Ragmi Jusufi 4 February 2008

AdminPKI – CP/CPS Class CD-T01

Certificate Policies and Certification Practice Statement for AdminPKI AdminCA-CD-T01

OID: 2.16.756.1.17.3.21.1

Project Name:	**Class CD-T01**
Project No:	
Version:	**V 1.0**

Status	in progress ☒	at checking stage ☐	approved for use ☐

Persons involved	
Authors:	Jusufi Ragmi, Christoph Grossmann
Approval:	Peter Balsiger
Users:	Subscribers, employees of AdminPKI, auditors, third parties
For information:	-

Change control, checking, approval			
When	**Version**	**Who**	**Description**
14.12.2007	X0.1	Ch.Grossman	Initial Draft
19.12.2007	V0.1	R.Jusufi	Revision
03.01.2008	V0.5	R.Jusufi	Additions
10.02.2008	V0.6	A.Zürcher/ Ch.Grossman	Review
06.03.2008	V0.7	R. Jusufii	Changes based on internal review

Management Summary

This document describes the Certificate Policies (CP) and the Certification Practice Statement (CPS) of AdminCA-CD-T01 at the Swiss Federal Office of Information Technology, Systems and Telecommunication (FOITT) [*Bundesamt für Informatik und Telekommunikation* (*BIT*)]. It describes the procedures used by the Certification Authority AdminCA-CD-T01 to issue certificates of classes C/C-Trustcenter and D.

Table of Contents

1 Introduction

1.1 Overview

This document describes the Certificate Policies (CP) and the Certification Practice Statement (CPS) of AdminCA-CD-T01 at the Swiss Federal Office of Information Technology, Systems and Telecommunication (FOITT) [*Bundesamt für Informatik und Telekommunikation* (*BIT*)]. It describes the procedures[1], used by the Certification Authority AdminCA-CD-T01 to issue certificates of classes C/C-Trustcenter and D.

This Statement was prepared for the Certification Authority, for the PKI Manager, for the employees of AdminCA-CD-T01, for the persons authorised to use the registration applications, for the persons responsible in the authorities that possess a certificate, and for the certificate users who rely on a certificate.

The customers of the Certification Authority are authorities[2] in the federal administration, or local authorities at cantonal or municipal level.

A separate Certificate Policy (CP) has not been created for AdminCA-CD-T01. The relevant information is included in this Statement.

The CPS is based on the specifications of RFC 3647 [3].

When AdminPKI is designated as the holder of rights and obligations, this means the Swiss Confederation represented by FOITT (*BIT*).

1.2 Identifying information

This document bears the title: "Certificate Policies and Certification Practice Statement for AdminPKI AdminCA-CD-T01"

The object identifier (OID) of this document is: 2.16.756.1.17.3.21.1.

The identification tree diagram ({2 16 756}) is managed by the Swiss Federal Office of Communication (*BAKOM*) and is divided into 8 sheets [19]). Sheet {2 16 756 1 n} displays the organisation names in line with recommendation F.500 from the ITU [20].

The identifier {2 16 756 1 17} indicates the organisation name *Admin*, which was assigned to the Swiss Federal Office of Information Technology, Systems and Telecommunication [*BIT*].

[1] The Certification Practice Statement (CPS) is a detailed description of how the services are implemented and of the processes for managing the certificates. The CPS is more detailed than the Certificate Policies (CP) used by the Certification Authority (CA). A Certificate Policy represents a certain level of security for the certificates managed under this CP. The Certification Practice Statement provides information on how the Certification Authority ensures this level of security.

[2] Any users of IT applications in the federal administration, or local authorities at cantonal or municipal level, which must use certificates for these IT applications, may also be customers of Admin-CA-CD-T01.

AdminPKI manages sheet {2 16 756 1 17 3}.
The marker 21.1. at the end of the OID indicates the CP/CPS of AdminCA-CD-T01.

1.3 PKI participants

1.3.1 Certification Authorities

The Certification Authority AdminCA-CD-T01 is part of AdminPKI and issues digital certificates of class C/C-TrustCenter and class D. AdminCA-CD-T01 is a self-signed certificate and is published by AdminPKI. Publication enables the validity of all the certificates issued in this hierarchy to be checked.

The purpose of AdminCA-CD-T01 is to issue user/organisation certificates and device/server certificates of classes C/C-TrustCenter and D. These are soft certificates and do not use any Secure Signature Creation Device (SSCD). A certificate of class C/C-Trustcenter is issued for natural persons and organisations and can be used for signing purposes, encryption, and authentication. Class D certificates are only for authentication.

The certification infrastructure duties of AdminPKI are:

- Adherence to and application of the provisions of this document
- Adherence to and application of the provisions of the framework agreement and the agreement between AdminPKI and its customers
- Application of the technical and human resources required to use the infrastructure
- Protecting the integrity and confidentiality of its own signature, authentication and encryption keys
- Use of its own signature, authentication and encryption keys only for the purposes for which they were issued and using the tools that are specified in this document
- Maintaining a log book of physical accesses and restriction of access to a known group of persons
- Guaranteeing the reliability of the following procedures:
    - Registration of the certificate applicant
    - Issue and revocation of certificates
    - Publication of the list of revoked certificates.
- If required, use of all available means to inform subscribers about cancellation of the certificate for a component of the infrastructure.

1.3.2 Registration Authority

The Certification Authority AdminCA-CD-T01 operates a central Registration Authority (RA), which is accessible to authorised persons at all times through a Web-based registration application.

Persons authorised to create certificates include, for example, for C-Trustcenter certificates, the Chief Officer or a person to whom he has delegated the duty, for C-group mailbox certificates, the person responsible for the e-mail address or his deputy, or for class D certificates, the person responsible for the application or deputies appointed by him.

The authorised person makes a request to AdminPKI for himself and a deputy to be admitted to the registration application for the relevant domain.
AdminPKI examines requests to register authorisations for the registration application. It grants the authorisations if all the required documents have been submitted.

The duties of the Registration Authority or authorised persons include:

- Identification and authentication of certificate applicants
- Initiation of operational requests. These involve:
    - Registration
    - Issue of the certificate
    - Revocation of the certificate
- Certificate renewal.

The registration application is operated by an administrative unit (federal, cantonal or municipal administration). A framework agreement and a SLA govern the relationship between AdminPKI and the authorised person/administrative unit.

The obligations of the authorised persons are:

- Adherence to and application of the provisions of this document
- Adherence to and application of the provisions of the framework agreement and the agreement between the authorised persons and AdminPKI
- Application of the technical and human resources required for use of the components
- Protecting the integrity and confidentiality of their own signature, authentication and encryption keys
- Use of their own signature, authentication and encryption keys only for the purposes for which they were issued, and using the tools that are specified in this document
- Adherence to legislation with regard to handling and maintaining personal data
- Guaranteeing the reliability of the registration procedure. This involves in particular:
    - Checking the data of the certificate applicant

  - Transferring a certificate issue request to the Certification Authority

- Informing the applicant of his rights and obligations
- Secure delivery of the P-12 file and password (which is required to open the P-12 file) to the applicant
- Checking the authenticity of a revocation request

1.3.3 Certificate owners

Certificate owners act on behalf of an administrative unit (federal, cantonal or municipal administration) within the context of the relevant application.

Certificate owners are any natural persons or legal entities or organisational units that own certificates from the Certification Authority AdminCA-CD-T01.

The special obligations of the certificate owner are:

- Adherence to and application of the provisions of this document
- Use of his keys with the applications approved by AdminPKI
- Possessing the basic knowledge required for appropriate use of the keys and certificates
- Ensuring sole control over his keys and of the activation code for the software certificate (password for the software certificate)
- Taking the precautions required to prevent loss or theft of the certificates
- Immediately notifying the authorised person or AdminPKI if he knows or suspects that his private key has been compromised
- Arranging revocation of his certificate if the information contained in it is not/no longer valid.

If the software certificate is passed on, the certificate owner surrenders this security attribute on his own responsibility.

1.3.4 Certificate users

A certificate user is a corporate body or a natural person or legal entity that uses a certificate within the scope of an application. A certificate user does not necessarily have to possess its/his own certificate.

The applications employed by the user must check the certificates in accordance with the checking procedures of the certification methods provided in recommendation X.509 of ITU-T [6].

1.3.5 Other participants

Employees who provide information on certificate applicants (e.g. Personnel Service) and System Administrators or IT employees (technicians) who operate the installations and conduct tests on the systems of the certificate users.

1.4 Use of certificates

1.4.1 Approved use of certificates

Certificates issued by AdminPKI may only be used in conjunction with applications approved by AdminPKI. The certificates are used for authentication, digital signature and encryption in different applications, depending on the settings of the attributes for key usage and the stipulations of this CP/CPS. Class D certificates are only used for authentication.

AdminPKI publishes a list of approved applications on its information site (http://www.pki.admin.ch).

1.4.2 Prohibited use of certificates

Certificate owners/users are not permitted to use their certificates for purposes other than those described in section 1.4.1.

