Federal Department of Finance FDF
Federal Office of Information Technology, Systems and Telecommunication FOITT
Basic products
eGovernment
PKI

Robert Dietschi 30 June 2007

Admin PKI – Class A

Certification Practice Statement / Certification Policy of the Admin PKI Certification Authority (qualified certificates)

OID: 2.16.756.1.17.3.1.4

Project name: **Class A**

Project no.: **-**

Version: **V2.1**
Status In process In test Approved for use

Participants	
Authors:	Dietschi Robert, Karolina Kohout
Validation:	Admin PKI Officer
Users:	Subscribers, Admin PKI employees, auditors, third parties
Cc:	-

Document history, Review, Validation			
When	**Version**	**Who**	**Description**
01.04.2006	X0.1	R. Dietschi	Version 1
21.08.2006	V1.0	R. Dietschi	
21.09.2006	V1.1	R. Dietschi	FOITT Review
01.06.2007	V2.0	R. Dietschi	KPMG Review
30.06.200	V2.1	R. Dietschi	KPMG Post audit

Executive summary

This document is the Certification Practice Statement [CPS] or Certification Policy [CP] of the Admin PKI Certification Authority of the Federal Office of Information Technology, Systems and Telecommunication FOITT. It describes the practices of the Admin PKI in issuing qualified

certificates within the meaning of the federal law on certification services with regard to electronic signatures (Electronic Signatures Act, SCSE) [1].

Contents

1 Introduction

1.1 Overview

This document is the Certification Practice Statement (CPS) or Certification Policy (CP) of the Admin PKI Certification Authority of the Federal Office of Information Technology, Systems and Telecommunication FOITT. It describes the practices of the Admin PKI in issuing qualified certificates[1] within the meaning of the federal law on certification services with regard to electronic signatures (Electronic Signatures Act, SCSE) [1].

In accordance with Art. 3 (3) SCSE, FOITT is recognised as an administrative unit of the Confederation.

Whenever the Admin PKI is mentioned as the holder of certain rights and obligations, it is the Swiss Confederation, represented by FOITT, that is meant.

The structure of this document is derived from Chapter 6 of the RFC 3647 standard [3].

1.2 Identification

The title of this document is: "*Certification Practice Statement / Certification Policy of the Admin PKI Certification Authority (qualified certificates)*".

It is identified by the OID **2.16.756.1.17.3.1.4**.

The identification tree structure ({2 16 756}) is managed by the Federal Office of Communications (OFCOM) and is subdivided into eight arcs [19]). The arc {2 16 756 1 n} identifies the organisation names according to ITU-T Recommendation F.500 [20].

The identifier {2 16 756 1 17} identifies the organisation name *Admin*, which is allocated to the Federal Office of Information Technology, Systems and Telecommunication FOITT.

The Admin PKI manages the arc {2 16 756 1 17 3}.

[1] *Qualified certificates are Class A certificates as defined using Federal Administration terminology.*

1.3 User groups

1.3.1 Certification Authorities

Qualified certificates are issued on the basis of a two-level Admin PKI[2] certification infrastructure.

First, the **top-level Certification Authority**, the *Admin-Root-CA*, is responsible for validating the public key certificate of secondary certification authorities.

At the second level, the individual **Certification Authorities** are responsible for issuing, validating, publishing, archiving and managing subscriber certificates. At present, only the *AdminCA-A-T01* Certification Authority issues and manages qualified certificates for subscribers.

The top-level Certification Authority differs from the secondary Certification Authorities mainly in its certificate, which it signs with its own private key. There is no certificate to verify the authenticity of the top-level CA's certificate. The verification must be made using alternative methods such as, for example, by comparing the digital fingerprint of the certificate published by the Admin PKI on its information website with the one saved locally by the application. Upon request, the Call Centre of the Federal Office of Information Technology, Systems and Telecommunication FOITT provides the fingerprint of the primary Certification Authority's certificate.

Figure 1: Admin PKI certification hierarchy

[2] *The Admin PKI infrastructure also manages and issues Class B certificates, which are used for the purposes of authentication, encryption and advanced signatures. The processes involved in issuing and managing Class B certificates are the same as those for issuing and managing qualified certificates.*

The obligations of the Admin PKI certification infrastructure are to:

- respect and apply the provisions set out in this document
- respect and apply the provisions set out in the framework contract and the agreement it has with its clients
- deploy the technical and human resources needed to operate the infrastructure
- protect the integrity and the confidentiality of its own signature, authentication and encryption keys
- use its own signature, authentication and encryption keys solely for the purposes for which they were issued and with the tools specified in this document
- keep a log of physical accesses and limit access to a known group of people
- guarantee the reliability of the processes for:
  - registering the subscriber
  - issuing and revoking certificates
  - publishing the Certificate Revocation List (CRL)
- use, if necessary, all means available to them to notify subscribers of the revocation of the certificate of a component in the infrastructure.

1.3.2 Local Registration Authority (LRA)

The tasks of the Registration Authority or Local Registration Authority [LRA] are to:

- identify and authenticate the certificate applicants
- initiate the operation requests, i.e.:

- registration
- issue of the certificate
- revocation of the certificate
- renewal of the certificate.

The LRA is operated by an administrative entity (federal, cantonal or municipal administration). A framework contract and a Service Level Agreement (SLA) bind the Admin PKI and the Local Registration Authority.

The obligations of the LRA are to:

- respect and apply the provisions set out in this document
- respect and apply the provisions set out in the framework contract and the agreement binding it to the Admin PKI
- deploy the technical and human resources needed to operate the component
- protect the integrity and the confidentiality of its own signature, authentication and encryption keys
- use its own signature, authentication and encryption keys only for the purposes for which they were issued and with the tools specified in this document
- respect the legislation on the processing and preservation of personal data
- guarantee the reliability of the registration process; in particular, this entails:
  - verification of the certificate applicant's personal data
  - transmission of a request to issue a certificate to the secondary Certification Authority
- inform the subscriber of his rights and obligations
- verify the authenticity of a revocation request
- inform the subscriber that his certificate has been published in the *Admin-Directory*.

1.3.3 Subscriber

The subscriber[3] is an individual who holds a qualified certificate and a Secure Signature Creation Device (SSCD) for implementation of his private key. He acts on behalf of an administrative unit (federal, cantonal or municipal administration) and within the framework of the application in question (cf. **xx**).

In the phase prior to certification, the subscriber is the certificate "applicant"; within the context of the X.509 certificate, he is the "subject", and in the downstream phase following certification, he is the "holder" of the certificate.

The specific obligations of the subscriber are to:

- respect and apply the provisions set out in this document
- use his signature keys with applications approved by the Admin PKI
- have the basic knowledge required for appropriate use of signature keys and certificates
- maintain sole control of his keys and the SSCD, protect the activation code for the SSCD

- take the necessary steps to prevent loss or theft of the SSCD
- immediately notify the Local Registration Authority or the Admin PKI if he knows or suspects that his private key has been compromised
- have his certificate revoked if the information it contains is not or no longer valid.

In signing the information note for subscribers, the subscriber confirms that he has take taken note of his rights and obligations.

1.3.4 User party

The user party is a physical person or legal entity using a certificate and a signature verification system to validate a certificate and the corresponding signature within the framework of an application (cf. **xx**). The user of a certificate does not necessarily hold a certificate of their own.

The applications used by the user party should verify the certificates in accordance with the validation procedure for certification paths set out in ITU – T Recommendation X.509.

[3] *The subscriber may also be a physical person who needs a qualified certificate within the framework of his relationship with an administration. This person must contact the administration in question to obtain a qualified certificate.*

1.3.5 Other participants

The Federal Office of Communications (OFCOM) issues technical and administrative instructions concerning certification services with regard to electronic signatures (RS 943.032.1).

The Swiss Accreditation Service (SAS) appoints the Certification Bodies (cf. 8.2), which are responsible for verifying that the Certification Service Providers (CSPs) respect the legal requirements for electronic signatures.

1.4 Use of certificates

1.4.1 Authorised use

Use of certificates issued by the Admin PKI is only permitted in connection with the applications authorised by the Admin PKI. These are certified applications that meet the requirements of the Electronic Signatures Act (cf. Art. 6, SCSE) and/or a law[4] ensuing from Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures.

The Admin PKI publishes the list of authorised applications on its information website.

1.4.2 Unauthorised use

Subscribers are not authorised to use their certificates for any purposes other than electronic signatures.

1.5 Document administration / Contact details

1.5.1 Document administration

The Admin PKI is responsible for the content, management and publication of this document (cf. 9.12).

1.5.2 Contact details

The contact person is the PKI Officer:

Federal Office of Information Technology, Systems and Telecommunication FOITT
PKI Officer
Basic Products
Monbijoustrasse 74
CH-3003 Bern

[4] *Example: Law on the framework conditions for electronic signatures (Signatures Law – SigG) of 16 May 2001.*

1.5.3 Content verification

The PKI Officer and the Admin PKI Security Officer are jointly responsible for verifying and updating the content of this document.

1.5.4 Approval procedure

See 9.12.

1.6 Glossary and abbreviations

1.6.1 Glossary

Subscriber	Individual who holds a qualified certificate and a Secure Signature Creation Device (SSCD). The subscriber acts on behalf of an entity (federal, cantonal or municipal administration) within the framework of the application in question. In the phase prior to certification, the subscriber is the certificate “applicant”; within the context of the X.509 certificate, he is the “subject”, and in the downstream phase following certification, he is the “holder” of the certificate.
Admin-Directory	Meta-directory of the Federal Administration in which the certificates and Certificate Revocation Lists (CRLs) are published and archived.
Top-level Certification Authority	In a hierarchical certification infrastructure, the top-level or “root” Certification Authority differs from the other Certification Authorities in that its certificate is signed by its own private key. There is no certificate to verify the authenticity of the root Certification Authority’s certificate. Verification must be conducted using alternative methods, such as by comparing the digital fingerprint of the certificate published by the supervisory body with the one saved locally by the application.
Certification Authority (CA)	Authority entrusted to issue and manage public key certificates and Certificate Suspension and Revocation Lists that comply with Recommendation X.509.
Registration Authority	Individual or organisation responsible for subscriber identification/ authentication before any certificates are issued but which does not sign or issue certificates itself. The Registration Authority is subordinate to, at least, a secondary Certification Authority.
Classes of certificates	The Federal Administration has defined different classes of certificates, each designated a letter from A to E. The classes of certificates differ in the procedure for identifying the certificate applicant, the certificate support and the extension of the use of keys.
Certificate	Subscriber’s public key, as well as other related information, digitally signed with the private key of the Certification Authority that issued it. The format of the certificate complies with Recommendation X.509.
Class A certificate	A Class A certificate is a qualified certificate under the Electronic Signatures Act (SCSE).

