Certificate Practice Statement (CPS) for SwUPKI Policy CA

Revision history:

Version	Date	Comment
1.0	2001-02-08	Initial release

1 Introduction

This is the Certificate Practice Statement (CPS) for SwUPKI Policy CA. It states the practices the CA employs in issuing and managing certificates. The CPS outlines the technical, procedural and personnel policies and practices of SwUPKI Policy CA. The numbering of chapters and sections is the same as in the SwUPKI CP, see below. Only the sections where practices are added are present in the CPS.

1.2 Identification

This is the CPS of the SwUPKI Policy CA, a member of SwUPKI (Swedish Universities' and University Colleges' Public Key Infrastructure). The CPS has been approved by the PMA of SwUPKI on 2001-02-08.

The CPS is published at URL:http://www.swupki-pca.umu.se/CPS.

As a member of SwUPKI, the SwUPKI Policy CA is operating in compliance with the CP of SwUPKI:

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)}

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

1.3.4 Repositories

See 2.6.

1.3.5 Sponsors

The SwUPKI PMA is the sponsor of Subscribers of CA certificates issued by SwUPKI PCA.

The CASO is the sponsor of certificates for persons and IT-systems involved in the operation of the PCA.

1.4 Contact Details

Questions regarding this CPS should be addressed to:
SwUPKI Policy CA, Umeå universitet, SE 90187 Umeå, Sweden or pca@swupki.su.se.

Further information may be found at URL: http://www.swupki.su.se/.

2 General Provisions

2.1.4 Subscriber Obligations

The Subscriber Agreement can be found at the PMA web-site http://www.swupki.su.se/.

2.6 Publication and Repository

The SwUPKI Policy CA website is http://www.swupki-pca.umu.se

The CRL repository contains X.509 version two (2) CRLs in accordance with the PKIX "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" [RFC2459] in {DER,PEM} format on

http://swupki-pca.umu.se/CRL/crl-v2.der

http://swupki-pca.umu.se/CRL/crl-v2.pem

3 Identification and Authentication

3.1.2 Need for Names to Be Meaningful

The `organizationName` component is included in the DN and shall be the official name of the organisation. The structure of the name for CA certificates shall be:

C=*Country Code*, O=*Official name*, CN=*Official name CA*

3.1.7 Method to Prove Possession of Private Key

The generation of the private key for CA certificates is done during the initial inspection and supervised by the PMA representatives.

For other certificates, requiring a PKCS #10 request for the certificate proves the possession of the private key.

3.2 Authentication for Routine Renewal of Certificates

Online renewal requests shall be signed by the Subscriber's private key with the valid private key of the Subscriber.

3.4 Authentication of Revocation Request

Revocation of certificates may be conducted after communication with the PMA, the Subscriber, CAO or CASO.

•Written request (on paper).

•Trusted electronic request (PKCS#7).

•Other trusted communication from the above.

A CAO must authenticate a request for revocation of a certificate.

4 Operational Requirements

4.1 Application for a Certificate

Information on the requirements for joining SwUPKI can be found on the URL:

http://www.swupki.su.se/

The PMA will approve the application after necessary inspection. The PMA will supervise the generation of the private key. The Subscriber then generates a PKCS#10 request for a CA Certificate. The PMA approves the request by signing it with the private key of the SwUPKI PMA and then delivers the request to the PCA. The transportation of the signed request from the PMA to the PCA can be either electronical or manual.

4.4.4 Revocation Request Grace Period

The revocation shall be done within 2 (two) workdays. Any other action taken as a result of a request for revocation of a certificate must be initiated within the same time limit.

4.4.7 CSS Publishing Frequency

If a certificate is revoked, the on-line CRL shall be update during the same work day.

4.5.1 Types of Event Recorded

The SwUPKI PCA personnel shall log the following in a manual log:

•Access to the CA machine: Who, why and what.

In addition to this, standard machine logs (syslog, messages) shall be kept.

4.5.2 Frequency of Processing Audit Log

The CASA shall periodically review the audit logs an note significant events in an audit log summary.

4.5.6 Audit Collection System

See 4.5.1

4.6 Records archival

The second backup mentioned in CP 4.6 is kept on removable media in a separate location. They are put in a box, whose key are kept by CAO #1 and #3 (see below). This box is put in a safe. Keys to this safe are kept by CAO #2 and #4. These secondary backups are kept on a bi-weekly basis (if changes have occured).

4.8.2 Entity Public Certificate Is Revoked

In the event of SwUPKI Policy CA private key compromise, or suspected compromise, the PCA operators must try to contact the PMA and subscribers with any possible means until contact is reached.

5. Physical, Procedural and Personnel Security

5.1.1 & 5.1.2 Site Location, Construction and Physical Access

The SwUPKI PCA site is placed in a locked cage in UMDAC's computer hall. The access to the hall is limited to selected staff members of UMDAC. Furthermore, the access to the cage inside the computer hall is even more restricted to selected staff members.

The CA system consists of a PC running Linux with OpenSSL.

The SwUPKI's private key will be stored on removable media. When not in use, the private key is locked up in a safe. Access to the safe must be requested from the UMDAC operators and logged by them. The key to the safe itself is kept by CAO #1 and CAO #2.

The SwUPKI PCA web site is placed on a networked machine and located in UMDAC's computer hall. It will be monitored for intrusion attempts and misuse by intrusion detection programs.

5.2.2 Number of Persons Required per Task

CASO: 1

CAO: 4

The CAO:s will be numbered #1, #2, #3 and #4.

The password to the PCA private key is divided in two parts. CAO #1 and CAO #2 are in possession of the first part and CAO #3 and CAO#4 are in possession of the second part.

CASA: 1

6 Technical Security Controls

6.1.6 Public Key Parameters Generation

The value of the exponent of the public (RSA) key shall be 3 or 65537 for End Entities, while it shall be 65537 for the CA and its trusted personnel.

6.2.1 Policy CA Private Signing Key

The SwUPKI PCA private key will be stored on a removable media and kept in a locked safe while not in use. All access to the SwUPKI's private key must be logged.

6.5.1 Specific Computer Security Technical Requirements

See 6.2.1

6.7 Network Security Controls

The SwUPKI PCA Certificate Management System is not connected to the network.

6.9 Life-Cycle Security Assurance

The installed executable software and the configuration files are verified at every login.

The SHA-1 checksums shall be kept on a removable media.

Appendix: CA Personnel

CASO: Karoline Westerlund

CAO: #1 Einar Hillbom
#2 Maria Magnusson

#3 Lena Timner
#4 Joakim Nyberg

CASA: Einar Hillbom