1.5 Management of the document / contacts

1.5.1 Responsibility for the Statement

AdminPKI is responsible for the content, management and publication of this document.

1.5.2 Contact person

The contact person is the AdminPKI Manager:

Swiss Federal Office of Information Technology, Systems and Telecommunication [*BIT*]
AdminPKI Manager
LZEPS
Monbijoustrasse 74
CH-3003 Berne, Switzerland

pki-info@bit.admin.ch

1.5.3 Maintenance of the Statement

The AdminPKI Security Officer may make typographic changes to this CPS or reformulate sections without changing the content and publish such amendments. The AdminPKI Manager is informed subsequently of the changes and can then lodge objections.

Relatively major changes or new versions of the document always require the approval of the AdminPKI Manager.

1.5.4 Responsibility for recognising a CPS

This CP/CPS remains valid until revoked by the responsible body (see section 1.5.1). It is updated as required, in which case it receives a new ascending version number.

1.6 Glossary and abbreviations

1.6.1 Glossary

Certification Services Provider (CSP) or Certification Authority (CA)	Body which confirms data using electronic means and which issues digital certificates for this purpose. Trust authority which issues and manages certificates with a public key and lists of suspended and revoked certificates that comply with recommendation X.509.
Certification Practice Statement (CPS)	Statement of the rules and practices that are effectively implemented by the Certification Services Provider for issuing certificates. The CPS defines the arrangements, policy and procedures that are used by the Certification Services Provider in accordance with its selected certificate policy.
Admin Directory	Meta-directory of the federal administration, in which the certificates and lists of revoked certificates are published and archived.
User of the certificate	Natural person or legal entity or process who/which relies on the verified electronic signatures when using the certificate.
Digital certificate	Electronic certificate which links a signature verification key with the name of a person.
Electronic signature or signature	Data in electronic form, which is attached to other electronic data or is linked logically with it, and which is used to authenticate this data.
Generating the certificates	Service provided by the Certification Services Provider; creation of a digital certificate on the basis of the name of the applicant for a certificate and any of the applicant's attributes that are checked at the time of registration.
Owner of the certificate	Natural person or legal entity or organisation that is the owner of a certificate. This person acts on behalf of an administrative unit (federal, cantonal or municipal administration) within the context of the relevant application.
PKCS#12	De facto standard of the company RSA Security, which defines the format for storing and transmitting asymmetrical key pairs, the corresponding certificates and other electronic key resources.

Registration Authority	Person or organisation responsible for identifying/authenticating a subscriber before certificates are issued to him, but which does not sign or issue any certificates.
Classes of certificates	The federal administration has defined various certificate classes, identified by a letter from A to D. The certificate classes differ with regard to the method for identifying the certificate applicant, the certificate holder and extension of key use.
Certificate	Public key of a subscriber as well as other related information that is signed numerically with the private key of the Certification Authority that issued the certificate. The format of the certificate complies with recommendation X.509.
Certificates of class C/C-Trustcenter and D	These are soft certificates and do not use any Secure Signature Creation Device (SSCD). A certificate of class C/C-Trustcenter is issued for natural persons and organisations and can be used for signing purposes, encryption and authentication. Class D certificates are only for authentication.
Qualified certificate	Digital certificate that meets the requirements of Art. 7 of the Electronic Signature Act (*ZertES*).
Activation password	A software certificate is cryptographically protected and can only be activated for use by means of a password.
Registration	Service provided by the Certification Services Provider, consisting of verifying the identity and, if necessary, the attributes of each applicant of a certificate before the applicant's certificate is created or the activation data (or the password) is assigned for activating use of the keys.
Certification Service Provider	Organisation which certifies data using electronic means and which issues digital certificates for this purpose.
Object identifier	Unique alphanumeric identifier that is registered in accordance with international standards in this area, to identify a particular object or class of objects.
Public Key Infrastructure (PKI)	Complete compilation of guidelines, processes, environments, servers, programs and workplaces that is used to manage the certificates and keys.

Integrity of the data	Assurance that the data is not altered between being created and being received.
Certificate Revocation List (CRL)	List that is kept up to date by the Certification Authority and which contains the numbers of the certificates that were invalidated (revoked) prior to the expiration date.
Sedex (Secure data exchange)	The Sedex platform provides subscribers with services for secure data exchange. Using public key technology, all content data is protected against viewing and alteration by third parties over the whole transmission route between two subscribers.
Service Level Agreement (SLA)	A written agreement between a service provider and the recipient of the service, documenting agreed service levels for a service. A SLA stipulates which products the recipient receives at the standard service level. It also defines the volume, the transfer price and any quality agreements that are higher than the standard.
Security guidelines	Security guidelines are a compilation of rules and directives that were created on the basis of a risk analysis. Their purpose is to reduce the probability of incidents (preventative measures) and to mitigate the effect of incidents (corrective measures), in order to safeguard the resources that are considered to be critical for the provider of electronic certification services. Specifying a strategy and guidelines for security enables the global security level to be clearly defined for an information system and particularly for each element of the security architecture.
Publication	Operation involving providing a certificate to a third party (user) to enable him to verify an electronic signature.
Renewal of a certificate	Operation that is carried out on the request of a subscriber or at the end of the period of a certificate's validity, involving creating a new certificate for the subscriber. The creation of a new certificate after cancellation is not a renewal.
Certificate Policy (CP)	Set of rules prescribing the applicability of a certificate for a particular group of people and/or a class of special applications with shared security requirements.

1.6.2 Abbreviations

ABBREVIATION	MEANING
CA	Certification Authority
RA	Registration Authority
UPS	Uninterruptible Power Supply
DSA	Digital Signature Algorithm
CB	Certification Body
DN	Distinguished Name
CPS	Certification Practice Statement
CSP	Certification Service Provider
FIPS	Federal Information Processing Standard
PKI	Public Key Infrastructure
OID	Object Identifier
ARL	Authority Revocation List
CRL	Certificate Revocation List
PIN	Personal Identification Number (PIN)
BAKOM	Federal Office of Communications [*Bundesamt für Kommunikation*]
BIT	Federal Office of Information Technology, Systems and Telecommunication (*BIT*)
CP	Certificate Policy
PKCS	Public Key Cryptography Standard
PKIX	Public Key Infrastructure (in accordance with X.509 standard)
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman
SAS	Swiss Accreditation Service
Sedex	Secure data exchange
SHA-1	Secure Hash Algorithm
SLA	Service Level Agreement
ITU	International Telecommunication Union

2 Information Service and Directory Service

2.1 Publication and Archiving Service

AdminPKI certificates and the lists of revoked certificates are published and archived in the electronic meta-directory *Admin-Directory*. *Admin-Directory* is a Directory Service in accordance with the X.500 standard from ITU-T [5].

The Intranet version of the Directory Service *Admin-Directory* is accessible from the Intranet network of the Swiss federal administration at the address www.directory.admin.ch or using the LDAP protocol (port 389).

The public version of *Admin-Directory* (*Admin-Directory Public*) is accessible from the Internet (LDAP protocol). The public version only contains a portion of the data held in the Intranet version.

2.2 Information Service

The purpose of the Information Service is to publish:

- the Certification Practice Statement of the Certification Authority *AdminCA-CD-T01* (this document)
- the registration directive of authorised persons
- the certificates of the Certification Authorities
- the Certification Revocation List (CRL)
- any amendments and/or additions affecting the Certification Authorities
- the list of approved applications for electronically signing documents
- the link to the list of revoked certificates
- the link to legal documents
- the URL of the Swiss Accreditation Service (SAS)
- the URL of the Classified Compilation of Swiss Federal Legislation (laws and ordinances passed by the Swiss Confederation)

The service can be accessed at the address http://www.pki.admin.ch/.

2.3 Updating the information

The dates for publication of the documents assigned to AdminPKI coincide with the date of entry into force.

AdminCA-CD-T01 updates its ARL at least once a year and immediately after it has cancelled a certificate.

AdminCA-CD-T01 updates its CRL at least every 7 days, and immediately after revocation of a certificate.

AdminPKI does not offer any online service (OCSP) to verify the validity of a certificate.

2.4 Access to the information

With the exception of personal data that is assigned to applications, 'read' access from the network of the federal administration exists for all data in the Intranet version of the *Admin-Directory*.

It is possible to access any data in *Admin-Directory Public* from the Internet. *Admin-Directory Public* is a partial mapping (DISP protocol) of the Intranet *Admin-Directory*.

3 Identification and authentication

AdminCA-CD-T01 delegates the tasks of identification and authentication of certificate applicants to the authorised persons (see section 1.3.2).

This section describes the practices that are prescribed by *AdminCA-CD-T01* and are observed by the authorised persons to identify and authenticate certificate applicants.[3]

3.1 Allocation of a name

3.1.1 Form of name

In each certificate issued by the Certification Authority *AdminCA-CD-T01* (see section 1.3.1), the issuer and the subject are identified by means of a distinguished name (DN). The DN, which has the form of a printable[4] and non-empty X.501 string, must meet the requirements of technical directive I006 (DT20) of the Federal Strategy Unit for IT [*ISB*] [9].