Qualified certificate	Digital certificate that meets the conditions of Art. 7 of the Electronic Signatures Act (SCSE).
Activation data	Personal data, apart from keys, required for activation of cryptographic modules.

Record	Document reporting on results obtains or providing evidence of an activity performed. Records may, for example, document traceability and provide evidence that certain checks, preventative or corrective measures have been carried out.
Certification Service Provider	Body that certifies data in an electronic environment and, to this end, issues digital certificates.
Object identifier (OID)	Unique alphanumeric identifier registered in compliance with international standards for designating an object or class of specific objects.
Public key infrastructure	All policies, processes, server environments, programs and workstations used for the administration of certificates and keys.
Data integrity	Verification that data have not been tampered with between creation and reception.
Certification Authorities' Certificate Revocation List	List of CA certificates that have been revoked by the top-level Certification Authority .
Certificate Suspension and Revocation List	List maintained by the Certification Authority containing the numbers of certificates revoked before their expiry date.
Certification Body (CB)	A body authorised under the accreditation rules to license and supervise Certification Service Providers. The Certification Body in Switzerland is *KPMG Klynveld Peat Marvick Goerderler SA*.
User party	A physical person or legal entity using a certificate and a signature verification system to validate a certificate and the corresponding signature within the framework of an application.
Security policy	A security policy is a set of rules and directives drawn up with respect to a risk analysis to mitigate the probability of incidents (preventative measures) and overcome the impact of any such incidents (corrective measures), so as to protect those resources identified as being sensitive for the electronic certification services provider. The specifications for a security policy and strategy can be used to clearly define the security level to be attained, in general, for an information system and, more specifically, for each element of the security architecture.

Publication	The action of making a certificate available to third parties (user party) to enable them to verify an electronic signature.

Renewal of a certificate	Operation performed at the request of a subscriber or at the end of a certificate's period of validity consisting in creating a new certificate for the subscriber. The regeneration of a certificate after revocation is not the same as renewal.
Electronic signature	Electronic data that are attached to or linked logically to other electronic data and which are used to verify their authenticity.
Advanced electronic signature	An advanced electronic signature is one that: 1. is uniquely linked to the signatory 2. is capable of identifying the signatory 3. is created using means that the signatory can maintain under his sole control 4. is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
Qualified electronic signature	An advanced electronic signature based on a Secure Signature Creation Device (SSCD) as defined in Art. 6 (1) and (2) of the Electronic Signatures Act (SCSE) and on a qualified certificate that is valid at the time of its creation.

1.6.2 Abbreviations

ABB.	FRENCH	ABB.	ENGLISH
AC	Autorité de certification	CA	Certification Authority
AE	Autorité d'enregistrement	RA	Registration Authority
ASC	Alimentation sans coupure	UPS	Uninterrupted Power Supply
ASD	Algorithme de signature numérique	DSA	Digital Signature Algorithm
CB	Organisme de certification	CB	Certification Body
DN	Nom distinctif	DN	Distinguished Name
EPC	Énoncé des pratiques de certification	CPS	Certificate Practice Statement

FSC	Fournisseur de services de certification	CSP	Certification Service Provider
FIPS	Federal Information Processing Standard	FIPS	Federal Information Processing Standard
ICP	Infrastructure des clés publiques	PKI	Public Key Infrastructure
IDO	Identificateur d'objet	OID	Object Identifier
LAR	Liste des autorités annulées (révo-quées)	ARL	Authority Revocation List
LRC	Liste de révocation de certificats	CRL	Certificate Revocation List
ND	Nom distinctif	DN	Distinguished Name
NIP	Numéro d'identification personnel	PIN	Personal Identification Number
OFCOM	Office fédéral de la télécommunication	OFCOM	Federal Office of Communication
OFIT	Office fédéral de l'informatique et des télécommunications	FOITT	Federal Office of Information Technology, Systems and Telecommunication
PC	Politique de certification	CP	Certificate Policy
PKCS	Norme relative à la cryptographie à clé publique	PKCS	Public-Key Cryptography Standard
PKIX	Infrastructure à clé publique (conforme à la norme X.509)	PKIX	Public Key Infrastructure X.509
RFC	Document RFC (Request For Comments)	RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (type d'algorithme)	RSA	Rivest-Shamir-Adleman
SAS	Service Suisse d'accréditation	SAS	Swiss Accreditation Service
SHA-1	Secure Hash Algorithm	SHA-1	Secure Hash Algorithm
SLA	Accord de niveau de service	SLA	Service Level Agreement

UIT	Union internationale des télécom-munications	ITU	International Telecommunication Union
USIC	Unité de stratégie informatique de la Confédération	FSUIT	Federal Strategy Unit for IT

2 Information service and directory service

2.1 Publication and archiving service

The Admin PKI certificates, the subscribers, and the Certificate Revocation Lists are published and archived in the electronic meta-directory *Admin-Directory*. *Admin-Directory* is a directory service compliant with the ITU-T's X.500 standard.

The *Intranet Admin-Directory* is accessible from the Federal's Administration's intranet at www.directory.admin.ch or using the LDAP (port 389).

The *Public Admin*-Directory, the public version of the *Admin-Directory*, is accessible from the Internet (LDAP). The public version contains only a subset of the data in the intranet version.

2.2 Information service

The information service is used to publish:

- the Certification Practice Statement / Certification Policy of the Admin PKI Certification Authority (this document)
- the LRA's registration directive
- the information note for the subscriber
- the Certification Authority's certificates
- the Certificate Revocation List (CRL)
- all modifications and/or extensions relating to the Certification Authorities
- the implementation and opening of a new secondary Certification Authority dedicated to the issuing of qualified certificates
- the list of applications authorised for electronic signing of documents
- the link to the Certificate Revocation List
- the link to the legal documents
- the web address of the Swiss Accreditation Service (SAS)
- the web address of the Classified Compilation of Federal Legislation (laws and implementing ordinances of the Swiss Confederation)

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

2.3 Information update

The documents related to the Admin PKI come into effect on their date of publication.

The certificates issued by the Admin PKI are published and archived in the *Admin-Directory* straight away (once they have been issued).

The Admin-Root-CA updates its ARL at least once a year and immediately after revoking a secondary Certification Authority's certificate.

The AdminCA-A-T01 updates its CRL at least every 7 (seven) days and immediately after revoking a subscriber certificate.

After each revocation, the CRL and/or ARL is published without delay. The Admin PKI does not offer an online certificate status protocol (OCSP) for checking the validity of a certificate.

2.4 Access control

With the exception of personal data associated with applications, all of the data from the *Intranet Admin-Directory* are available on a read-access basis from the Federal Administration's network.

All of the data from the *Public Admin-Directory* are accessible via the Internet. The *Public Admin-Directory* is a partial replication (DISP) of the *Intranet Admin-Directory.*

3 Identification and authentication

The Admin PKI delegates subscriber identification and administrative tasks to Local Registration Authorities (LRA) (cf. 1.3.2).

This chapter describes the practices issued by the Admin PKI and followed by the Local Registration Authorities to identify and authenticate subscribers[5].

3.1 Name allocation

3.1.1 Naming convention

In each certificate issued by the secondary Certification Authority *AdminCA-A-T01* (cf. 1.3.1), the issuer and the subject are identified by means of a Distinguished Name (DN). The DN, which takes the form of a X.501 non-empty printable string[6], must comply with the provisions of the I006 Technical Directive (TD20) of the Federal Strategy Unit for IT [FSUIT] [9].

3.1.2 Use of explicit names

See the I006 Technical Directive (DT20) of the Federal Strategy Unit for IT [FSUIT] [9].

The subscriber (cf. 1.3.3) is a physical person acting on behalf of an administrative unit (federal, cantonal or municipal administration). The subscriber is identified by his last and first names and a unique code (see also 3.1.5). The subscriber's certificate does not contain any information on his function, title (if any) and/or organisational unit.

In the case of pseudonyms, the subscriber's Distinguished Name contains the word PSEUDO.

3.1.3 Anonymity and pseudonyms

The use of a pseudonym is subject to the approval of the Admin PKI.

[5] *Subscriber: cf. 1.3.3*

[6] *T.50 character set*

3.1.4 Interpretation rules for the various name forms

The table below specifies the conversion of special characters from the T.61 to the T.50 character set:

T.61	T.50	T.61	T.50	T.61	T.50
+	-	ë	e	ø	o
/	-	Ë	E	oe	oe
à	a	ì	i	OE	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 names

In accordance with the provisions of the I006 Technical Directive, the Admin PKI assigns to the attribute of the certificate subject a unique value comprising the certificate applicant's first and last names and a hash code. For the Federal Administration, the hash code is obtained from the personnel number. For the cantons, the hash code is obtained using a cantonal identification number, possibly also a number to identify the municipality and the personnel number.

If the name to be included in a certificate creates a dispute with another user, the Registration Authority to which the certification application had been sent will inform the Admin PKI of this. The Admin PKI is responsible for resolving any such disputes.

3.1.6 Certification, authentication and role of trademarks

No text.

The subscriber certificate does not contain any information concerning a trademark.

3.2 Initial registration

3.2.1 Proof of possession of a private key

The signature keys are generated (cf. 4.1) in a signature creation device (smart card) as defined in 6.1 of this document. Key generation is initialised by the Local Registration Authority in the presence of the certificate applicant.

The activation data (PIN and PUK), which are used to generate and activate the use of signature keys, should be specified by the certificate applicant, who alone has possession of these.

In reality, the certificate applicant is in possession of the signature keys.

3.2.2 Authentication of the identify of an administrative entity

No text.

The certificate does not contain any information concerning the subscriber's capacity to represent a specific legal entity.

3.2.3 Verification of the identity of the certificate applicant

In order to guarantee the trustworthiness of the link between a pair of cryptographic keys, or to be more specific, a public key and a subscriber, the Admin PKI must ascertain the identity of the certificate applicant for itself and using official, valid documents, such as a passport or ID card.

The tasks of identifying the certificate applicants and gathering all the information required for issuing a certificate is delegated to the Local Registration Authority.

The Local Registration Authority must:

- verify the content of the certificate application form
- verify that the applicant is registered in the *Admin-Directory*
- ensure that the applicant's name in the directory is the same as that on the ID presented[7]
- scan the identification documents presented.

The electronic version of the identification document is attached to the electronic certificate application that is submitted to the AdminCA-A-T01.

3.2.4 Unverified data

All information required for identification of the applicant is verified. No other information is verified by the Local Registration Authority.

