key may be in the form of a password.

Private keys must not be escrowed.

An Entity may optionally back up its own private key. If so, the keys must be copied and stored in encrypted form and protected at a level no lower than stipulated for the primary version of the key.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

All public keys are archived by the Issuing CA.

6.3.2 Usage Periods for the Public and Private Keys

No RSA key of length 1024 shall have a validity period longer two years and no key of length 2048 shall have a validity period longer than 10 years.

Suggested validity periods for keys are:
Policy CA public signature verification key (2048 bits) and certificate – ten years;
Policy CA private signing key (2048 bits) – seven years;
CA public signature verification key (2048 bits) and certificate – three years;
CA private signing key (2048 bits) – one year;
End Entity public signature verification key (1024 bits) and certificate – two years;
End Entity private signing key (1024 bits) – two years.

Key lengths must be at least 1024 bits and should be determined in organisational Threat-Risk Assessments. Key lengths and validity periods shall be stated in the CPS.

6.4 Activation Data

Any activation data must be unique and unpredictable. The activation data, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected. Where passwords are used, an Entity must have the capability to change its password at any time.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The workstations and servers used in the CA system shall be configured to provide the minimal functionality required to provide the assigned CA or RA services.

The security controls shall provide access control and traceability down to an individual level on all transactions and functions affecting the use of CA's private signing keys as described in the CPS. This functionality may be provided by the operating system, or through a combination of operating system, PKI CA software, and physical safeguards.

Initialisation of the system operating a CA's private signing keys shall require co-operation of at least two operators, both of which are securely identified by the system. A detailed log must be kept manually over all important steps of the initialising process.

Activation of a CA's private signing keys shall meet requirements stated in 6.2.2

Registration of initial authorisations for a Certificate Management System shall be done in the presence of a security officer (CASO) and one operator (CAO). A record of the configuration procedure shall be signed by each of the participants, and then filed.

The CPS shall include a description of significant security measures for the CA system.

6.5.2 Computer Security Rating

The Certificate Management System (CMS) does not require a formal rating as long as it fulfils all requirements in section 6.5 (this section).

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The CMS and cryptographic modules used must have been developed using well established techniques and methodology and shall be well tested.

6.6.2 Security Management Controls

The configuration of the CMS as well as any modifications and upgrades must be documented and controlled.

The PMA shall be notified of significant changes.

6.7 Network Security Controls

The CA system must be protected from attack through any open or general purpose network with which it is connected. Such protection must be provided through the installation of a device configured to allow only the protocols and commands required for the operation of the CA.

A CA must ensure that its CPS defines those protocols and commands required for the operation of the CA.

Communication to and from a CMS, operating a CA's private certificate signing key, over an external network requires establishment of an encrypted channel of sufficient strength.

6.8 Cryptographic Module Engineering Controls

No stipulation.

6.9 Life-Cycle Security Assurance

The code that makes up the CMS shall be integrity protected by the organisation holding the master copy. The integrity protection shall provide an authentication code on downloads and otherwise delivered software in the form of a hash value or a digital signature, which uniquely match the correctly delivered code. The authenticity of the authentication code must be verified at installation time. If the correct value is not obtained, the software

shall not be installed. The organisation holding the master copy shall be notified of the discrepancy, and a new copy of the software shall be obtained.

The installed executable software shall be integrity protected using a method that is at least as strong as the integrity protection on the downloaded or delivered software. The authenticity of the installed code shall periodically be verified (see the CPS). If the authenticity cannot be verified, the CMS shall immediately be halted, and the CASO of the workstation should be notified. The hash used in the validation process shall be an approved cryptographic-strength hash; e.g., SHA-1.

In no case should the application execute for more than 24 hours without being checked for changes.

There are no life-cycle security assurance requirements imposed on the workstations used by RA's who are simply "information verifier/forwarders".

7 Certificate and CRL Profiles

This chapter specifies the certificate format and the CRL format. Further coding conventions and other specific information regarding the content of required and recommended fields and extensions in certificates and CRLs shall be specified in the CPS.

7.1 Certificate Profile

All PKI End Entity software must support and correctly process the base (non-extension) X.509 fields and extensions identified in chapter 4 of PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [RFC2459] as prescribed in the same document.

7.1.1 Version Numbers

The CA must issue X.509 Version 3 certificates, in accordance with the PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [RFC2459].