3.1.2 Information value of names

See technical directive I006 (DT20) of the Federal Strategy Unit for IT [*ISB*] [9].

The certificates bind the public key of a person/organisation to his/its identity information. As a result, other subscribers can be sure that particular public keys belong to a particular identity in each case.

The name must uniquely identify the certificate owner and exist in the "common name" (CN) of the certificate.

Some examples:

DN for group mailbox certificates: cn='Organisation name', [ou = …,] ou=group email boxes, ou=egovservices, o=admin,c=ch

DN for sedex: cn=123456789,ou=identities,dc=<domain-name>,dc=admin,dc=ch
(Subject DN an authority (e.g. municipality of Belp) is given a (fictitious) ID, e.g.123456789)

3.1.3 Anonymity and pseudonyms

The use of pseudonyms requires the approval of *AdminCA-CD-T01*.

[3] Certificate owner: see 1.3.3

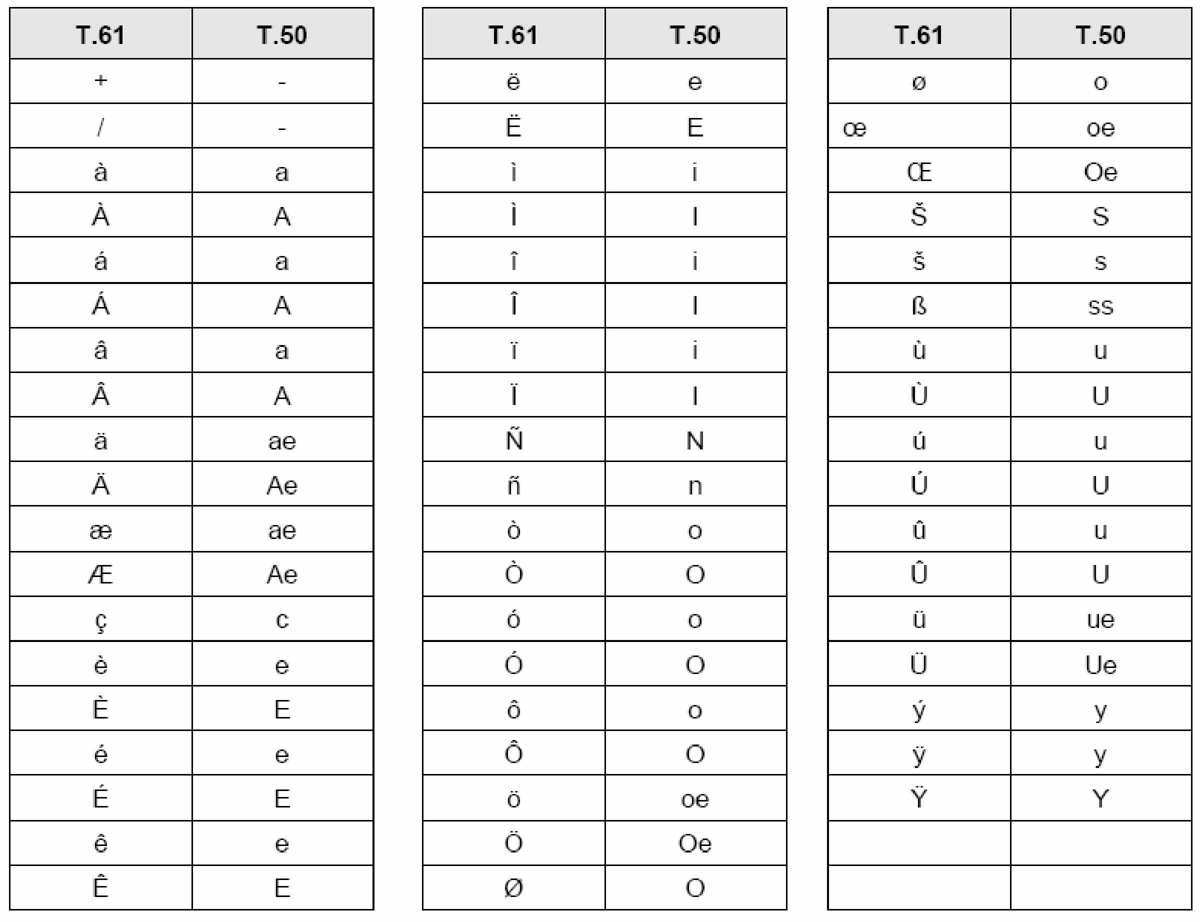
[4] T50 character set

If certificates with pseudonyms are created, the Certification Authority must retain the real identity of the certificate owner in its documentation.

3.1.4 Rules for interpreting the various forms of name

Permitted characters are: a-z A-Z 0-9 ' ( ) + , - . / : = ? space.

Please refer to the table below to convert special characters in the T.61 character set into the T.50 character set.



T.61	T.50	T.61	T.50	T.61	T.50
+	-	ë	e	ø	o
/	-	Ë	E	œ	oe
à	a	ì	i	Œ	Oe
À	A	Ì	I	Š	S
á	a	î	i	š	s
Á	A	Î	I	ß	ss
â	a	ï	i	ù	u
Â	A	Ï	I	Ù	U
ä	ae	Ñ	N	ú	u
Ä	Ae	ñ	n	Ú	U
æ	ae	ò	o	û	u
Æ	Ae	Ò	O	Û	U
ç	c	ó	o	ü	ue
è	e	Ó	O	Ü	Ue
È	E	ô	o	ý	y
é	e	Ô	O	ÿ	y
É	E	ö	oe	Ÿ	Y
ê	e	Ö	Oe		
Ê	E	Ø	O		

3.1.5 Uniqueness of the names

AdminCA-CD-T01 allocates a unique value to the owner of the certificate in accordance with the stipulations of technical directive I006. This value consists of the surname and first name (or the name of the organisation or ID of an authority) of the certificate applicant and a hash code. In the case of the federal administration the hash code is obtained using the Personnel No. At canton level the hash code is obtained using a number issued by the canton, and possibly by means of a number issued by the municipal authority, as well as using the Personnel No.

If a legal dispute arises with another user due to the name that is to appear on a certificate, the Registration Authority at which the certification was applied for informs *AdminCA-CD-T01* about this legal dispute. AdminPKI is responsible for settling this legal dispute.

3.1.6 Identification, authentication and function of trademarks

Irrelevant.

The certificate owner receives no information with regard to a trademark.

3.2 Initial registration

3.2.1 Proof of owning a private key

The private key and the certificate are downloaded by the authorised person (see section 1.3.2) of the registration application in a PKCS#12 file, and forwarded for installation to certificate applicants or technicians (for organisation certificates) by encrypted e-mail or on diskette/CD, via a software distribution system, or through private shares. The activation password is notified to the certificate applicant/technician by other means (e.g. new e-mail, phone, fax, in writing, etc.). The PKCS#12 file is installed on the local machine. As a consequence the private keys are in the possession of the certificate owner.

Since the PKCS#12 file can be copied like any other file, a backup copy can simply be made and held at a secure location (for the eventuality that the software needs to be re-installed on the machine).

The same software certificate can be installed on more than one machine. If the software certificate is passed on, the certificate owner surrenders this security attribute on his own responsibility. In the event that the AdminPKI infrastructure is misused by using a copy of the software certificate, the original owner may be investigated and held responsible.

The activation password, which enables use of the keys to be activated, is exclusively in the possession of the certificate applicant/owner.

3.2.2 Authentication of an administrative unit

The certificate contains information with regard to the subscriber's authorisation to represent a particular legal entity.

3.2.3 Authentication of the certificate applicant

In order to guarantee the correctness of the link between a pair of cryptographic keys, or more accurately between a public key and a certificate owner, the authorised persons must satisfy themselves as to the identity of the certificate applicant.

The task of identifying the certificate applicant and compiling the information required to issue a certificate is delegated to the authorised person.

The authorised persons must:

- check the content of the Web form for applying for a certificate
- check whether the applicant is subject to registration in the Directory Service *Admin-Directory*
- satisfy themselves that the name of the applicant in the Directory is identical with the name in the certificate application form[5]

3.2.4 Unverified data

All the information required to identify the applicant is verified. No further information is verified by the authorised persons of the registration applications.

3.2.5 Signatory power

In the case of a certificate application on behalf of an organisation or legal entity, the applicant must present a valid power of attorney issued by the organisation or legal entity.

3.2.6 Cross-certification (recognition)

A Certification Authority is not authorised to recognise other Certification Authorities (cross-certification).

3.3 Certificate renewal (re-key)

The procedure for renewing a certificate is identical to the procedure for obtaining the first certificate.