[7] *The Admin-Directory does not accept special characters from the T.61 character set. Before comparing names, the Local Registration Authority must convert the special characters according to the rules for interpretation of the various forms of names (cf. 3.1.4). In case of doubt, the Local Registration Authority should contact the Security Officer of the Admin PKI.*

3.2.5 Verification of the subscriber's specific capacities

No text.

The certificate does not contain any information concerning the subscriber's capacity to represent a specific legal entity.

3.2.6 Cross-certification

A secondary Certification Authority which issues qualified certificates within the meaning of the Electronic Signatures Act is not authorised to cross-certify other Certification Authorities.

3.3 Renewal of the certificate

The procedure for renewing a certificate is the same as that for obtaining the first certificate. The subscriber should appear before a Local Registration Authority for the purposes of identification and authentication.

A new pair of signature keys is generated.

3.4 Authentication of a revocation request

The procedure for requesting revocation is outlined in 4.9.3.

The subscriber can request revocation of his certificate:

- by appearing in person before the Local Registration Authority
- by sending his revocation request by post
- by signing the revocation request using his signature key, provided that the revocation request is not made as a result of signature creation data being compromised or suspected of being compromised, lost or stolen
- by contacting the Call Center of the Federal Office of Information Technology, Systems and Telecommunication
- using a web application accessible from the Admin PKI information website www.pki.admin.ch

The Local Registration Authority ascertains the identity and the authorisation of the applicant by comparing the details given in the certificate application file with those presented by the subscriber.

The administrative unit (cf. 1.3.3) may request revocation of a certificate by sending a revocation request, together with its reasons, by post.

The Local Registration Authority may decide to revoke a subscriber's certificates.

4 Operational requirements

4.1 Certificate request

4.1.1 Who can submit a certificate application

Any employee of an administrative unit (federal, cantonal or municipal administration) that has signed a framework contract and concluded a Service Level Agreement with the Admin PKI may submit a certificate application (cf. 1.3.3). The personal details of the certificate applicant (last and first names, distinctive hash code, e-mail address) are published in the Admin-Directory.

4.1.2 Registration process

The process of obtaining a certificate comprises four stages: identification and authentication of the applicant (1), generation of the application (2), validation of the application (3) and issuing of the certificate (4).

The task of identifying/authenticating the certificate applicant is delegated to the Local Registration Authority, which should ascertain the identity of the applicant for itself and by means of official, valid documents (passport or ID card). The Local Registration Authority should scan the ID document presented. This document is then attached to the certificate application, which is forwarded to the secondary Certification Authority. The Registration Authority should also

verify the authenticity of the application (by checking the application form and checking the data in the *Admin-Directory*).

The Local Registration Authority should inform the applicant about his obligations and the responsibility associated with the use of certificates and the Secure Signature Creation Device (SSCD).

The signature keys are generated in the SSCD (smart card). The activation data used to generate and activate the use of signature keys (PIN and PUK) should be specified by the certificate applicant, who alone has possession of these.

Once authenticated, the certificate applications are validated by the Local Registration Authority and forwarded to the secondary Certification Authority for execution. The certificate is issued and sent to the applicant.

4.2 Processing of the certificate application

Additional information is available in the Admin PKI registration directives for the LRA [21].

4.2.1 Identification and authentication of the applicant

The task of identifying/authenticating the certificate applicant is delegated to the Local Registration Authority, which should ascertain the identity of the applicant for itself and by means of official, valid documents (passport or ID card). The Local Registration Authority should scan the ID document presented. This document is then attached to the certificate application, which is forwarded to the secondary Certification Authority.

4.2.2 Acceptance/rejection of the certificate application

Anyone whose personal data are published in the *Admin-Directory* may complete the certificate application form and send it to the Local Registration Authority.

The Local Registration Authority should verify the authenticity of the application (by checking the application form, the data in the *Admin-Directory*, and the applicant's identity). If the data are incomplete and/or the certificate applicant cannot be identified, the Local Registration Authority halts the application process.

4.2.3 Processing of the certificate application

The Local Registration Authority must:

- verify the authenticity and the content of the certificate application so as to accept/reject the application
- verify the identity of the certificate applicant

- initialise the key generation process in the signature device
- issue/validate the certificate application
- forward the certificate application to the secondary Certification Authority for execution
- leave the application in the certificate applicant's file.

Certificate applications, validated by the Local Registration Authority, are processed in real time (upon receipt) and automatically by the secondary Certification Authority. The secondary Certification Authority should:

- verify the authenticity and the integrity of the certificate application
- accept/reject the application
- issue the certificate.

4.3 Issuance of the certificate

4.3.1 Actions of the secondary Certification Authority during the issuance process

Certificate applications, submitted by the Registration Authority, are processed automatically and in real time by the secondary Certification Authority.

The secondary Certification Authority should:

- verify the authenticity and the integrity of the certificate applications
- verify the uniqueness of the public key to be certified
- issue and validate the certificate by signing it using its signature key
- publish and archive the certificate in the *Admin-Directory*. The consent of the administrative unit employing the subscriber is required for publishing the certificate in the public version of the *Admin-Directory*
- transmit the certificate to the Local Registration Authority so as to save it on the signature device of the certificate applicant.

4.3.2 Notification of issuance of a certificate to the applicant

The applicant is notified by e-mail of the issuance of the certificate. The e-mail address in the certificate is used for this purpose.

4.4 Acceptance of the certificate

4.4.1 Acceptance procedure

In signing the information note for the subscriber, the subscriber confirms that he has noted his rights and obligations. More specifically, his signature indicates:

- his acceptance of the conditions of the use and management by AdminCA-A-T01 of his certificate and, if need be, his data for the creation and verification of an electronic signature as outlined in this document
- his agreement with the conditions of publication of his certificate
- his consent to the preservation of his personal and certification data by the Local Registration Authority
- his acceptance of the obligations this entails for him
- his confirmation of the accuracy of the information contained in the certificate.

Should the Admin PKI cease to exist, the subscriber also agrees to his file being forwarded to the Certification Service Provider that takes over the Admin PKI certification tasks.

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

The certificates issued are published in the *Intranet Admin-Directory* (accessible from the federal administration network). Upon request, they are also published in the *Admin-Directory* Internet version.

4.4.3 Notification of issuance of the certificate to other bodies

The cantonal and municipal administrative units that have signed a framework contract and concluded a Service Level Agreement with the Admin PKI are notified of the issuance of certificates.

4.5 Use of keys and the certificate

The sphere of utilisation of the signature keys and the qualified certificate is specified in 1.4. The signature keys and the corresponding qualified certificate are reserved exclusively for the electronic signature of documents and the verification of said electronic signature.

4.5.1 Use of keys and the certificate by the subscriber

Subscribers are authorised to use their private keys with those IT applications that have been approved and published by the Admin PKI.

The use of keys by the subscriber is subject to the following conditions:

- the subscriber should use his private keys for approved applications and approved purposes
- the subscriber has the basic knowledge required for appropriate use of signature keys and certificates
- the subscriber uses a signature device approved by the Admin PKI. A list of approved signature devices is published on the information website.
- the subscriber must be aware of his responsibility and obligations, as set out in this document
- the subscriber should maintain sole control of his keys and his signature device. He should take the necessary precautions to prevent its loss, disclosure to third parties, unauthorised use or modification
- the subscriber should immediately notify the Local Registration Authority or the Call Centre of the Federal Office of Information Technology, Systems and Telecommunication FOITT if he finds out or suspects that his private key has been compromised.
- the subscriber is not authorised to use his certificate in any manner whatsoever other than for the purpose of an electronic signature
- the user must have his certificate revoked if the information it contains is not or no longer valid.

4.5.2 Use of the certificate by third parties (user parties)

The 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 required for appropriate use of certificates
- the third party must use a signature verification device approved by the Admin PKI
- the third party must verify the certificate before use in accordance with the validation procedure for the certification paths set out in ITU – T Recommendation X.509.

4.6 Extension of the validity of a certificate

A subscriber who wishes to extend the validity of a certificate (cf. RFC3647 [3], 4.4.6), has to submit a new certificate application and appear before the Local Registration Authority for the purposes of identification. The provisions of chapters 4.1, 4.2, 4.3 4.4 and 4.5 are applicable.

This certificate application entails the generation of a new pair of signature keys in the subscriber's signature device.

4.7 Replacement of the certificate

A subscriber who wishes to replace a valid, expired or revoked certificate (cf. RFC3647 [3], 4.4.7) has to submit a new certificate application and appear before the Local Registration Authority for the purposes of identification. The provisions of chapters 4.1, 4.2, 4.3 4.4 and 4.5 are applicable.

This certificate application entails the generation of a new pair of signature keys in the subscriber's signature device.

4.8 Modification of the certificate content

A subscriber who wishes have the content of a valid certificate modified (cf. RFC3647 [3], 4.4.7) should submit a new certificate application and appear before the Local Registration Authority for identification purposes. The provisions set out under 4.1, 4.2, 4.3 4.4 and 4.5 are applicable.

This certificate application entails the generation of a new pair of signature keys in the subscriber's signature device.

4.9 Suspension and revocation of the certificate

The subscriber certificate may be revoked, which is definitive.

Suspension of a certificate is not authorised (cf. 3.4 on the technical and administrative instructions concerning certification services with regard to electronic signatures [2]).

4.9.1 Reasons for revocation

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

- the private keys or activation codes (PIN/PUK) have been or are suspected of being compromised
- the trustworthiness of the link between the signature key and the subscriber can no longer be guaranteed
- the certificate contains information that is no longer valid
- the subscriber has received a certificate through unlawful means
- the subscriber has been dismissed or suspended
- a term or contract has expired
- the subscriber has not respected his obligations or other agreements, regulations or law that may apply
- the administrative unit employing the subscriber did not respect its obligations
- the Local Registration Authority that validated the certificate application did not respect its obligations
- the signature device is faulty

- the subscriber has lost his signature device
- the Admin PKI ceases its certification operations.

4.9.2 Who can request revocation

The secondary Certification Authority accepts certificate revocation requests from:

- the subscriber
- the Local Registration Authority that issued/validated the certificate application
- the administrative entity employing the subscriber
- the Admin PKI Security Officer.

A certificate may also be revoked following a legal ruling. This revocation request must be submitted in writing to the Admin PKI Officer (cf. 1.5) and include the reasons for the request.

The Local Registration Authority and the Admin PKI Officer must ascertain that the person making the request is authorised to do so.

