Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Finance FDF

Federal Office of Information Technology, Systems and Telecommunication FOITT
Basic products
eGovernment

Passport 06

Certification guidelines and regulations

Certificate Practice Statement (CPS) of the Country Signing CA Switzerland

Author	Jürg Porro		
Publication date	08.09.2006		
Version	1.0		
Status	in process	under inspection	authorised for use
	□	□	☒

Staff involved	
PL, TPLs	-
Inspection	Mr. Markus Waldner; Mr. Roman Vanek
Authorisation	Mr. Markus Waldner; Mr. Roman Vanek
Information, notification	Published on www.pki.admin.ch Original: (http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_52_1.pdf) English: (http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_52_1_e.pdf)

Authorisation

Place and date: Bern, 04.09.06

Signed: Waldner

Vanek

Modification checking, inspection, authorisation			
Date	***Version***	***Name / Function***	***Description***
21.06.2006	0.82	J. Porro	First version for internal review
22.06.-26.06.2006	0.84	J. Porro	CSCA and S3 regulations incorporated, minor revisions, legal content.
13.07.2006	0.86	J. Porro	Minor revisions
25.07.2006	0.99	J. Porro	Project description and project issues
31.08.2006	0.99-1/2	J. Porro	Incorporation of review/comments by Messrs Waldner and Vanek
08.09.2006	1.0	J. Porro	Published version

Codesigning Officer BIT PKI

Digital unterschrieben von Codesigning Officer BIT PKI
DN: cn=Codesigning Officer BIT PKI, c=CH, o=admin, ou=Bundesrat, Eidg. Finanzdepartement, Bundesamt fuer Informatik - Telekom., email=Andreas.Zuercher@BIT.admin.ch
Grund: Ich bestätige die Richtigkeit und Integrität dieses Dokuments
Datum: 2006.10.25 15:44:28 +02'00'

Contents

1 General

1.1 Purpose of the document

The present document contains the certification guidelines of the Swiss Country Signing CA (CSCA - Country Signing Certification Authority) and describes the implementation regulations (procedures) for these certification guidelines.

Certification guidelines comprise a body of regulations defining the area of use of certificates for a specified group of users and/or application class with common security requirements.

The implementation regulations of the certification guidelines provide information on how this level of security is ensured.

1.2 Background information

1.2.1 Area of application

These certification guidelines are valid exclusively for certificates that are issued by the CSCA for data signature in Passport06.

The certificates cannot be used for electronic signatures under the terms of the Digital Signature Law.

1.2.2 "Biometric Passport" Pilot Project

In the course of its sittings on 15th September 2004 and 13th April 2005 the Federal Council instructed the Federal Department of Justice and Police (FDJP) to introduce biometric passports in the context of a time- and quantity-limited pilot project.

The FDJP subsequently, in mid-2005, asked the Federal Office of Information Technology, Systems and Telecommunication (FOITT) to act as Public Key Infrastructure (PKI) supplier, and approved the consequent FOITT tender.

In the context of this tender, the corresponding public key infrastructure for biometric passport data signature (both CSCA and signature server) was successfully completed by FOITT.

1.2.3 Outlook

The Swiss people's acceptance of the agreement to participate in Schengen on 5th June 2005 has also produced a change in the situation regarding the definitive introduction of biometric passports in Switzerland.

The Council of the European Union adopted the EU Identity Document Regulation on 13th December 2004 (see paragraph 1.2.4 below). For Switzerland this regulation represents a further step in preparing for Shengen.

This development has to be implemented as soon as possible: at the latest, in any event, within two years of the agreement coming into force. Taking into account the legislative process, as foreseeable from today's perspective, biometric passports and travel documents must be introduced by autumn/early winter 2008, or in the event of a referendum, by the beginning of 2009 at the latest.

1.2.4 Introduction of biometric data in the EU

On 13 December 2004, the EU adopted Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States (the EU Identity Document Regulation) and so laid the basis for the introduction of biometric data in the passports and travel documents of the member states of the European Union (EU) and those of the other Schengen countries. A central element of this regulation is the requirement that in the passport be stored electronically, at the first stage, a facial image, and at the second stage, two fingerprints. The following deadlines for introduction apply:

- 28th August 2006: an electronically stored facial image;
- 28th June 2009: two electronically stored fingerprints.

The obligation to include biometric data only applies to passports and travel documents having a validity of more than twelve months. Unlike the International Civil Aviation Organization (ICAO) and the USA, the EU has laid down a number of binding requirements for the protection of the data stored in the chip to prevent unauthorised reading. Attention is drawn particularly to the protection of data stored in the chip against unauthorised remote access by means of the Basic Access Control (BAC) procedure and the limitations on access to and reading of fingerprints, to be stored in the chip in the future, by means of the Extended Access Control procedure (EAC).