3.4 Authentication of a revocation request

The procedure for applying for revocation is described in section 4.9.3. A subscriber can apply for cancellation of his certificate:

- by speaking personally to the authorised person(s)
- by sending his application for revocation by post to the authorised persons
- by e-mail, by signing his application for revocation using his signature key, provided the application for revocation is not being lodged due to any compromise of data on signature creation or any suspicion of compromise, or due to loss or theft of such data

[5] Admin-Directory does not accept any special characters from the T.61 character set. Before comparing names, the authorised person for the registration application must convert the special characters in accordance with the rules for interpreting the various forms of name (see section 3.1.4). In case of doubt the authorised person must refer to the AdminPKI Security Officer.

- by referring to the Service Desk of the Federal Office of Information Technology, Systems and Telecommunication [*BIT*]

The authorised person satisfies himself as to the identity and entitlement of the applicant. The authorised person can decide whether the certificates of a certificate owner are to be revoked.

4 Operating requirements for the certificate's life-cycle

4.1 Application for a certificate

4.1.1 Who can apply for a certificate?

Certificates of class C/C-Trustcenter and D may be applied for by members of an administrative unit (federal, cantonal or municipal administration) that have concluded a framework agreement and SLA with AdminPKI.

4.1.2 Registration process

AdminPKI provides a modular Web-based registration application for the registration process, depending on the intended purpose.

The *authorised person* (see section 1.3.2) makes a request to AdminPKI for himself and a *deputy* to be admitted to the registration application for the relevant domain (e.g. sedex, group mailboxes, class D etc.). They may apply for certificates for any persons/organisations and download them. They are responsible for their publication and installation and are obliged to revoke the certificates through the registration application on suspicion of violation of the CP/CPS.

AdminPKI examines requests to register authorisations for the registration application. It grants the authorisations if all the required documents have been submitted.
The registration application is operated by an administrative unit (federal, cantonal or municipal administration). A framework agreement and an SLA govern the relationship between AdminPKI and the authorised person.

The certificate applicant refers to the authorised person with the requirement to obtain a certificate. The formalities are dealt with at this stage (e.g. identification of the person/organisation).

The authorised person then prepares an entry for the person /organisation of the relevant certificate applicant in the federal administration's directory, *Admin-Directory*.

The authorised person uses an AdminPKI class B certificate (strong authentication) to log in to the registration application. After identification/authentication of the certificate applicant, the authorised person carries out the instructions in the registration application. The application generates the cryptographic keys and applies for the certificates from the CA, which generates the certificate and returns it to the registration application.

The authorised person must inform the certificate applicant about his obligations and responsibility with regard to using the certificates.

4.2 Handling the application for a certificate

Additional information is included in the registration directives of AdminPKI for authorised persons.

4.2.1 Identification and authentication of the applicant

The task of identifying/authenticating the certificate applicant is performed by authorised persons. The authorised persons must be satisfied as to the identity of the applicant.

4.2.2 Approval/rejection of the application for a certificate

The authorised person must verify that the application is genuine (checking the application form, checking the data in *Admin-Directory*, checking the identity of the applicant). If the data is incomplete and/or the certificate applicant is not identifiable, the authorised person stops processing the application.

4.2.3 Handling the application for a certificate

The authorised person must:

- verify that the application for a certificate is genuine and check the content and/or accept or reject the application
- verify the identity of the certificate applicant
- initiate the process of generating key pairs
- issue/validate the application for a certificate
- forward the application for a certificate to the Certification Authority for processing

Applications for a certificate confirmed by an authorised person are automatically processed in real-time (from the time of receipt) by the Certification Authority.

The Certification Authority must:

- check that the application for a certificate is genuine and complete
- accept/reject the application
- issue the certificate.

4.3 Issue of the certificate

4.3.1 Steps taken by the Certification Authority during the issuing procedure

Applications for a certificate submitted by an authorised person are automatically processed in real-time by the Certification Authority.

The Certification Authority must:

- check that the applications for a certificate are genuine and complete
- check that the public key to be certified is unique
- issue and validate the certificate by signing it using its signature key
- forward the certificate to the registration application, and make it available for download.

4.3.2 Notifying the applicant regarding issue of the certificate

Issue of the certificate is notified to the applicant by means of an e-mail. The e-mail address indicated in the certificate is used for this purpose.

4.4 Acceptance of the certificate

4.4.1 Acceptance procedure

The certificate and private keys are made available for download through the registration application in the form of a PKCS#12 file.
Depending on whether a natural person or organisation is involved, the P 12 file is passed on to the certificate applicant or technician (see section 3.2.1). The certificate applicant or technician (for organisation certificates) carries out the installation on the local machine.

4.4.2 Publication of the certificate by the Registration Authority AdminCA-CD-T-01

The issued certificates are published in the *Admin-Directory* (accessible from the federal administration network) and in *Admin-Directory Public*.

The public keys of sedex (organisation certificates) are published in the user directory of sedex.
Publication is also possible in other directories on request.

4.4.3 Notifying the issue of the certificate to other authorities

The issue of certificates is notified to the cantonal and municipal administrative bodies that have concluded a framework agreement and SLA with AdminPKI.

4.5 Use of the keys and certificate

The application area for keys and the certificate is stated in section 1.4.

4.5.1 Use of the keys and certificate by the certificate owner

The certificate owners/users are entitled to use their private keys for the applications that have been approved by the AdminPKI Manager and published by the Information Service.

Use of the keys by the certificate owners/users is subject to the following conditions:

- The certificate owner/user must use his private keys for approved applications and for appropriate purposes
- The certificate owner/user possesses the basic knowledge required for correct use of the keys and certificates
- The certificate owner/user must be aware of his responsibility and obligations as stipulated in this document
- The certificate owner/user must retain sole control over his keys.
- The certificate owner/user must take all necessary precautions to prevent the loss, modification or unauthorised use of his keys.
- The certificate owner/user must notify the authorised person or the Service Desk of the Federal Office of Information Technology, Systems and Telecommunication [*BIT*] without delay if he discovers that his private key has been compromised, or suspects that this is the case.
- The certificate owner/user must arrange to have his certificate revoked if the information contained in it is no longer valid.

4.5.2 Use of the certificate by third parties (third-party users)

Use of the certificate by third parties is subject to the following conditions:

- The third party is aware of the content of the CP/CPS
- The third party has the basic knowledge that is necessary to use the certificates correctly
- Before using the certificate, the third party must check its validity in accordance with the procedure for checking the certification methods provided in recommendation X.509 of ITU-T.

4.6 Certificate renewal

The procedure for renewing a certificate is identical with the procedure for initial registration. The authorised person uses the registration application to check the issued certificates for validity. Those users whose certificates expire soon (within the next 30 days) are displayed, so the authorised person can issue new certificates.

4.7 Replacing the certificate

The procedure for replacing a certificate is identical with the procedure for initial registration.

4.8 Changing the content of a certificate

The procedure for changing the content of a valid certificate is identical with the procedure for initial registration.

4.9 Suspending and revoking a certificate

The certificate of the certificate owner may be revoked (withdrawn).

The authorised person immediately establishes the identity of the applicant and/or the correctness of the application and revokes the certificate through the registration application. The revocation is final.

Suspension of the certificate is permitted. The authorised person suspends the certificate through the registration application. The certificate is temporarily declared to be invalid. It may, however, be declared to be valid again at a later point in time. The certificate owner/user may no longer use it for the period of suspension.

4.9.1 Reasons for revocation

The Certification Authority may revoke a certificate for the following reasons:

- The private keys or the activation password have been, or are suspected to have been, compromised
- The correctness of the link between the key and the certificate owner can no longer be guaranteed
- The certificate contains information that is no longer valid
- The certificate owner has obtained a certificate in an improper way
- The certificate owner has been rejected or blocked
- A time limit has expired or a contract has lapsed
- The certificate owner has infringed his obligations or other agreements, requirements or legislation that may be in force

- The administrative unit that is the employer of the certificate owner has not fulfilled its obligations
- The authorised person who has acknowledged the application for a certificate has not fulfilled his obligations
- AdminPKI has discontinued its certification operations.

4.9.2 Who can request revocation?

The Certification Authority accepts revocation applications from:

- the certificate owner
- the authorised person who has issued/acknowledged the application for a certificate
- the administrative unit that is the employer of the certificate owner
- the AdminPKI Security Officer.

The authorised person and the AdminPKI Security Officer must satisfy themselves that the applicant is authorised to apply for revocation.

4.9.3 Procedures for applying for revocation

4.9.3.1 Revocation due to compromise of the signature keys

If the private key of a certificate owner is compromised, the following procedure must be followed:

1. The certificate owner must initiate the revocation procedure. He can submit his application for revocation:

- to the authorised person (during office opening hours)
- to the Service Desk of the Federal Office of Information Technology, Systems and Telecommunication (outside office opening hours)
- by signed e-mail.

2. The authorised person or the Service Desk must verify the authenticity of the application for revocation.

If the application was submitted in an e-mail with a digital signature, the authorised person verifies the authenticity by checking the digital signature.

3. The application for revocation is forwarded automatically through the registration application to the Certification Authority.