4.9.3 Procedures for requesting revocation

4.9.3.1 Revocation resulting from signature keys being compromised

The following procedure applies when a subscriber's private key has been compromised:

1. The subscriber must initialise the revocation process. He can send his revocation request:
   - to the Local Registration Authority (during office hours),
   - to the Call Centre of the Federal Office of Information Technology, Systems and Telecommunication (outside of office hours). If the Call Centre is not available, he can send the request via the web application on the Admin PKI information website: www.pki.admin.ch.
   - by secure e-mail

2. The Local Registration Authority, or the Call Centre, must authenticate the revocation request by asking the subscriber to appear in person or with the revocation password.

   If the request has been sent in an e-mail containing the digital signature, the Local Registration Authority authenticates it by verifying the digital signature.

3. The revocation request is placed in the subscriber's file.
4. The revocation request is forwarded to the secondary Certification Authority for execution.
5. The secondary Certification Authority processes revocation requests that can be automatically authenticated.
6. The secondary Certification Authority informs the Registration Authority or the subscriber that the revocation has been executed.

The Local Registration Authority should make enquiries to determine how the subscriber's keys were compromised and decide whether the subscriber should be allowed to submit a new certificate application.

4.9.3.2 Revocation caused by loss of or damage to the signature device

If the signature device is lost, the procedure is the same as for requesting revocation after signature keys have been compromised (cf. 4.9.3.1). The same procedure also applies if the signature device has been damaged.

The Local Registration Authority should make enquiries to determine how the subscriber's keys were lost and decide whether the subscriber should be allowed to submit a new certificate application.

4.9.3.3 Revocation on account of non-compliance

If the subscriber does not respect his obligations, the Local Registration Authority must revoke the certificates. The procedure for revocation on account of non-compliance is the same for revocation after signature keys have been compromised (cf. 4.9.3.1).

The Local Registration Authority accepts revocation requests from the administrative entity employing the subscriber or the Admin PKI Security Officer.

The Local Registration Authority must make enquiries to determine why a subscriber does not respect his obligations and decide whether the subscriber should be allowed to submit a new certificate request.

4.9.4 Period for submission of a revocation request

If a subscriber's signature keys have been compromised or his signature device lost, he may request revocation of his certificate straight away.

4.9.4 Period for execution of a revocation request

The secondary Certification Authority processes automatically authenticated revocation requests immediately upon receipt.

After each revocation, the secondary Certification Authority generates a Certificate Revocation List and publishes this immediately in the Admin-Directory.

4.9.6 Control requirements for Certificate Revocation Lists

Upon receipt of a signed message, the user party should verify the validity of the subject's certificate and the validity of the CRL issuer.

4.9.7 Frequency of publication of CRLs and ARLs

The Admin-Root CA updates its ARL after revoking a secondary Certification Authority's certificate or once a year if no Certification Authority's certificate has been revoked during this period.

The secondary Certification Authority updates its CRL:

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

4.9.8 Period for publication of the CRL

The secondary Certification Authority publishes a new CRL at least 24 hours after receiving a revocation request.

4.9.9 Online control of the Certificate Revocation List

The secondary Certification Authority does not offer an OCSP-type online verification service (cf. [3], 4.4.9).

4.9.10 Requirements associated with online verification

No text.

4.9.11 Other forms of publication of Certificate Revocation Lists

The secondary Certification Authority does not offer an alternative to the CRLs and ARLs.

4.9.12 Replacement of a certificate where keys have been compromised

See 4.7 and 4.9.3.1.

4.9.13 Suspension of a certificate

The revocation of a certificate is definitive. The suspension of certificates is not authorised (cf. [2], 3.4.1, h).

4.9.14 Who can request revocation

No text, cf. 4.9.13.

4.9.15 Procedure for requesting suspension

No text, cf. 4.9.13.

4.9.16 Duration of suspension

No text, cf. 4.9.13.

4.10 Service for verification of certificate status

4.10.1 Operational characteristics

The service for verification of certificate status is based on the Certificate Revocation List (CRL). The CRL contains revoked certificates which have not expired. The CRL is published by:

- the directory service *Admin-Directory*
- the information service at www.pki.admin.ch

4.10.2 Service availability

The service for verification of certificate status is 99% available during office hours. Outside of office hours, the service is available but without any guarantees. In 80% of cases, any system downtime should not exceed 24 hours.

4.10.3 Options

No options.

4.11 End of contractual relationship

The end of a contractual relationship is defined in the framework contract and the agreement between the Admin PKI and its clients.

4.12 Escrow / recovery of signature keys

The implementing provisions of the Electronic Signatures Act (cf. [1]) prohibits the Admin PKI from making a copy of subscribers' signature keys and offering a recovery service for signature keys.

4.12.1 Policy on escrow / recovery of signature keys

No text, cf. 4.12.

4.12.2 Session keys and recovery practices

No text, cf. 4.12.

5 Physical security; security of procedures and of personnel

5.1 Physical security controls

5.1.1 Location

The Admin PKI certification infrastructure is operated on the premises of the Federal Office of Information Technology, Systems and Telecommunication FOITT. The area reserved for the Admin PKI certification infrastructure is a secured zone.

5.1.2 Physical access

Physical access to the certification infrastructure is set out in the directive on access control.

Only persons in possession of a badge issued by the Security Officer are permitted to access the rooms housing the IT hardware of the Admin PKI. Access is prohibited to all persons not accompanied by an Admin PKI employee.

Movement detectors are connected to the building's monitoring station.

5.1.3 Electrical system and air conditioning

The rooms housing the certification infrastructure have an air-conditioning system for regulating the temperature and humidity levels.

All electrical components are connected to an uninterruptible power supply unit, which also controls the electricity supply.

5.1.4 Water damage

The rooms housing the certification infrastructure are equipped with water detectors, which are connected to the building's monitoring station.

In the event of an alarm, the computer systems for the certification infrastructure are automatically stopped and the electricity supply is cut.

5.1.5 Fire prevention and protection

The rooms housing the certification infrastructure are equipped with smoke and heat detectors, which are connected to the building's monitoring station.

In the event of an alarm, the computer systems for the certification infrastructure are automatically stopped and the electricity supply is cut.

5.1.6 Data storage devices

All storage devices containing data for the certification infrastructure, including tape cartridges, are kept in a fireproof safe located in the rooms housing the certification infrastructure.

5.1.7 Disposal

For the disposal of data devices, the Admin PKI uses destruction devices according to the classification of the information, paper (such as shredders) and storage media (shredders).

5.1.8 Off-site storage (backup site)

The Admin PKI has a backup site, if necessary, to ensure business continuity.

The Admin PKI uses two off-site protected installations for data storage.

5.2 Control of procedures

5.2.1 Trusted roles

To ensure segregation of critical tasks, there are 7 (seven) trusted roles defined within the Admin PKI. An individual may be assigned more than one role provided that this does not adversely affect the security of the services offered.

The trusted roles are as follows:

1. PKI Officer

   The PKI Officer represents the Admin PKI vis-à-vis the management of the Federal Office of Information Technology, Systems and Telecommunication FOITT. His main tasks within the framework of the Admin PKI are to approve the security and certification policies and guarantee operation of the infrastructure.

2. Security Officer

   The Security Officer is responsible for applying the Admin PKI's physical and functional security policy and its environment. He manages the physical access controls to the platform and is authorised to access the archives and analyse the event logs.

3. Service Officer

   The Service Officer is responsible for all of the services furnished by the Admin PKI. In particular, his tasks are to enter into support contracts with the suppliers, ensure the availability of the certification infrastructure and hire and train the staff of the Admin PKI.

4. System Engineer

   He is entrusted with the start-up, configuration and maintenance of the component's IT platform. He takes charge of administration of the system and the network of the platform, which forms the basis – fully or partially – for the registration, generation and revocation of the certificates and the other services provided by the Admin PKI.

5. Operator

   The Operator monitors the correct functioning of the Admin PKI and reboots, if necessary, the certification services.

6. Controller

   The Controller, appointed by the Admin PKI Security Officer, conduct regular compliance checks of the implementation of certification policies, certification practices and services actually provided by the Admin PKI.

7. LRA Officer

   The LRA Officer is responsible for identifying the certificate applicants and personalising the SSCD (smart card).

5.2.2 Number of persons required per task

With the exception of those carried out by the Operators (cf. 5.2.1), all tasks must be performed by at least two persons working together.

The Local Registration Authority is a special case, as the LRA Officer carries out his tasks solely in the presence of the certificate applicant.

The following procedures require three persons operating together:

- updates of signature keys for the certification infrastructure
- replacement of save modules for signature keys of the certification infrastructure
- putting backup copies of signature keys into service

5.2.3 Identification and authentication of each role

The Admin PKI has set up an access-rights management system for identifying and authenticating its staff performing an action in accordance with their roles. This rights management is implemented using security mechanisms that are used to segregate the trusted functions identified in 5.2.1 and 5.2.2 according to the security objectives defined in 6.5.

5.2.4 Segregation of roles

The Service Officer assigns the roles to the staff of the Admin PKI. He ensures that there are no conflicts of interest.

5.3 Personnel security control

5.3.1 Required competencies, qualifications and history

The Admin PKI staff are employees of the Federal Administration appointed for an indefinite period of time. The have the general education, expertise, experience and qualifications required for furnishing certification services. Normally, they are posted on a full-time basis to tasks associated with their responsibilities within the framework of the certification infrastructure. Each employee is personally informed by the Service Officer of the extent and limits of his sphere of responsibility.

Each employee's employment contract contains a confidentiality clause.

The employees of the Local Registration Authorities are employees of an administrative unit (federal, cantonal or municipal administration); they undergo a certification process before being appointed.

5.3.2 Prior control procedures

Before being appointed, employees of the Admin PKI and of the Local Registration Authorities are subject to a security control for individuals as defined in Article 10 (1) (a) of the ordinance on the security controls related to individuals [13].

5.3.3 Requirements of initial training

The Admin PKI staff receive training in the software, hardware and internal operating procedures of the component on which they are working. Employees must be aware of and understand the implications of the operations for which they hold responsibility.

5.3.4 Requirements and frequency of training sessions

Every new employee receives initial training in the system, the security policies, the emergency procedures, the software and the operations he conducts.

Every employee must attend a training session after each major change to the system, organisation, tools or procedures.

5.3.5 Job rotation

No text at present.

5.3.6 Sanctions for unauthorised actions

The sanctions to be applied if an Admin PKI employee abuses his rights or performs an operation outside of his remit are set out in the Federal Law on the Liability of the Confederation, Members of its Authorities and its Officials (RS 170.323).