The values of the base (non-extension) X.509 fields shall be:

Field	Comment – Content
`version`	Version of X.509 certificate, version is 3 (value is 2)
`serialNumber`	Unique serial number for certificate
`signature`	The OID for the algorithm used by the CA to sign the certificate.
`issuer`	X.501 type distinguished name of CA. It is recommended that the `organizationName` component is included in the name. See 3.1.2
`validity`	The first and last date in the validity period for the certificate
`subject`	See `issuer` above.
`subjectPublicKeyInformation`	The OID of the algorithm for the certified public key and the certified public key itself.
`issuerUniqueID`	not used
`subjectUniqueID`	not used

7.1.2 Certificate Extensions

The following table states extensions that are required, recommended, not recommended and not allowed in certificates complying with this CP. It also states whether each extension shall be marked critical or not:

Extension	Required	Recommended	Not recommended	Not allowed
`authorityKeyIdentifier`	NC			
`subjectKeyIdentifier`	NC			
`keyUsage`	C			
`certificatePolicies`	C			
`policyMapping`				EE, CA
`subjectAltName`		NC		
`issuerAltName`		NC		
`subjectDirectoryAttributes`			NC	
`basicConstraints`	CA/C			EE
`extKeyUsage`		If applicable: EE /NC		
`cRLDistributionPoint`	NC			
`authorityInformationAccess`		NC		

C = critical, NC = noncritical, EE = End Entity certificate, CA = CA certificate.

The following table specifies the values of required certificate extensions and recommends values for some recommended extensions.

Extension	**Comment – Content**
`authorityKeyIdentifier`	Can be used to identify a particular public key when a CA has several. Fingerprint of CAs public key, and serial number of CA certificate.
`subjectKeyIdentifier`	Fingerprint of the subjectPublicKey.
`keyUsage`	End Entity certificate – RSA key: digitalSignature, nonRepudiation, keyEncipherment. CA certificate – RSA key: keyCertSign, cRLSign.
`certificatePolicies`	End Entity and cross-certification certificate: OID, URI of CPS and UserNotice (short explicit text see 2.1.2). CA certificate – OID.
`subjectAltName`	E-mail address is recommended.
`issuerAltName`	E-mail address, and http URI to CA web site are recommended.
`basicConstraints`	CA certificate: true Shall not appear in end End Entity certificates
`cRLDistributionPoint`	URI of CRL.
`authorityInformationAccess`	The id-ad-caIssuers OID: URI of CAs superior to the issuing CA's certificate.

If further extensions are used, their values and whether they are critical or not shall be specified in the CPS.

7.1.3 Cryptographic Algorithm Object Identifiers

The CA must use and End Entities must support, for signing and verification, the following algorithms:
RSA – {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 };
SHA-1 – sha1WithRSAEncryption, {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }.

The CA only issues certificates for keys for these algorithms.

In addition, the CA and End Entities must support the algorithms approved by PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [RFC2459] for verification.

7.1.4 Name Forms

Each DN must be in the form of an X.501 UTF8String.

7.1.5 Processing Semantics for Critical Certificate Policy Extension

Critical extensions shall be interpreted as defined in PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [RFC2459].

7.2 CRL Profile

All PKI End Entity software must support and correctly process the CRL fields and extensions identified in chapter 5 of PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [RFC2459] as prescribed in the same document.

7.2.1 CRL Version Numbers

A CA must issue X.509 Version 2 CRLs, in accordance with the PKIX ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile” [RFC2459]. As a complement to CRLs, the CA may provide an OCSS meeting the requirements of this policy.

The values of the fields and entry fields of the X509 Version 2 CRL shall be:

CRL Field	**Comment – Content**
version	Version of X.509 CRL, version is 2 (value is 1)
signature and signatureAlgorithm	sha-1WithRSAEncryption shall be used by the CA to sign the CRL. OID: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
issuer	See 7.1.1.
thisUpdate	Required
nextUpdate	Required
CRL Entry Field	
userCertificate	Serial number of revoked certificate
revocationDate	Required

7.2.2 CRL and CRL Entry Extensions

All PKI user software must correctly process all CRL extensions and CRL entry extensions identified in PKIX ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile” [RFC2459].