4. The Certification Authority is responsible for the revocation applications, which can be checked automatically for authenticity.

5. The Certification Authority automatically informs the authorised person (through the registration application) that the revocation has been carried out.

4.9.3.2 Revocation due to an infringement

If the certificate owner does not fulfil his obligations, the authorised person must revoke the certificates. The procedure for revocation due to an infringement is the same as for revocation due to compromise of the keys (see section 4.9.3.1).

The authorised person accepts revocation applications on the part of the administrative unit that is the employer of the certificate owner, and on the part of the AdminPKI Security Officer.

4.9.4 Time limit for applying for revocation

In the event that a certificate owner's keys are compromised, the certificate owner must apply for revocation of his certificate without delay.

4.9.5 Period for processing an application for revocation

The Certification Authority processes revocation applications, which were checked automatically for authenticity, as soon as they are received.

After each revocation the Certification Authority compiles a list of cancelled certificates and publishes this list promptly in the *Admin-Directory*.

4.9.6 Requirements with regard to checking the lists of revoked certificates

On receiving a signed message, the user is obliged to check the validity of the subject's certificate and the validity of the issuer of the CRL.

4.9.7 Frequency of publishing the CRL and the ARL

AdminPKi updates its ARL once a year if none of the Certification Authority's certificates were cancelled during this period.

The Certification Authority updates its CRL:

- after every certificate revocation
- every 7 (seven) days if no certificate has been revoked in this period.

4.9.8 Time limit for CRL publication

The Certification Authority publishes a new CRL no later than 24 hours after receiving an application for revocation.

4.9.9 Online checking of the list of revoked certificates

The Certification Authority does not offer any online verification service of the type OCSP.

4.9.10 Requirements with regard to online verification

Does not apply.

4.9.11 Other forms of publishing the list of revoked certificates

The Certification Authority does not offer any alternative to the CRL and the ARL.

4.9.12 Exchange of the certificate in the event of the key being compromised

See section 4.7 and section 4.9.3.1.

4.9.13 Suspension of the certificate

Suspension (discontinuation for a period of time) of certificates is permitted, although it is not recommended for organisation certificates.

4.9.14 Who can request suspension?

The Certification Authority accepts suspension applications from:

- the certificate owner
- the authorised person who has issued/acknowledged the application for a certificate
- the administrative unit that is the employer of the certificate owner
- the AdminPKI Security Officer.

4.9.15 Procedure for applying for suspension

If a certificate owner has made his application for revocation and if it is not possible to verify his identity, the certificates are suspended for the time being by authorised persons.

4.9.16 Period of suspension

Certificates may not remain suspended for longer than three (3) working days.

4.10 Service for enquiring about the status of certificates

4.10.1 Operational features

The service for checking the status of certificates is based on the certificate revocation list, CRL. The CRL lists the revoked certificates for which the expiry date has not yet passed. The CRL is published by:

- the directory service *Admin-Directory*
- the Information Service with the address www.pki.admin.ch

4.10.2 Availability of the service

The availability of the service for checking the status of certificates is 99% during office opening hours. Outside office opening hours the service is not guaranteed to be available. In 80% of cases, outage of the certification service may not exceed 24 hours.

4.10.3 Optional features

Options are not available.

4.11 End of contractual relations

The end of contractual relations is governed by the framework agreement and the SLA between AdminPKI and its customers.

4.12 Archiving and Retrieval of keys

The *Key Archive Server* is part of the registration application and works transparently in the background. It stores the certificate applicants' key pairs, enabling lost keys to be reinstated at any time.

The authorised persons do not need to apply for a new certificate. Instead, they may give the certificate owner his existing certificate.

5 Security measures in relation to infrastructure, organisation and personnel

AdminPKI is housed in a protected room and is operated by skilled staff. All the processes for the commissioning and production of certificates by the Certification Authorities operated at the location are defined in detail and, in the case of qualified certificates, have been checked by an independent body. All the construction-related and organisational security measures are documented in a security plan (not publicly available).

5.1 Security measures in relation to infrastructure

5.1.1 Location and construction-related measures

AdminCA-CD-T01 is operated in the specially-protected server rooms of the Federal Office of Information Technology, Systems and Telecommunication.

5.1.2 Access control

Physical access to AdminCA-CD-T01 is regulated in the AdminPKI Access Regulation [22]. Access authorisation is granted by the AdminPKI Manager.

5.1.3 Power supply and air-conditioning

The room in which the certification infrastructure is located is equipped with an air-conditioning system to regulate the temperature and air humidity.

All electrical components are connected to an uninterruptible power supply.

5.1.4 Prevention of water damage

The room in which the certification infrastructure is located is equipped with water detectors, connected to the building's monitoring station.

5.1.5 Fire protection

The room in which the certification infrastructure is located is equipped with smoke detectors and heat detectors, connected to the building's monitoring station.

In an emergency the IT systems of the certification infrastructure are switched off automatically and disconnected from the power supply.

5.1.6 Data carriers

All data carriers holding information related to the certification infrastructure, including backup copies, are held in a fire-proof safe.

5.1.7 Waste disposal

All paper documents and magnetic tapes that are earmarked for disposal are placed in a filing cabinet that is certified for classified documents and destroyed in a controlled manner.

5.1.8 Storage outside the building

AdminPKI has a backup site which can be used, if required, to ensure continuation of operations.

AdminPKI uses two storage facilities for protected data offsite.

5.2 Organisational security measures

The roles in AdminPKI are divided into the following three areas:

□ AdminPKI Verantwortlicher □ Entwicklungsverantwortlicher □ Sicherheitsverantwortlicher □ Serviceverantwortlicher	□ Betrieb □ Operations	□ Fachspezialisten □ Lieferanten

AdminPKI Manager Development Officer Security Officer Services Officer	Operations	Specialists Suppliers

5.2.1 Positions of trust

In order to ensure that critical duties are separated, a distinction is made at AdminPKI between several positions of trust. More than one duty may be assigned to one and the same person, provided it does not impair the security of the services offered.

The positions of trust are:

1. Duties AdminPKI Manager

The AdminPKI Manager represents AdminPKI on the management board of the Federal Office of Information Technology, Systems and Telecommunication [*BIT*]. His principal duties for AdminPKI consist of approving the Security Policies and Certificate Policies and ensuring that the infrastructure is available for use.

2. Duties of the AdminPKI Security Officer

The Security Officer is responsible for applying the policies to ensure the physical and functional security of AdminPKI and its environment. He manages control of physical access to the platform, is authorised to access the archives and he analyses the incident journals.

3. Duties of the AdminPKI Services Officer

The Services Officer is responsible for all the services provided by AdminPKI. His duties include in particular the conclusion of support contracts with suppliers, ensuring the availability of the certification infrastructure and recruiting and training AdminPKI employees.

4. Duties of the AdminPKI Development Officer

The Development Officer is responsible for startup, configuration and maintenance of the AdminPKI IT systems. He ensures there is proper management of the system and of the network for the platform on which the registration, creation and revocation of certificates and the other services provided by AdminPKI are based, either partly or fully.

5. Duties of the AdminPKI Operating Officer

The Operating Officer is responsible for setting up the business organisation, operating the certification infrastructure, as well as carrying out the procedures for backup and, if required, recovery. He is also involved in planning new operations, and implementing adaptations/modifications to the certification infrastructure.

6. Duties of AdminPKI Operations

The Operations staff monitor the operation of the certification infrastructure with the aid of the monitoring infrastructure, carry out certain pre-defined activities on the systems, perform the backup processes and, if required, recovery.

7. Auditor's duties

The auditor (external firm) appointed by BIT's legal service is responsible for conducting regular checks on the applications, Certificate Policies, Certification Practices and the actual provision of services by AdminPKI.

5.2.2 Employees involved in each step

The following table lists the processes that require the cooperation of two persons in order to safeguard functions or sensitive information ("dual control").

Process	**Role I**	**Role II**
Updating signature keys of the infrastructure	Security Officer	Operating Officer
Replacing HSMs (Hardware Security Modules)	Security Officer	Operating Officer

All other duties at AdminCA-CD-T01 are carried out by Operations staff by themselves.

5.2.3 Identification and authentication of the roles

AdminPKI has set up management of access rights in order to identify and authenticate its staff to ensure that actions carried out are in line with their duties.

Physical access to each of the IT systems is regulated by access control measures.

5.2.4 Separation of duties

The Services Officer assigns duties to AdminPKI staff. He ensures that conflicts of interest do not arise.

5.3 Security measures in relation to personnel

5.3.1 Required competencies, qualifications and experience

AdminPKI staff members are employees of the federal administration and are permanent employees. The employees possess the training, expertise, experience and qualifications that are required to provide certification services. Normally they work full-time on the tasks that fall within their area of competence in the context of the certification infrastructure. Each employee is informed by the Services Officer personally about the scope and limits of his area of responsibility.

The employment contract of each employee includes a confidentiality clause.