5.3.7 Staff on a fixed-term contract

The security requirements concerning temporary staff and suppliers' employees are the same as those applicable to staff of the Federal Administration (cf. 5.3.1, 5.3.2, 5.3.3 and 5.3.4).

5.3.8 Documentation furnished to staff

Employees have access to all of the Admin PKI documentation, in particular the following documents:

- Certification Practice Statement / Certification Policy of the Admin PKI certification authority (this document)
- Security Policy
- Operating and Organisation Manual
- other manuals on the systems and application software and hardware.

5.4 Procedure for verification of system security

5.4.1 Types of events registered

The events associated with certificate issuance and management are registered automatically and/or manually for the purposes of verification.

The following data are registered:

System:

- operations conducted on the workstations and hardware on the Admin PKI's network
- unauthorised attempts to access the networks and computer hardware of the certification infrastructure

Certification:

- Registration: registration of a new subscriber, renewal application
- Certificate generation: for the Certification Authority, the subscriber
- Certificate revocation: revocation request, revocation report
- Operations conducted on workstations and related to operations provided by the Admin PKI: start and stop of the application, change of password, modification of configuration settings for the certification tool
- Physical access to the key management centre and other related centres
- Destruction of keys, activation data and other designated information
- Staff changes.

The following details are registered for each event: date and time of operation, recipient of operation, name of person conducting the operation, name of the persons present, name of the person requesting the operation, result of the event, type of operation, cause of the event.

5.4.2 Frequency of event log processing

The event logs are analysed online by a program for monitoring the certification infrastructure. At least once a week, the Security Officer specifically analyses the event logs.

5.4.3 Storage period for event logs

The "system" event logs and the "application" event logs are stored for a period of at least eleven years.

5.4.4 Protection of event logs

The event logs are stored on a dedicated server. Only authorised and authenticated Admin PKI employees have access to the event logs.

The information stored off-site is encrypted.

5.4.3 Storage procedures for event logs

The event logs are saved every day as part of the normal backup of the Admin PKI host system.

5.4.6 Log collection system

An internal server within the certification infrastructure collects all of the event logs.

5.4.7 Notification following a critical event

The program for analysing event logs notifies the Security Officer and the operators responsible for operation in the event of a critical event.

5.4.8 Evaluation of vulnerability

At least once a week, a program analyses the components of the Admin PKI to identify any loopholes and prevent potential attacks on the certification infrastructure.

In the event of a critical error, the Security Officer is notified immediately.

5.5 Archiving of certificates and other documents

5.5.1 Types of data to be archived

The Admin PKI archives all data and event logs associated with certificate issuance and management. In particular, this includes:

- contracts or agreements with Admin PKI clients and operators of the Local Registration Authorities
- subscriber certificates and components of the Admin PKI
- all Certificate Revocation Lists (CRLs) that have been issued
- revocation requests and survey reports, if any
- subscriber's personal identification data, all elements used for registration, the nature of the documents presented by the certificate applicant
- event logs
- audit reports

- incident reports
- loophole analysis reports

5.5.2 Storage period for archives

The Admin PKI archives are stored for a minimum period of 11 (eleven) years.

5.5.3 Protection of archives

The application logs are signed by the certification application and then encrypted before being saved and encrypted.

Only the Security Officer has access to the archived data.

5.5.4 Procedure for copying archives

The Admin PKI uses two off-site protected installations for data storage/archiving.

5.5.5 Time-stamping of archives

Each event that is registered and archived is dated. The time is supplied by a reference clock housed by a local IT system. All the components of the Admin PKI's central infrastructure are synchronised according to this clock.

5.5.6 Archiving system

The archiving system is internal within the Admin PKI.

5.5.4 Procedures for recovery of archives

The recovery or analysis of archived files must be approved by the Security Officer.

5.6 Change of key for a component of the Admin PKI

The validity of the keys used by the components of the Admin PKI is monitored by the System Engineer. The generation of new keys and the issuance of certificates must be authorised by the Security Officer.

Depending on the nature of the change (end of the period of validity, renewal of keys after revocation, etc.), the measures taken must comply with the procedures outlined in 4.2, 3.2 and 3.3.

Whenever a component renews its keys, it informs its users of this, if necessary.

5.7 Compromised data and disaster recovery

5.7.1 Incident management

The incident management procedure is issued by the Security Officer and communicated to all employees of the certification infrastructure.

5.7.2 Corruption of computing resources, software or data

The Admin PKI implements the necessary measures to prevent any of the information or hardware it holds from being compromised or stolen. If these are stolen, compromised, or suspected of being compromised, the Security Officer sets the business continuity plan in motion.

The Security Officer for the certification infrastructure works in close cooperation with the IT Security delegate from the Federal Office of Information Technology, Systems and Telecommunication.

If necessary, the Admin PKI can have an operating backup site at its disposal within five days after the loss of its site in Berne.

5.7.3 Compromise of an Admin PKI signature key

If the keys of the top-level and secondary Certification Authorities are compromised or suspected of being compromised, the PKI Officer is immediately notified of this. After analysing the situation, the PKI Officer starts, if necessary, the procedure for revocation of all certificates of the subscriber in question. This entails:

- informing the subscribers
- informing the Swiss Accreditation Service and the Certification Body
- revoking the Certification Authority's certificate and the subscribers' certificates
- generating new signature keys for the Certification Authority
- informing the Local Registration Authorities
- issuing the subscribers' certificates.

5.7.4 Business continuity plan

The Admin PKI's business continuity plan is set in motion immediately after an accident/disaster. It aims to guarantee availability with the same restrictions for all basic services, in order of priority: (1) certificate revocation (generation and distribution of revocation information) and (2) issuance of new certificates.

It covers the following points:

- corruption of computing resources, software or data
- revocation of the certificate of an Admin PKI component
- compromise of the key of an Admin PKI entity
- continuation/resumption of activities following a disaster.

It takes the following parameters into account:

- minimum period for recovery of services
- putting a mirror site into service
- Security Policy
- practical tests, courses and staff training.

The business continuity plan is strictly confidential.

5.8 Cessation of operations

5.8.1 Cessation of operations by the Admin PKI

The Admin PKI informs the supervisory body (SAS), the Certification Body (CB) and its clients at least thirty days before ceasing its certification operations[8].

Any outstanding valid certificates are revoked and a Certificate Revocation List [CRL] is generated and published on the Admin PKI information website for a minimum period of 11 years.

The Admin PKI signature keys and backup copies are destroyed.

The information concerning certification is archived at the Federal Office of Information Technology, Systems and Telecommunication for a minimum period of 11 years from the last day of operations.

5.8.2 Cessation of operations by a Local Registration Authority

The Admin PKI informs the Certification Body (CB) of the cessation of operations by a Local Registration Authority or the transfer of operations to another Local Registration Authority.

The certification-related details are either transferred to another Local Registration Authority or archived at the Federal Office of Information Technology, Systems and Telecommunication for a minimum period of eleven years.

[8] *The Admin PKI does not plan to transfer its certification service to another Certification Service Provider.*

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

The keys of top-level and secondary Registration Authorities, used for signing certificates and CRLs, are generated, used and stored within a secure cryptographic module (hardware security module) designed to meet FIPS 140-1 Level 4 criteria.

Subscribers' signature keys are generated, used and stored within a secure cryptographic module (Hardware Security Module) designed to meet EAL4+ criteria.

6.1.2 Delivery of the private key to a subscriber

The signature keys are generated in the subscriber's secure signature creation device (cf. 6.1). The subscriber alone has control of this device.

6.1.3 Delivery of the subscriber's public key to a Certification Authority

The subscriber's public key is included in the certification request and transferred to the Certification Authority by means of a secure protocol.

6.1.4 Publication of the Certification Authorities' public key

The Admin PKI provides its clients with a CD containing the Certification Authorities' certificates (cf. 1.3.1). Upon request, the Call Centre of the Federal Office of Information Technology, Systems and Telecommunication FOITT provides the fingerprint of the top-level Certification Authority's certificate.

The Admin PKI Certification Authorities' certificates are published:

- by the Admin-Directory publication and archiving service (cf. 2.1)
- on the Admin PKI information website (cf. 2.2)

6.1.5 Cryptographic requirements

The signature and hash algorithms are specified by the Security Officer.

The secure hash algorithm is SHA1.

The size of the RSA signature keys used by the top-level and secondary Certification Authorities is 2048 bits, while the subscribers' signature keys are 1536 bits.

The Admin PKI Security Officer checks once a year whether the size of the keys remains adequate or should be increased.

6.1.6 Generation of public key parameters and quality control

The subscribers' signature keys are generated in a secure signature creation device designed to meet the EAL4+ criteria, while those of the top-level and secondary Certification Authorities are generated in a hardware module designed to meet the FIPS 140-1 Level 4 criteria.

6.1.7 Use of the key

The Admin PKI ensures and ascertains that its signature keys can only be used for the purposes of subscriber and CRL certificate signature.

The subscribers' signature keys can only be used for signature purposes and in connection with the applications authorised by the Admin PKI (cf. 1.4.1).

The "key usage" extension of a subscriber's certificate is equivalent to "non repudiation".

6.2 Protection of the cryptographic module's private key and technical controls

6.2.1 Standards related to the cryptographic module

The top-level and secondary Certification Authorities use key and signature generation modules designed to meet the FIPS (cf. 6.1) and EAL4+ criteria.

6.2.2 Control of the Admin PKI signature keys

The activities concerning service activation/deactivation and the replacement of cryptographic modules, on the one hand, and the processes of generation, saving and recovery of the Admin PKI's signature keys, on the other hand, require the presence of three Admin PKI employees (cf. 5.2 and 5.3).

6.2.3 Key escrow

There is no escrow of private keys.

6.2.4 Private key backup copy

The backup copies of the top-level and secondary Certification Authorities' signature keys are protected with a security level that is as high as the keys in use.

If signature keys are no longer used, they should be revoked and the corresponding backup copies should be destroyed.

Under no circumstances are backup copies made of the subscriber's signature keys.

6.2.5 Private key archiving

The signature keys (private keys) are not archived.

6.2.5 Private key utilisation

The signature keys in use do not leave the signature creation device.

6.2.7 Protection of the signature creation key

The signature keys are stored in the signature creation module (cf. 6.1). They are encrypted and protected by an access code.

6.2.8 Private key activation methods

The secondary Certification Authority's signature keys are activated once the PKI application is opened. The application is opened by the Security Officer.

The PIN activation code is used to activate the subscriber's signature key.

6.2.9 Private key deactivation method

The secondary Certification Authority's signature creation keys are deactivated once the PKI application is closed.