The following table lists CRL extensions and CRL entry extensions that are required, recommended, and allowed in CRLs complying with this CP. It also states whether each extension shall be marked critical or not:

CRL Extension	**Required**	**Recommended**	**Allowed**
authorityKeyIdentifier	NC		
issuerAltName		NC	
cRLNumber	NC		
deltaCRLIndicator			C
issuingDistributionPoint	C		
CRL Entry Extension			
reasonCode	NC		
invalidityDate		NC	

The following table gives the stipulations for the extensions and entry extensions:

CRL Extension	**Comment – Content**
authorityKeyIdentifier	See 7.1.2
issuerAltName	See 7.1.2
cRLNumber	Sequence number of CRL
deltaCRLIndicator	Contains the sequence number of the base CRL if this CRL is a delta CRL. A complete CRL must also be issued.
issuingDistributionPoint	URI of CRL, options allowed.
CRL Entry Extension	
reasonCode	Specified reason codes are strongly recommended.
invalidityDate	Date of known or suspected compromise or invalidation.

8 Specification Administration

8.1 Specification Change Procedures

8.1.1 Items That Can Change without Notification

Contact information.

8.1.2 Changes with Notification

Prior to making any changes to this certificate policy, the PMA will notify the Policy CA and all its subordinate CAs, and all CAs that are directly cross-certified with the Policy CA.

8.1.2.1 List of Items

All items except the contact information in this certificate policy are subject to the notification requirement.

8.1.2.2 Notification Mechanism

The PMA will notify, in writing, all CAs mentioned in 8.1.2 of any proposed changes to this certificate policy. The notification must contain a statement of proposed changes, the final date for receipt of comments, and the proposed effective date of change. The PMA may request CAs to notify their Subscribers of the proposed changes and/or publish them on the CA web sites. The PMA will also post a notice of the proposal on the PMA web site.

The PMA will notify, in writing, all CAs mentioned in 8.1.2 of any changes to this certificate policy.

8.1.2.3 Comment Period

The comment period will be 30 days unless otherwise specified. The comment period will be defined in the notification.

8.1.2.4 Mechanism to Handle Comments

Written and signed comments on proposed changes must be directed to the PMA. Decisions with respect to the proposed changes are at the sole discretion of the PMA.

8.1.2.5 Period for Final Change Notice

The PMA will determine the period for final change notice.

8.1.2.6 Items Whose Change Requires a New Policy

If a policy change is determined by the PMA to warrant the issuance of a new policy, the PMA may assign a new Object Identifier (OID) for the modified policy.

8.2 Publication and Notification Policies

This policy definition, digitally signed by an authorised representative of the CA, can be obtained:
on the PMA web site: http://www.swupki.su.se
in electronic form via e-mail from info@swupki.su.se

CAs issuing certificates that identify this certificate policy shall post copies of this CP on their CA web site.

8.3 CPS Approval Procedures

Accepting the level-one CA of a new member of SwUPKI amounts to, among other things, approving its CPS. This must be in accordance with procedures specified by the PMA. Where a CPS contains information relevant to the security of a CA, all or part of the CPS need not be made publicly available.

REFERENCES

[RFC2119] IETF, Network Working Group, S. Bradner, ”Key words for use in RFCs to Indicate Requirement Levels”, Request for Comments: 2119, March 1997. Available at: http://www.ietf.org.

[RFC2459] IETF, Public-Key Infrastructure (X.509) Working Group. R. Housley, W. Ford, W. Polk, D. Solo, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”, Request for Comments: 2459, January 1999. Available at http://www/ietf-org.

[RFC2510] IETF, Public-Key Infrastructure (X.509) Working Group. C. Adams, S. Farrell, “Internet X.509 Public Key Infrastructure Certificate Management Protocols”, Request for Comments: 2510, March 1999. Available at http://www/ietf-org.

[RFC2527] IETF, Public-Key Infrastructure (X.509) Working Group. S. Chokhani, W. Ford, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, Request for Comments: 2527, March 1999. Available at http://www/ietf-org.

[X509] ISO/IEC 9594-8, *Information Technology—Open Systems Interconnection—The Directory: Authentication Framework*. Also published as ITU-T X.509 Recommendation. For X.509 v3 certificates, see edition ITU-T Rec. X.509 (1993 E) or ISO/IEC 9594-8:1995 with Technical Corrigendum 1 and Amendment 1 (Certificate Extensions) applied.