The authorised persons are employees of an administrative agency (federal, cantonal or municipal administration). These employees are subject to a certification process prior to being employed.

5.3.2 Preparatory checks

Prior to being employed, AdminPKI employees and the authorised persons must undergo a personal security check in accordance with Article 10, Para. 1, point a. of the Ordinance on Security Checks for Persons [13].

5.3.3 Requirements in respect of initial training

AdminPKI employees are trained in the software, hardware and internal operational workflows of the component for which they work. The employees must be familiar with the work for which they are responsible and understand its effects.

5.3.4 Requirements and frequency of training

Each new employee receives initial training in the system, security policy, emergency plan, software and in the job for which he is responsible.

After each major enhancement of the system, organisation, tools and methods, each employee must complete a further training session.

5.3.5 Job rotation

Not applicable at present.

5.3.6 Penalties for unauthorised acts

The penalties that are imposed on an employee of AdminPKI if he abuses his rights or performs acts for which he is not authorised are regulated in the Federal Act on the Responsibility of the Swiss Confederation, the Members of its Official Bodies and their Officers (SR 170.323).

5.3.7 Contracts with temporary staff

The security requirements with regard to temporary employees and the staff of suppliers/external service providers are the same as those that apply to employees of the federal administration (see sections 5.3.1, 5.3.2, 5.3.3 and 5.3.4).

5.3.8 Documentation provided to staff

Staff have access to the entire documentation of AdminPKI and in particular to the following documents:

- the Certification Practice Statement of the Certification Authority *AdminCA-CD-T01* (this document)
- security policy
- operational and organisational manual
- manuals on the hardware and software relating to the system and applications

5.4 Security monitoring

5.4.1 Types of registered events

Events related to the issue and administration of certificates are registered automatically and/or manually for checking purposes.

The following data is registered:

System:

- Operations carried out by AdminPKI on the IT systems
- Prohibited attempts at accessing the networks and IT systems of the certification infrastructure

Certification:

- Registration: registration of a new certificate applicant and request for renewal
- Certificate creation: the Certification Authority, the certificate owner
- Certificate revocation: request for revocation, revocation report
- Operations carried out by AdminPKI: starting and stopping the application, password change, change to the configuration parameters of the certification tool
- Physical access to the key administration centre and other associated facilities
- Destruction of keys, of data relating to activation and of certain other information
- Personnel changes.

The following information is registered per event: date and time of the operation, recipient of the operation, name of the person carrying out the operation, names of persons present, name of the person who requested the operation, result of the event, type of operation, and reason for the event.

5.4.2 Frequency of log file analysis

Log files are checked regularly as part of a daily check in accordance with the policies in the AdminPKI operating manual entitled "Periodic Monitoring of Functions and Activities" [23]. This activity is recorded in writing and initialled by the person performing the check.

5.4.3 Retention period for log files

System-related and application-related log files are held for at least 11 years.

5.4.4 Backup procedure for log files

The log files are stored on a dedicated server. Only authorised and authenticated AdminPKI employees have access to the log files.

The information stored offsite is encrypted.

5.4.5 Monitoring system

The log files are backed up each day as part of AdminPKI's routine backup of the host system.

5.4.6 System for collecting the log files

An internal server of the certification infrastructure collects all the log files.

5.4.7 Notification in the event of serious incidents

The software for analysing the log files automatically informs the Security Officer and the staff responsible for operations in the event of a critical incident.

5.4.8 Assessment of vulnerability

At least once a week a program analyses the components of AdminPKI with the objective of identifying any vulnerabilities and warning of possible attacks on the certification infrastructure.

In the event of critical anomalies, the Security Officer is informed immediately.

5.5 Archiving the certificates and other documents

5.5.1 Data types to be archived

AdminPKI archives all data and log files that relate to the issue and management of certificates. These involve in particular:

- Contractual agreements or arrangements with AdminPKI customers
- Certificates of certificate owners and of components of AdminPKI
- All compiled Certificate Revocation Lists (CRL)
- Revocation applications, if present
- Identification data of certificate owners, all information used for registration and the type of documents that the certificate applicant has submitted
- Log files
- Audit reports
- Incident reports
- Vulnerability analysis reports

5.5.2 Retention period for archives

AdminPKI archives are held for at least 11 (eleven) years.

5.5.3 Protection of the archives

The application logs are signed by the certification application. They are then encrypted before being stored in encrypted form.

Only the Security Officer has access to the archived data.

5.5.4 Procedure for copying the archives

AdminPKI uses two offsite storage/archiving facilities for protected data.

5.5.5 Time-stamp required for archives

Each registered and archived event is date-marked. The time information is provided by a reference clock located in a local IT system. All components of the central AdminPKI infrastructure are synchronised with this clock.

5.5.6 Archiving system

The archiving system is an internal AdminPKI system.

5.5.7 Procedure for retrieving data from the archives

Retrieval or analysis of archive files must be approved by the Security Officer.

5.6 Key modification for an AdminPKI component

The validity of the keys that are used by the components and staff of AdminPKI is monitored by the Services Officer. The creation of new keys and the issue of certificates must be approved by the Security Officer.

Depending on the type of modification (end of the validity period, renewal of the keys due to revocation etc.), the steps taken must be in accordance with the processing procedures described in sections 4.2, 3.2 and 3.3.

New certificates and their fingerprints are published.

5.7 Protection against data being compromised and the disaster-recovery plan

5.7.1 Incident management

The procedure for managing incidents is laid down by the Security Officer and is notified to all employees of the certification infrastructure.

5.7.2 Destruction of IT resources, programs or data

AdminPKI takes all necessary steps to prevent any compromise of data and any theft of information or hardware owned by AdminPKI. In the eventuality of any theft, compromise of data or suspicion thereof, the operations recovery/continuation plan is put into action by the Security Officer.

The certification infrastructure's Security Officer works closely with the IT security officer of the Federal Office of Information Technology, Systems and Telecommunication [*BIT*].

If required, AdminPKI has an emergency facility which can be operational 5 days after the destruction of its facility in Berne.

5.7.3 Compromise of the AdminPKI signature keys

In the event that the Certification Authorities' keys have been or are suspected to have been compromised, the AdminPKI Manager is informed immediately. After analysing the situation, the AdminPKI Manager puts into action, if necessary, the procedure to revoke all the relevant certificates of the certificate owners. The following steps are taken:

- Informing the certificate owners
- Informing the Swiss Accreditation Service
- Revoking the certificates of the Certification Authority and certificate owners
- Creating new signature keys for the Certification Authority
- Informing the authorised persons
- Issuing new certificates to the previous certificate owners.

5.7.4 Continuity plan

AdminPKI's continuity plan is used after a disaster. The purpose of the continuity plan is to ensure availability under the same original conditions for the basic services in the following order of priority: (1) cancellation of certificates (creation and distribution of the cancellation information) and (2) issue of new certificates.

The continuity plan relates to the following:

- Compromise of IT resources, programs and data
- Revoking the certificate of an AdminPKI component
- Compromise of an AdminPKI unit key
- Continuation/recovery of operations after an incident.

The continuity plan takes the following parameters into account:

- Minimum period for resuming services
- Putting a mirror site into service
- Security policy
- Practical tests, education and training of staff.

The continuity plan is strictly confidential.

5.8 Discontinuation of operations

AdminPKI shall inform the supervisory authority (SAS), the certification body (CB) and its customers at least 30 (thirty) days before the end of its certification activities[6].

Valid certificates will be revoked and a Certificate Revocation List (CRL) will be compiled and published on the AdminPKI information site for a minimum period of 11 years.

The AdminPKI signature keys and the backup copies will be destroyed.

[6] AdminPKI does not intend to assign its certification service to another certification service provider.

6 Technical security measures

6.1 Generation and installation of key pairs

6.1.1 Generating key pairs

Generating, using and storing the keys of the Certification Authority AdminCA-CD-T01 that are used to sign the certificates and lists of cancelled certificates is performed in a secure encrypted module (Hardware Security Module) complying with the FIPS 140-1 level 4 standard.

Generating the key pairs for applicants is described in section 4.4.1.

The algorithms for generating keys have been approved by the AdminPKI Manager.

6.1.2 Delivery of private keys to certificate owners

Delivering the key pairs for applicants is described in section 4.4.1.

6.1.3 Transmitting the public keys to AdminCA-CD-T01

For the purpose of generating the certificates, the certificate owner's public keys are transmitted to AdminCA-CD-T01 using a secure protocol.

6.1.4 Publication of the AdminCA-CD-T01 public key

The certificate of the root certification authority (AdminCA-CD-T01) is published by the AdminPKI Manager.

On request, the Service Desk of the Federal Office of Information Technology, Systems and Telecommunication [*BIT*] will supply a copy of the certificate of the primary certification authority.

The certificates of the AdminPKI certification authorities are published:

- by the Publication and Archiving Service, *Admin-Directory* (see section 2.1)
- by the AdminPKI information page (see section 2.2)

6.1.5 Cryptographic requirements

The AdminPKI Manager has approved the signature and encryption algorithms that are used by AdminCA-CD-T01.