6.2.9 Private key destruction method

The method for destroying signature creation data is peculiar to the cryptographic resource and is material. This method ensures that, once destroyed, the signature creation data cannot be found again. The process for the destruction of signature creation data has to be approved by the Security Officer.

6.2.11 Characteristics of the cryptographic modules

See 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Archiving of public keys

The signature verification data (public key) are archived for a minimum period of 11 (eleven) years.

6.3.2 Utilisation periods for public and private keys

The period of validity of certificates issued by the Admin PKI is:

- 20 (twenty) years for the top-level Certification Authority (Root CA)
- 10 (ten) years for the secondary Certification Authorities
- 3 (three) years for subscriber certificates.

The period of utilisation of the signature creation keys is:

- 7 (seven) years for the Secondary Certification Authorities
- 3 (three) years for subscribers.

6.4 Activation data

6.4.1 Activation data generation and installation

The subscriber determines his own activation data (PIN and PUK) and activates these at the start of the process for generating his creation data and verifying his signature.

6.4.2 Activation data protection

The subscriber should protect the confidentiality and integrity of his signature creation data.

The Local Registration Authorities should notify the subscribers of the consequences of divulging their activation data. They should also give instructions on choosing a password.

6.4.2 Other aspects of activation data

The activation data should comprise at least eight characters.

6.5 IT security controls

6.5.1 Specific security requirements on workstations

The Admin PKI implements a certain number of controls associated with the software of the PKI application, such as:

- access control to the software services of the PKI application
- mandatory segregation of tasks for the PKI functions
- identification and authentication of Admin PKI employees
- logging of events, periodic verification of the logs
- filtering of network inputs/outputs

6.5.2 Workstation security level

The risk assessment of the certification services conducted by the Admin PKI provided a basis for defining the security level of the systems and hardware (workstations) for the various entities in the Admin PKI.

6.6 Lifecycle technical controls

6.6.1 Systems development control

A risk assessment is conducted prior to any development of a component of the Admin PKI.

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

6.6.2 Security management controls

Each development of the Admin PKI certification infrastructure must be documented, appear in the operating procedures, comply with the assurance maintenance plan in the products evaluated, and be approved by the Security Officer.

The Admin PKI ascertains that:

- control procedures on the modifications exist
- the security of the hardware device is not altered by a third party or in any other manner during transport
- the security of the hardware device is not altered by a third party or in any other way while in use or, if applicable, in storage
- the hardware device operates correctly
- the processing and storage capacity meets the subscribers' needs
- the appropriate increase and maintenance of the system are made.

6.6.3 Component security controls

The Security Officer regularly checks the integrity of the components of the Admin PKI certification infrastructure.

6.7 Network security control

The Admin PKI network is an exclusive segment connected by a gateway to the Federal Administration's *BV-Netz* network. The gateway is configured so as to accept only the protocols needed for operation of the Admin PKI.

6.8 Time-stamping service

The Admin PKI offers a time-stamping service. The rules associated with the operation of the Admin PKI apply to the time-stamping authority. Further details are available at [14].

7 Certificates and Certificate Revocation Lists

The certificates and Certificate Revocation Lists [CRL] issued by the Admin PKI meet the requirements of the technical and administrative instructions concerning certification services with regard to electronic signatures (cf. [2], 3.4).

The Admin PKI does not offer an online OCSP-like service.

7.1 Format of the subscriber certificate

The ASN1 structure of the subscriber certificate is described in Annex B2.

The structure of the certificate consists of a basic certificate and additional fields (extensions).

The basic certificate contains the following fields in the tsbCertificate sequence as per Art. 7 of the SCSE [1] and the RFC 3280 standard, 4.1:

- Version of the certificate contains the number 2, designating a version 3 certificate.
- Certificate series number: contains an integer designating the certificate series number. L'AdminCA-T-01 is responsible for the content of this field.
- The identifier of the signature algorithm used to sign the certificate: contains the object identifier 1 2 840 113549 1 1 5, which designates the algorithm shaWithRSAEncryp-tion.
- Name of the Certification Service Provider CSP: contains the distinguished name of AdminCA-T-01: CN = AdminCA-T-01, OU = Certification Authorities, OU= Services, O = admin, C = ch
- Period of validity of the subscriber certificate: contains the period during which the subscriber certificate is presumed to be valid. The field notBefore indicates the date on which the certificate comes into effect, the field notafter indicates the date of expiry. The period of validity of subscriber certificates must not exceed 3 (three) years.
- Name of the certificate holder (subscriber): contains the subscriber's distinguished name, e.g.: C = ch, O = admin, OU = Weisse Seiten, CN = User Test NQW5PM
- Verification key and algorithm for the signature of the certificate holder: contains the object identifier 1 2 8 840 113549 1 1 1, which designates the algorithm rsaEncryption and the subscriber's public key.

The subscriber certificate contains the following extensions of the *tbsCertificate* sequence in accordance with the document RFC 3280 [8], 4.2. :

- AuthorityKeyIdentifier

  - identifies the public key to be used to verify the signature of a certificate

  - non-critical extension

- Key usage

  - identifies the public key to be used to verify the signature of a certificate

  - critical extension

- CertificatePolicies

  - includes the field policyQualifiers, within which the qualifiers CPS Pointer and User Notice indicate, respectively, the CSP's certification practices and the user note.

  The object identifier is {2.16.756.1.17.3.2.17}.

  The certification practices are available at the address
  http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_1_4.pdf

- non-critical extension

- Distribution points of the Certificate Revocation List (CRLDistributionPoints)
  - identifies the point(s) of distribution of the Certificate Suspension and Revocation List
  - non-critical extension
- Point of access to the Certification Service Provider's certificate (AuthorityInformation Access)
  - non-critical extension
- Statement specifying that the certificate is issued as a qualified certificate (qcStatements)
  - object identifier as defined in the standard ETSI 101 862 0 (cf. Annex [18])
  - critical extension
  - object identifier: {0.4.0.1862.1.1}
- Statement specifying that the signature key is protected by a Secure Signature Creation Device (qcStatements)
  - object identifier as defined in the standard ETSI 101 862 0 (cf. Annex [18]): {0.4.0.1862.1.4}
  - critical extension
- Transaction limit value (qcStatements)
  - object identifier as defined in the standard ETSI 101 862 0 (cf. Annex [18]): {0.4.0.1862.1.2}
  - critical extension
- Extension of other issuer name
  - object identifier: {2.5.29.18}
  - alternative name: { O=ZertES Recognition Body: KPMG Klynveld Peat Marwick Goerdeler SA}
  - non-critical extension

7.2 Profile of the Certificate Revocation List CRL

The ASN1 structure of the subscriber certificate is described in Annex B4.

The Certificate Revocation List [CRL] contains the fields tbsCertList, signatureAlgorithm and signatureValue in accordance with document RFC 3280, 5.

The sequence tbsCertList contains the following fields:

- version, the value of which is 1 to indicate that this is a version 2 CRL
- signature: identifier of the algorithm used to sign the CRL
- issuer: contains the distinguished name of AdminCA-T-01:
- thisUpdate: time of publication of the CRL
- nextUpdate : time of publication of the next CRL

- revokedCertificates, containing the certificate's series number and the revocation date;

The CRL contains the non-critical extensions authorityKeyIdentifier and cRLNumber within the sequence tbsCertList, in accordance with the document RFC 3280 [8], 5.2.

7.3 OSCP

The Admin PKI does not offer an online OCSP-like service.

8 Compliance controls

8.1 Frequency and circumstances

The supervision of recognised providers is governed by the Electronic Signatures Act. This task is performed by the Certification Body, in accordance with the rules of accreditation.

Apart from the supervision conducted by the supervisory body, the Admin PKI components must demonstrate to the Security Officer, at least every 12 months, that they are operating in full compliance with the requirements of this document.

This rule does not apply to the Local Registration Authorities, which are controlled at least once every three years.

8.2 Identity and powers of the auditor

The Certification Body is KPMG Klynveld Peat Marwick Goerdeler SA, Zurich.

The Admin PKI Security Officer commissions an independent company to conduct the internal audits.

8.3 Relationship between the auditor and the Admin PKI

The Certification Body is an independent firm that performs compliance checks on the basis of a mandate.

The internal audits are conducted by an independent company commissioned by the Admin PKI.

8.4 Object of the inspection

The object of the inspection is determined by the Certification Body.

The internal audits fall under the remit of the Security Officer. The Security Officer may coordinate the content of the internal audits with the Certification Body.

8.5 Measures adopted in the case of irregularities

In agreement with the Certification Body, the PKI Officer and the Security Officer decide on the measures to be adopted to correct/eliminate any irregularities brought to light in the course of audits.

8.6 Communication of results

The measures to be adopted to eliminate/correct any irregularities brought to light in the course of audits are communicated to the relevant administrative units (federal, cantonal, municipal administration).

There are no plans to publish the audit reports.

9 Framework conditions

9.1 Fees

9.1.1 Issue and renewal of the subscriber certificate

The fees associated with the issue, renewal, management and use of certificates are set out in the agreement between the Admin PKI and the administrative unit (federal, cantonal or municipal administration) employing the subscriber (cf. 1.3.3).

The costs generated through the operation of a Local Registration Authority LRA (registration procedure, user support, provision of the Crytoki device, etc.) are borne by the administrative unit (federal, cantonal or municipal administration) operating the LRA.

The costs generated by the user party are borne by that user party.

9.2 Financial liability

9.2.1 Insurance protection

The FOITT is a party that is legally non-independent of the Swiss Confederation. Therefore, the Swiss Confederation holds the rights and obligations and is the person responsible under Art 16 SCSE and responsible for the insurance cover within the meaning of Art. 2 OSCSE.

The declaration of guarantee from 1 June 2006 in accordance with Art. 2 (2) OSCSE of the Federal Department of Finance replaces the insurance under Art. 2 (1) OSCSE. This declaration stipulates that the Swiss Confederation itself bears the risks incurred in the operations of the FOITT, as the Certification Service Provider with regard to electronic signatures, and therefore does not take out any insurance in this respect.

9.2.2 Insurance cover for subscribers and the LRAs

The subscribers and the Local Registrations Authorities ensure they have sufficient insurance cover for their liability under the Electronic Signatures Act.

9.3 Data protection

9.3.1 Confidential information

All information concerning the users of the Admin PKI certification services which does not appear in either the subscriber certificate or the Certificate Revocation List is deemed confidential.

9.3.2 Non-confidential information

The information in the certificates and the contents of the Certificate Revocation Lists are deemed non-confidential.

The information derived from the content of the certificate is also deemed non-confidential.

9.3.3 Protection of confidential data

The Admin PKI takes the necessary steps to protect the confidential information it holds.

Only in the following cases may confidential data be used and communicated externally:

- when performing the services defined in this document
- to comply with legal requirements
- to perform work or services entrusted to service providers.

9.4 Personal data

The Admin PKI and the Local Registration Authorities apply the relevant provisions of the law on data protection and the law on the electronic signature.

The Admin PKI and the Local Registration Authorities may process only the personal data that is needed for execution of their tasks. Any trade in such data is prohibited.

9.5 Intellectual property rights

The Admin PKI holds the intellectual property rights to the following documents:

- The Admin PKI – Class A Certification Practice Statement / Certification Policy of the Admin PKI certification authority (qualified certificates)".
- Registration directives of the Admin PKI
- Contracts and other agreements between the Admin PKI and its clients (federal, cantonal or municipal administrative unit)
- certificates issued.

Reproduction or representation (including publication and distribution), in whole or in part, by any means whatsoever (specifically: electronically, mechanical, optical, photocopy, saving to computer) that is not authorised in advance and in writing by the Admin PKI or its authorised representatives is strictly prohibited.

Under no circumstances does the subscriber or the administrative unit (federal, cantonal or municipal administration) employing the subscriber acquire ownership of the certificate issued by the Admin PKI. Solely the right of use is acquired.

9.6 Guarantees and assurances

9.6.1 Representations and guarantees of the Admin PKI's Certification Authorities

The Admin PKI undertakes to respect the requirements set out in the Electronic Signatures Act (SCSE) and in this document (cf. 1.3.1).

9.6.2 Representations and guarantees of the Local Registration Authorities (LRAs)

The LRAs are bound by contract to respect all of the requirements set out in the Electronic Signatures Act as well as this document (cf. 1.3.2).

9.6.3 Representations and guarantees of the subscriber

The subscribers undertake to respect the requirements set out in this document (cf. 1.3.3).

9.6.4 Representations and guarantees of the user party

The “user party” undertakes to respect its commitments as set out in the law and in this document (cf. 1.3.4).

9.6.5 Representations and guarantees of other parties

No text.

9.7 Limits of the guarantee

All additional guarantees are excluded.

9.8 Liability and limitation of liability

9.8.1 Liability and limitation of liability of the Admin PKI

The Admin PKI is liable within the meaning of Art. 16 OSCSE to the subscriber and to third parties who have used a qualified certificate for all damage they incur as a result of the Admin PKI failing to observe its obligations as set out in the Electronic Signatures Act and the corresponding implementing provisions.

The Admin PKI will not be held liable if the certificates it issues are used for purposes other than those mentioned in this document.

In all other cases, the liability of the Admin PKI is as follows:

- in the event of breach of contract, the Admin PKI is liable for proven damages, unless it can demonstrate that it did not commit a fault
- in the event of mere negligence, the liability of the Admin PKI is limited to CHF 100,000 per event and per calendar year for the material damage sustained
- in the event of mere negligence, the liability of the Admin PKI is limited to the exchange value of the services agreed on during the current year, up to a maximum of CHF 50,000 per event and per calendar year for the financial losses incurred.

All liability for consequential damages, loss of earnings or loss of data is expressly excluded.

The Admin PKI is not liable for consequential delays and damages resulting from cases of *force majeure*, natural events (e.g. lightning, natural catastrophes), power outages, armed conflicts, war, strikes, unforeseeable restrictions by the authorities, the circumvention of locking systems, remote login applications, hacking, computer viruses (including Trojan horses, etc.) aimed at

data processing installations, etc. If the Admin PKI cannot meet its commitments as a result of such events, the implementation of the contract or the deadline for implementation of the contract will be postponed in accordance with the event. The Admin PKI declines all liability concerning damages incurred as a consequence of contract implementation being postponed.

9.8.2 Liability of subscribers

The liability of subscribers, as employees of the Confederation or a canton, is set out in the liability laws applicable to the Confederation and the canton for damages associated with unlawful use of the signature key.

9.8.3 Liability of the LRAs

The liability of the LRAs is defined in the contract with the Admin PKI, subject to the provisions of Art. 16 OSCSE.

9.9 Indemnification

The Admin PKI does not rule on indemnification, subject to the provisions of chapters 9.6 / 9.8.

9.10 Enforcement, validity, applicability

9.10.1 Enforcement

This document comes into force on the day on which it is published on the Admin PKI information website (cf. 2.2).

9.10.2 Validity

This document is valid:

- until replaced by a new version

or

- until the Admin PKI ceases operations as a Certification Service Provider

9.10.3 Applicability in the case of non-validity

The provisions concerning the law on data protection and on archiving remain applicable, even if this document is no longer valid.

9.11 Communication with subscribers

The Admin PKI communicates with the subscribers via e-mail.

9.12 Administration of this document

The PKI Officer may correct typographical errors or reorganise any section of this document and re-publish it without any prior notice.

The modification of any element of this document in any manner other than spelling corrections or reorganisation of text is subject to 30 days' prior notice. The Security Officer and the Certification Body (cf. 8.2) participate in the review and approval process.

If necessary, the subscribers are notified of the changes made.

9.13 Resolution of disputes

The resolution of disputes is specified in the framework contract and the agreement between the Admin PKI and the recipients of the certification services.

9.14 Applicable laws

The laws of Switzerland apply, in particular the law on the electronic signature. The place of jurisdiction is Berne.

9.15 Transfer of rights and obligations

The subscriber is not permitted to transfer his rights and obligations.

The rights and obligations within the remit of the Federal Office of Information Technology, Systems and Telecommunication may also be assigned to other departments within the Administration.

9.16 Other provisions

9.16.1 Language

The French-language version of this document is binding in the case of dispute.

Annexes

Annexe A - References

[1] Federal law on certification services with regard to electronic signatures (Electronic Signatures Act, SCSE) of 19 December 2003 (as amended on 21 December 2004)

[2] Technical and administrative instructions concerning certification services with regard to electronic signatures (RS 943.032.1) of 1 September 2005

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

[4] Federal law on the protection of data (LPD) of 19 June 1992 (as amended on 12 December 2006)

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

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

[7] RFC 2459, Internet X.509 Public Key Infrastructure, Certificate and CRl Profile, January 1999

[8] RFC 2510, Internet X.509 Public Key Infrastructure, Certificate Management Protocols, March 1999

[9] Technical Directive I006 – DT20, Admin-Directory structure, FSUIT 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 notice for users of the Admin PKI Class A

[13] Ordinance on the security controls related to individuals (OCSP)

[14] Time-Stamping Authority Policy

[15] Federal law of 6 October 1995 on technical barriers to trade (LETC) and the relevant implementing provisions.

[16] Admin PKI – Class B, Certification Practice Statement of the Admin-CA3 certification authority

[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] RS 784.101.113 / 2.7 Technical and administrative instructions concerning the management of communication parameters

[20] ITU-T F.500 Version 08-1992 International public directory services
[21] The Admin PKI's registration directives for the LRA

Annexe B - Structure ASN1

Annex B1 - AdminCA-T-01 Certification Authority

X.509 Field	OIDs/Values	Comments
version	2	v3 cert
serialNumber	xxxxx	Integer value defined at key ceremony
signature {		
algorithm	{1.2.840.113549.1.1.5}	sha1WithRSAEncryption
parameters	NULL},	
issuer {	{2.5.4.3:Admin-Root-CA}, {2.5.4.11:Certification Authorities}, {2.5.4.11:Services}, {2.5.4.10:Admin}, {2.5.4.6:CH}},	Printable String (UTF8String), directoryName
validity {		
notBefore	“YYMMDDHHMMSSZ”,	UTC TIME, ETSI TS 102 280
notAfter	“YYMMDDHHMMSSZ”},	UTC TIME, ETSI TS 102 280
subject {	{2.5.4.3:AdminCA-A-T01}, {2.5.4.11:Certification Authorities}, {2.5.4.11:Services}, {2.5.4.10:Admin}, {2.5.4.6:CH}},	Printable String (UTF8String), directoryName
subjectPublicKeyInfo {		
algorithm {	{1.2.840.113549.1.1.1},	rsaEncryption
parameters	NULL},	
subjectPublicKey {	…..},	BIT STRING 2048 bit
extensions {		
authorityKeyIdentifier {		
extnId	{2.5.29.35},	
extnValue	…..},	OCTET STRING, 160 bit SHA1 of root subjectPublicKey BIT STRING
subjectKeyIdentifier {		
extnId	{2.5.29.14}	
extnValue	…..},	OCTET STRING, 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage {		
extnId	{2.5.29.15},	
critical	TRUE,	BOOLEAN

extnValue	‘000001100},	certSign, crlSign
certificatePolicies {		
extnId	{2.5.29.32},	
extnValue	{2.16.756.1.17.3.1.0},	
extnId	{{1.3.6.1.5.5.7.2.2},	
extnValue	{This is the Admin-Root-CA CPS},	UTF8String, id-qt-unotice RFC 3280

X.509 Field OIDs/Values Comments

extnId	{1.3.6.1.5.5.7.2.1},	
extnValue	{http://www.informatik.admin.ch/PKI/links/CPS_2_16_756_1_17_3_1_0.pdf}},	IA5String, cps
issuerAltName {		
extnId	{2.5.29.18},	UTF8String, directoryName
extnValue	{O=ZertES Recognition Body: KPMG Klynveld Peat Marwick Goerdel SA}},	
basicConstraints {		
extnId	{2.5.29.19},	
critical	TRUE,	BOOLEAN
extnValue	{cA TRUE},	BOOLEAN
pathLenConstraint	0 },	INTEGER, no child CA
crlDistributionPoints {		
extnId	{2.5.29.31},	
extnValue	{http://www.pki.admin.ch/crl/Admin-Root-CA.crl ldap://admindir.admi.ch/cn=Admin-Root-CA,ou=Certification Authorities,ou=Services,o=Admin,c=CH c=ch,o=Admin,ou=Services,ou=Certification Authorities,cn=Admin-Root-CA},	uri IA5String ldap uri IA5String X509 name, IA5String CA inherits Admin-Roo CA CDPs
AuthorityInfoAcess {	SEQUENCE {	
extnId	{1.3.6.1.5.5.7.1.1},	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE {	
accessmethod	{1.3.6.1.5.5.7.48.2},	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia	uri IA5String
AccessDescription	SEQUENCE {	
AccessMethod	{1.3.6.1.5.5.7.48.1},	id-ad-ocsp
accessLocation	http://ocsp.pki.admin.ch}}},	uri IA5String
qcStatments {		
etxnId	{1.3.6.1.5.5.7.1.3},	
critical	TRUE	BOOLEAN
extnValue	SEQUENCE OF {	OCTET STRING
QCStatment	SEQUENCE	
statmentId	{0.4.0.1862.1.1}}}}}	qcs-Qccompliance
signatureAlgorithm {		
algorithm	{1.2.840.113549.1.1.5}	sha1WithRSAEncrypti
parameters	NULL},	
signature	…..	2048 bit BIT STRING

```
KeyUsage ::= BIT STRING {
digitalSignature (0),
nonRepudiation (1),
keyEncipherment (2),
dataEncipherment (3),
keyAgreement (4),
keyCertSign (5),
cRLSign (6),
encipherOnly (7),
decipherOnly (8) }
```