The hash algorithm is SHA1.

The length of the RSA signature key that is used by the Certification Authority AdminCA-CD-T01 is 2048 bits. The certificate owners' signature keys are 1024 bits long.

Once a year the AdminPKI Security Officer examines whether the length of the keys is sufficient or must be increased.

6.1.6 Creating the parameters for the public key and quality control

The Certification Authority's signature keys are created in a hardware module that complies with the FIPS 140-1 Level 4 standard.

The certificate owners' signature keys are generated using a registration application and subsequently installed in the certificate owners' equipment.

6.1.7 Use of the key

AdminPKI provides an assurance and ensures that its signature keys can be used exclusively for the purpose of signing the certificate owners' certificates and the CRL (Certificate Revocation List).

The certificate owners' key pairs may only be used for the purposes as defined in section 1.4.1, and only in conjunction with applications that have been approved by AdminPKI.

6.2 Protection of the private key and technical checks on the encryption module

6.2.1 Relevant standards

The Certification Authority uses key creation and signature modules that comply with the FIPS standard (see section 6.1).

6.2.2 Control over the private keys

The presence of 2 (two) employees of AdminPKI (see section 5.2.2) is required for the following tasks: starting up and shutting down and replacing the encryption modules, and creating, backing up and retrieving AdminCA-CD-T01 signature keys.

6.2.3 Retrieval of private keys

The private keys of AdminCA-CD-T01 are archived and may be retrieved.

6.2.4 Replacement copy of the private key

The replacement copies of the Certification Authority's signature keys are protected with a security level that is equally as high as that of the keys in use.

If the signature keys are not being used, they must be revoked and the corresponding replacement copies must be destroyed.

The private keys of the certificate owners are stored at AdminCA-CD-T01 on the Key Archive Server and may be retrieved. This applies as long as the Certification Authority AdminCA-CD-T01 remains operational.

6.2.5 Archiving the private key

The private keys are not archived.

6.2.6 Use of the private key

The signature keys in use do not leave the facility for creating signatures.

6.2.7 Transfer of the private key to the cryptographic module

The signature keys are stored in the module for signature creation (see section 6.1). They are encrypted and protected by means of an access code.

The private encryption keys of the certificate owners are generated in the local infrastructure (registration application) of the authorised persons. They are transferred to the certificate owner's equipment using a secure method.

6.2.8 Activation of private keys

The private signature keys of AdminCA-CD-T01 are activated on starting the CA application. The CA application is started by the AdminPKI Security Officer.

The activation code (password) enables the activation of the certificate owner's private key.

6.2.9 Deactivation of private keys

The private signature keys of AdminCA-CD-T01 are deactivated when the CA application is shut down. Only the AdminPKI Security Officer can restart the CA application.

6.2.10 Destruction of private keys

The method for destroying the signature creation data is specific to the encryption resource and hardware-dependent. This method guarantees that the signature creation data cannot be restored after its destruction. The procedure for destroying the signature creation data must be approved by the AdminPKI Security Officer.

6.2.11 Properties of the encryption modules

See section 6.2.1.

6.3 Other aspects of managing key pairs

6.3.1 Archiving public keys

The data on verifying signatures (public key) is archived for at least 11 (eleven) years.

6.3.2 Period of use for public and private keys

The period of use[7] for public and private AdminCA-CD-T01 keys is:

- public key for verification of signatures and certificates of AdminCA-CD-T01: ten (10) years;
- private signature key of AdminCA-CD-T01: seven[8] (7) years;
- public key for verification of signatures of the certificate owner: three (3) years, or as the case may be, (2) years, depending on the intended purpose
- private signature key of the certificate owner: three (3) years; or as the case may be, (2) years, depending on the intended purpose
- public key of the certificate owner for encryption and associated certificate: three (3) years; or as the case may be, (2) years, depending on the intended purpose
- private encryption key of the certificate owner: no expiration date.

AdminCA-CD-T01 may provide for other periods of use in order to meet other requirements to be fulfilled by the Certification Practice Statement.

6.4 Activation data

6.4.1 Choice and installation of the activation data

The certificate issuing applications offer the private keys and certificates as PKCS#12 files for delivery and installation in the certificate user's environment. These files are protected against unauthorised access by means of a password generated by the application.

6.4.2 Protection of activation data

For security reasons the certificate user must transfer the keys and certificates contained in the file into his own key storage. This personal key storage must be protected against unauthorised access by means of the user's own password.

[7] This is the period of use and not the period of validity.

[8] The private signature key of AdminCA-CD-T01 is valid for ten years, although it may only be used for seven (7) years. The signature keys of AdminCA-CD-T01 must be renewed after seven years.

6.4.3 Other aspects of the activation data

Passwords must consist of at least 8 characters.

6.5 IT security controls

6.5.1 Particular need for security at workplaces

AdminPKI uses the following control mechanisms with regard to IT security in the operating systems of the various IT systems and in the applications:

- Access control to the services of the applications;
- Separation of duties for the functions of AdminPKI;
- Use of smartcards for entering the authorisation profile of the staff and administrators of AdminPKI;
- Archiving the events (creation, suspension, revocation) relating to the life-cycle of CA keys and the certificate owner keys;
- Investigating security-related events;
- Filtering network input and output

6.5.2 Security level of the workplace

An analysis by AdminPKI of the risks associated with the certification services enabled the security level of the IT systems for the various agencies of AdminPKI to be determined.

6.6 Technical monitoring of the systems' life-cycles

6.6.1 Monitoring system development

A risk analysis is conducted prior to any development of an AdminPKI component.

Priority is given to the use of reliable products that are secure and protected against any unauthorised alteration.

6.6.2 Monitoring security management

AdminPKI has established configuration management for hardware and software alterations.

6.6.3 Monitoring the security of the components

The AdminPKI Security Officer checks the integrity of the components of the AdminPKI certification infrastructure on a regular basis.

6.7 Monitoring the security of the networks

The AdminPKI network is an exclusive segment that is linked to the BV-network of the federal administration via a gateway. The gateway is configured such that it only accepts the protocols that are necessary for AdminPKI operations.

6.8 Technical monitoring of the cryptographic module

All operations to generate and secure the signature keys of AdminPKI are carried out using equipment complying with the FIPS 140-1 Level 4 standard [10] as a minimum.

7 Certificates and Certificate Revocation List

The certificates and Certificate Revocation Lists (CRL) that are issued by AdminPKI comply with the stipulations of the technical and administrative regulations for certification services related to electronic signatures [2].

AdminPKI does not provide any OCSP online service.

7.1 Certificate profile

The following fields of the basic attributes are used:

Version	2 (certificate in accordance with Version 3)
serialNumber	Serial number of the certificate, allocated by AdminPKI AdminCA-CD-T01; the serial number of each certificate issued by AdminPKI AdminCA-CD-T01 is unique
Signature	Contains the OID of the combination of signing and hash algorithm with which the certificate was signed
Issuer	Distinguished Name (DN) of the entity that signed and issued the certificate; currently this is AdminPKI AdminCA-CD-T01.
Validity	Period during which AdminPKI AdminCA-CD-T01 guarantees that it provides information about the status of the certificate
Subject	Distinguished Name (DN) of the entity to which the public key in the certificate is registered
subjectPublicKeyInfo	Contains the public key and the OID of the relevant public key algorithm

The following fields of the extended attributes are used:

authorityKeyIdentifier	Contains a hash value of the public key with which the certificate was signed; this makes it easier to verify the signature of the certificate and certificate chain.
subjectKeyIdentifier	Contains a hash value of the public key of the subject. This allows a distinction to be made between the keys if a subject has more than one key (for example, after renewing the keys). It also makes it easier to search for a certificate using a particular public key.
keyUsage	This field indicates the intended purpose(s) of the public key (digitalSignature (0), nonRepudiation (1), keyEncipherment (2), dataEncipherment (3), KeyAgreement (4), KeyCertSign (5), cRLSign (6), encipherOnly (7), decipherOnly (8))
certificatePolicies	This field contains the OID of the CPS
CRLDistributionPoints	Designates the point(s) where the CRL is made available

7.2 Blocked list profile (CRL profiles)

AdminPKI AdminCA-CD-T01 compiles the suspension and revocation lists in accordance with recommendation X.509 of ITU-T 0.

The suspension and revocation lists contain the following fields:

version	1 (CRL in accordance with Version 2)
signature	OID of the algorithm with which the CRL was signed
Issuer	Distinguished Name (DN) of the CA that compiled the CRL
thisUpdate	Date/time the CRL was issued
nextUpdate	Latest date on which the next CRL will be published
revokedCertificate	List of revoked and suspended certificates

The following extension fields are used:

CRLNumber	Each CRL has its own consecutive ascending number
reasonCode	Indicates the reason for revoking a certificate; depending on the entry used, applications may respond differently
invalidityDate	Indicates the (assumed) date from which the private key is compromised or the certificate must be considered invalid for a different reason

7.3 OCSP

AdminPKI does not offer any OCSP online service.