Usage	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Digital Signature, Non repudiation				x			x		
Data Encipherement				x			x		
Key Agreement					x				
Cert Sign, CRL sign				x			x		

Annex B2 – Subscriber certificate

X.509 Field	OIDs/Values	Comments
version	2	v3 cert
serialNumber	xxxxx	Integer value defined at key ceremony
signature {		
algorithm	{1.2.840.113549.1.1.5}	sha1WithRSAEncryption
parameters	NULL},	
issuer {	{2.5.4.3:AdminCA-A-T01}, {2.5.4.11:Certification Authorities}, {2.5.4.11:Services}, {2.5.4.10:Admin}, {2.5.4.6:CH}},	Printable String (UTF8String), directoryName
validity {		
notBefore	“YYMMDDHHMMSSZ”,	UTC TIME, ETSI TS 102 280
notAfter	“YYMMDDHHMMSSZ”},	UTC TIME, ETSI TS 102 280 (3 years)
subject {	{2.5.4.3:CN=Last First Hash}, {2.5.4.11:Weisse Seiten}, {2.5.4.10:Admin}, {2.5.4.6:CH}},	Printable String (UTF8String), directoryName
subjectPublicKeyInfo {		
algorithm {	{1.2.840.113549.1.1.1},	rsaEncryption
parameters	NULL},	
subjectPublicKey {	…..},	BIT STRING 1536 bit
extensions {		
authorityKeyIdentifier {		
extnId	{2.5.29.35},	
extnValue	…..},	OCTET STRING, 160 bit SHA1 of root subjectPublicKey BIT STRING
subjectAltName {		
extnId	{2.5.29.17},	
extnValue	…..},	SEQUENCE, CONTEXT SPECIFIC RFC822 Name
subjectKeyIdentifier {		
extnId	{2.5.29.14}	
extnValue	…..},	OCTET STRING, 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage {		
extnId	{2.5.29.15},	
critical	TRUE,	BOOLEAN
extnValue	‘010000000},	nonRep

certificatePolicies {		
extnId	{2.5.29.32},	
extnValue	{2.16.756.1.17.3.2.17},	
extnId	{{1.3.6.1.5.5.7.2.2},	
extnValue	{This is the QC EE ClassA CPS},	UTF8String, id-qt-unotice RFC 3280

X.509 Field OIDs/Values Comments

extnId	{1.3.6.1.5.5.7.2.1},	
extnValue	{http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_1_4.pdf}},	IA5String, cps
issuerAltName {		
extnId	{2.5.29.18},	UTF8String, directoryName
extnValue	{ O=ZertES Recognition Body: KPMG Klynveld Peat Marwick Goerdeler SA}},	
crlDistributionPoints {		
extnId	{2.5.29.31},	
extnValue	{http://www.pki.admin.ch/crl/AdminCA-A-T01.crl ldap://admindir.admi.ch/cn=AdminCA-A-T01,ou=Certification Authorities,ou=Services,o=Admin,c=CH c=ch,o=Admin,ou=Services,ou=Certification Authorities,cn=AdminCA-A-T01},	uri IA5String ldap uri IA5String X509 name, IA5String CA inherits Admin-Root-CA CDPs
AuthorityInfoAcess {	SEQUENCE {	
extnId	{1.3.6.1.5.5.7.1.1},	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE {	
accessmethod	{1.3.6.1.5.5.7.48.2},	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia	uri IA5String
AccessDescription	SEQUENCE {	
AccessMethod	{1.3.6.1.5.5.7.48.1},	id-ad-ocsp
accessLocation	http://ocsp.pki.admin.ch}}},	uri IA5String
qcStatments {		
extnId	{1.3.6.1.5.5.7.1.3},	
extnValue	SEQUENCE OF {	OCTET STRING
QCStatment	SEQUENCE {	
statmentId	{0.4.0.1862.1.1}},	qcs-QcCompliance
QCStatment	SEQUENCE {	
statmentId	{0.4.0.1862.1.2},	qcs-QcLimitValue
statmentInfo	SEQUENCE {	monetary value
currency	CHF,	ISO 4217 currency codes
amount	xx,	CHF defined at registration time
exponent	xx}}},	INTEGER defined at registration time
QCStatment	SEQUENCE {	
statmentId	{0.4.0.1862.1.4}}}}}	qcs-QcSSCD

signatureAlgorithm {		
algorithm	{1.2.840.113549.1.1.5}	sha1WithRSAEncryption
parameters	NULL},	
signature	…..	1536 bit BIT STRING

Annex B3 – Time-Stamping Authority (TSA)

X.509 Field	OIDs/Values	Comments
version	2	v3 cert
serialNumber	xxxxx	Integer value defined at key ceremony
signature {		
algorithm	{1.2.840.113549.1.1.5}	sha1WithRSAEncryption
parameters	NULL},	
issuer {	{2.5.4.3: Admin-CA3}, 2.5.4.11:Certification Authorities}, {2.5.4.11:Services}, {2.5.4.10:Admin}, {2.5.4.6:CH}},	Printable String (UTF8String), directoryName
validity {		
notBefore	“YYMMDDHHMMSSZ”,	UTC TIME, ETSI TS 102 280
notAfter	“YYMMDDHHMMSSZ”},	UTC TIME, ETSI TS 102 280
subject {	{2.5.4.3: TSA-A-T01},{2.5.4.11: Server }, {2.5.4.10:Admin}, {2.5.4.6:CH}},	Printable String (UTF8String), directoryName
subjectPublicKeyInfo {		
algorithm {	{1.2.840.113549.1.1.1},	rsaEncryption
parameters	NULL},	
subjectPublicKey {	…..},	BIT STRING 2048 bit
extensions {		
authorityKeyIdentifier {		
extnId	{2.5.29.35},	
extnValue	…..},	OCTET STRING, 160 bit SHA1 of AdminCA3 subjectPublicKey BIT STRING
subjectKeyIdentifier {		
extnId	{2.5.29.14}	
extnValue	…..},	OCTET STRING, 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage {		
extnId	{2.5.29.15},	
critical	TRUE,	BOOLEAN
extnValue	‘000000010},	nonRepudiation

extendedkeyUsage {		
extnId	{2.5.29.37},	
critical	TRUE,	BOOLEAN
extnValue	‘1 3 6 1 5 5 7 3 8},	timeStamping
basicConstraints {		
extnId	{2.5.29.19},	
critical	TRUE,	BOOLEAN
extnValue	{cA FALSE},	BOOLEAN
lengConstraint	0},	INTEGER

 X.509 Field OIDs/Values Comments

certificatePolicies {		
extnId	{2.5.29.32},	
extnValue	{2.16.756.1.17.3.2.18},	
extnId	{{1.3.6.1.5.5.7.2.2},	
extnValue	{This is the TSA CPS},	UTF8String, id-qt-unotice RFC 3280
extnId	{1.3.6.1.5.5.7.2.1},	
extnValue	{http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_1_3.pdf}},	IA5String, cps
issuerAltName {		
extnId	{2.5.29.18},	UTF8String, directoryName
extnValue	{ O=ZertES Recognition Body: KPMG Klynveld Peat Marwick Goerdeler SA}},	
crlDistributionPoints {		
extnId	{2.5.29.31},	
extnValue	{http://www.pki.admin.ch/crl/AdminCA3.crl ldap://admindir.admi.ch/cn=AdminCA3,ou=Certification Authorities,ou=Services,o=Admin,c=CH c=ch,o=Admin,ou=Services,ou=Certification Authorities,cn=AdminCA3},	uri IA5String ldap uri IA5String X509 name, IA5String CA inherits AdminCA3 CDPs
AuthorityInfoAcess {	SEQUENCE {	
extnId	{1.3.6.1.5.5.7.1.1},	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE {	
accessmethod	{1.3.6.1.5.5.7.48.2},	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia}}},	uri IA5String
AccessDescription	SEQUENCE {	
AccessMethod	{1.3.6.1.5.5.7.48.1},	id-ad-ocsp
SubjectInfoAccess {		
extId	{1 3 6 1 5 5 7 1 11},	OCTET STRING
extValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 3},	id-ad-timeStamping
accessLocation	“http://tsa.pki.admin.ch”}}}}}	uri, IA5String
signatureAlgorithm {		
algorithm	{1.2.840.113549.1.1.5}	sha1WithRSAEncryption
parameters	NULL},	
signature	…..	2048 bit BIT STRING

Annex B4 – Certificate Revocation List

X.509 Field	OIDs/Values	Comments
version	2	v3 CRL
signature {		
algorithm	{1.2.840.113549.1.1.5}	sha1WithRSAEncryption
parameters	NULL},	
issuer {	{2.5.4.3:AdminCA-A-T01}, {2.5.4.11:Certification Authorities}, {2.5.4.11:Services}, {2.5.4.10:Admin}, {2.5.4.6:CH}},	Printable String (UTF8String), directoryName
thisUpdate	“YYMMDDHHMMSSZ”,	UTC TIME, ETSI TS 102 280
nextUpdate	“YYMMDDHHMMSSZ”},	UTC TIME, ETSI TS 102 280
subject {	{2.5.4.3: AdminCA-A-T01},{2.5.4.11: Server }, {2.5.4.11:Services}, {2.5.4.10:Admin}, {2.5.4.6:CH}},	Printable String (UTF8String), directoryName
revokedCertificates {	SEQUENCE OF SEQUENCE	
{ userCert serialNumber	xxxx	INTEGER
revocationDate	“YYMMDDHHMMSSZ”,	UTC TIME, ETSI TS 102 280
crlEntryExtensions {{	SEQUENCE OF SEQUENCE	OPTIONAL
invalidityDate	2.5.29.24	
generalizedTime	“YYMMDDHHMMSSZ”,	UTC TIME, ETSI TS 102 280
}}		
{	Context Specific	
{	SEQUENCE	
{	SEQUENCE	
crlNumber	2.5.29.20	INTEGER
}}}		
signature	…..	2048 bit BIT STRING