8 Audits and other evaluation criteria

AdminPKI is a recognised service provider for qualified signatures in Switzerland, and is subject to the provisions of *ZertES* [1] and the technical and administrative regulations to which reference is made.
After certification in July 2007, the recognition body conducts a recertification each year. The recognition institution is the company KPMG Klynfeld Peat Marwick Goerdeler SA, Zurich.

Since all AdminPKI services are operated in a high security zone, the annual recertifications also have a positive effect on the quality of AdminCA-CD-T01.

8.1 Time between audits

AdminCA-CD-T01 is obligated to verify compliance with the requirements of this CP/CPS at least every 24 months by means of a conformity audit. The conformity audit is conducted by an internal agency independent of AdminCA-CD-T01.

8.2 Identification and competencies of the auditor

The internal auditor is an independent firm which carries out audits in accordance with the statutory and regulatory provisions.

Coordination is performed by the AdminPKI Security Officer. The audits reports are addressed to the AdminPKI Manager and the Security Officer.

8.3 Relationship between the auditor and AdminPKI

The internal audits are conducted by an independent firm, engaged by BIT's legal service for this purpose.

8.4 Object of the audit

The conformity audit report must address the following items:

- The CP/CPS provides a sufficiently detailed description to derive the technical, organisational and personnel directives.
- AdminCA-CD-T01 actually applies the technical, organisational and personnel directives.
- The authorised persons carry out the technical, organisational and personnel directives of AdminCA-CD-T01.

8.5 Measures to be taken if discrepancies are found

The AdminPKI Manager and the Security Officer decide, in coordination with the internal auditor, which measures are to be taken to correct/remedy the discrepancies detected during the audits.

8.6 Notification of the results

The content of the audit report is confidential.

9 General conditions

9.1 Fees

9.1.1 Issue and extension of the subscriber certificate

The fees for services provided in relation to AdminCA-CD-T01 are included in its product package for the maintenance and operation of the applications. Details are regulated in the relevant SLA [24].
The SLAs are renewed each year and adjusted as required.

9.2 Financial responsibility

9.2.1 Insurance cover

The federal administration does not take out any insurance; instead, it is a self-insurer.

9.2.2 Insurance cover for certificate owners

Not required.

9.3 Data protection

9.3.1 Confidential information

The information to be treated as confidential is as follows:

- All private keys that are held by AdminCA-CD-T01 under this Policy
- The audit logs and records.

9.3.2 Non-confidential information

However, the following information is not confidential:

- the certificates, the Certificate Revocation Lists (CRL) and the information about persons or organisations contained in these documents and in public directories;
- this CPS.

9.3.3 Safeguarding confidential information

The operator of AdminCA-CD-T01 is responsible for steps to safeguard confidential information. Data may only be processed in the course of providing the service and only passed on to third parties if a confidentiality agreement has been signed beforehand and the staff entrusted with the tasks have been obligated to comply with the statutory provisions relating to data protection.

Confidential documents may be inspected for auditing or review purposes in the presence of the AdminPKI Manager.

9.4 Confidentiality of personal data

Data concerning natural persons and organisations as certificate holders is collected and verified to the extent required to issue the certificates and to ensure trust in such certificates.

In all other respects the provisions of the (Swiss) Data Protection Act shall apply.

9.5 Intellectual property

The Swiss Confederation is the owner of this CPS.

The Certificate Policies and Certification Practice Statement for AdminCA-CD-T01 (CP/CPS, this document) is generally accessible and may be used or passed on by third parties in unaltered form.

Under no circumstances does the administrative agency (federal, cantonal or municipal administration) which is the employer of the certificate holder, or the certificate holder, acquire ownership of the certificate issued by AdminPKI. The certificate holder only receives the right to use this certificate.

9.6 Obligations and guarantees

9.6.1 Obligations of AdminCA-CD-T01

The operator of AdminCA-CD-T01 undertakes to carry out all the tasks described in the context of the CP/CPS to implement the provisions.

9.6.2 Obligations of the Registration Authority

The authorised persons are obliged to observe all the requirements in SLAs and this document.

Obligations of the authorised persons are described in section 1.3.2.

9.6.3 Obligations of the certificate owners

All information that is submitted to the Registration Authority (authorised persons) or AdminCA-CD-T01 must be complete and truthful.

Obligations of the certificate owners are described in section 1.3.3.

9.6.4 Obligations of the certificate users

The "user" provides an assurance that he will comply with his obligations under the law and in accordance with this document (see section 1.3.4).

9.6.5 Declarations and guarantees of other persons

Does not apply.

9.7 Limits of the guarantee

Any other guarantee is excluded.

9.8 Liability and limitation on liability

None.

9.9 Compensation

Not applicable.

9.10 Entry into force, validity, applicability

9.10.1 Entry into force

This document enters into force on the date of its publication on the information site of AdminPKI (see section 2.2).

9.10.2 Validity

This document is valid:

- until it is replaced by a new version

or

- until AdminPKI ceases its activity as a provider of certification services.

9.10.3 Applicability in the event that the document becomes invalid

The provisions relating to the Data Protection Act and archiving remain applicable even if this document is invalidated.

9.11 Information for subscribers

AdminCA-CD-T01 informs authorised persons via signed e-mail or by letter. General information or announcements are published on the AdminPKI website (http://www.pki.admin.ch).

9.12 Management of this document

Amendments to this document are made after consulting the AdminPKI Manager and obtaining his approval. Each change to the CP/CPS results in an update to its version number and date.

9.13 Bodies for mediation between the parties

Mediation takes place at management board level of the offices that are directly involved.

9.14 Place of jurisdiction

Not applicable.

9.15 Compliance with legal requirements

AdminCA-CD-T01's agreements with its staff, authorised persons, certificate owners, certificate users and other PKIs are based on:

- Government and Administration Organisation Act [*Regierungs- und Verwaltungsorganisationsgesetz* (*RVOG*)] of 21 March 1997 (as at 13 June 2006);
- Swiss Federal IT Ordinance [*Bundesinformatikverordnung* (*BInfV*)] of 26 September 2003 (as at 1 August 2007);
- Federal Data Protection Act [*Bundesgesetz über Datenschutz*] (as at 1 January 2008).

9.16 Other provisions

9.16.1 Scope

All the regulations contained in this CP/CPS apply between the operator of AdminCA-CD-T01 and the certificate holders (natural persons or legal entities or, as the case may be, organisational units, which use certificates of certificate holders in the context of applications).

9.16.2 Language

In case of disputes the German version of this document shall prevail.

9.16.3 Validity

The issue of a new version replaces all previous versions.

Appendices

Appendix A – References

[1] Swiss Federal Electronic Signature Act [*Bundesgesetz über die elektronische Signatur* (*ZertES*)] of 19 December 2003

[2] Technical and Administrative Regulations for Certification Services related to Electronic Signatures [*Technische und administrative Vorschriften bezüglich der Zertifizierungsdienstleistungen im Bereich der elektronischen Signatur*] (RS 943.032.1) of 1 September 2005

[3] RFC 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

[4] Swiss Federal Data Protection Act [*Bundesgesetz über den Datenschutz* (*DSG*)] of 19 June 1992 (as at 1 January 2008)

[5] ITU-T X.500, The Directory: Overview of concepts, models and services

[6] ITU-T X.509, Standard: Authentication framework

[7] RFC 2459 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile

[8] RFC 2510 - Internet X.509 Public Key Infrastructure Certificate Management Protocols

[9] Technical Directive No 20 (TW 20) I006, version 2.0: Structure of the Admin Directory, ISB www.isb.admin.ch

[10] FIPS 140-1: Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, Federal Information Processing Standards, 1994

[11] RFC 2526, Public Key Infrastructure Certificate Policy and Certificate Practices Framework, March 1999

[12] Information sheet for users of AdminPKI Class A

[13] Ordinance on Security Checks for Persons [*Verordnung über die Personensicherheitsprüfungen* (*PSPV*)]

[14] Time-Stamping Authority Policy

[15] Federal Law on Technical Barriers to Trade [*Bundesgesetz über Handelshindernisse* (*LETC*)], of 6 October 1995, and the associated implementation regulations

[16] AdminPKI – CP/CPS Class A, Certification Practice Statement of the Certification Authority AdminPKI (qualified certificates)

[17] RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[18] ETSI TS 101 862, v1.3.2 (2004-06), Qualified Certificate Profile

[19] SR 784.101.113 / 2.7 Technical and Administrative Regulations for Management of Communication Parameters

[20] ITU-T F.500 Version 08-1992 International public directory services

[21] Registration Policy of AdminPKI for LRA

[22] AdminPKI Access Regulation for PKI, Version 1.5.1

[23] AdminPKI operating manual "Periodic Monitoring of Functions and Activities" v 1.9

[24] Service Level Agreement between AdminCA-CD-T01 operator and BSF (to be done)