Special access rights for reading fingerprints must therefore be ensured. Thus a country can determine which other country has the right to read the fingerprints stored in the chip. For this, digital certificates will be created and passed on to the authorised countries. By means of these certificates, the individual authorised reading devices will in turn be certified. Fingerprints will then only be readable by a correspondingly certified reading device. For this functionality a further PKI needs to be built (keyword EAC).

1.2.5 National regulations

In Switzerland the introduction of biometric passports has legislative implications. The Identity Document Regulation (SR **143.11**) has to be adapted for the pilot project.

Definitive introduction will require revision of the Identity Document Law AwG (SR **143.1**), the Law on Visits by and Settlement of Foreigners ANAG (SR **142.2**) and/or the Law on Foreigners AuG (BBl 2005 7365), and the Regulation on the Issuance of Travel Documents for Foreigners RDV (SR **143.5**). In addition, incorporation of EU legislation (Schengen) means that corresponding treaties have to be concluded.

1.3 Units responsible for this document

1.3.1 Contact regarding this document and its publication

Federal Office of Information Technology, Systems and Telecommunication - FOITT

e-Government Section, Monbijoustrasse 74, CH-3003 Berne (Service provider)

Andreas Zürcher
Security Officer PKI
andreas.zuercher@bit.admin.ch
+41 (0) 31 323 87 63

Jürg Porro
PL PKI Passport06
juerg.porro@bit.admin.ch
+41 (0) 31 325 87 60

1.3.2 Authorisation procedure for this document

Federal Office of Police (fedpol)

Identity Documents Section, Nussbaumstrasse 29, CH-3003 Berne (contracting authority)

Markus Waldner
GPL, Biometric Passports
markus.waldner@fedpol.admin.ch
+41 (0) 31 325 74 41

Roman Vanek
Head of Identity Documents Section
roman.vanek@fedpol.admin.ch
+41 (0) 31 323 20 77

1.4 Points of contact

Contracting authority (Federal Office of Police - fedpol)

Identity Documents Section; Roman Vanek; 031 323 20 77

General IT (IT Service Centre FDJP ISC- FDJP)

Administrative Applications Section; Fritz Grossenbacher, 031 323 79 05

Passport production (Federal Office for Buildings and Logistics - FBL)

Identity Documents Section; Stephan Horisberger, 031 325 50 07

PKI Operator (Federal Office of Information Technology, Systems and Telecommunication - FOITT)

e-Government Section; Peter Balsiger, 031 325 40 43

1.5 Abbreviations

The following abbreviations are used in this document:

Abbreviation	Description
CA	Certification Authority
CP	Certificate Policy
CPS	Certificate Practice Statement (implementation regulations in respect of certification guidelines)
CRL	Certificate Revocation List (blocking list)
DN	Distinguished Name (name of certificate holder (Subject DN) or certificate issuer (Issuer DN))
DSA	Digital Signature Algorithm.
EAC	Extended Access Control.
EC	Elliptic Curve. Mathematical structure, on which various cryptographical procedures are based.
ECDSA	Variant of DSA signature procedure, which is based on EC. Defined in [X9.62-1998].
FIPS	Federal Information Processing Standards (publication). Standards published by NIST.
ICAO	International Civil Aviation Organization.
NIST	U.S. Department of Commerce / National Institute of Standards and Technology. Sets standards in, amongst other mathematical structures, elliptic curves.
PKD-CH	Public-Key Directory CH. Where, in the context of the adoption of biometric passports, all required information will be accessible to all participating countries.
PKI	Public Key Infrastructure.
RDN	Relative Distinguished Name (O=Organisation, OU=Organisational Unit, L=Locality, ST=State / Province, CN=Common Name, C=Country)
RSA	The Public-Key System developed by Rivest, Shamir and Adleman.

References

Abbreviation	Source
FIPS 186-2	Digital Signature Standard (DSS), NIST, 27th January 2000
X9.62-1998	The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute, 20. September 1998
PKI Spez	Requests to PKI, fedpol (ID: DK000229)
ISDS	Information security and data protection plan, BIT
	Council Regulation (EC) No. 2252/2004 of 13th December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States (Official Journal L 385 of 29.12.2004, P. 1 – 6).
	Decision K(2005) 409 of 28th February 2005 (facial image) and Decision K(2006) 2909 of 28th June 2006 (Amendment; Fingerprints) on the technical specifications on standards and security features and biometrics in passports and travel documents issued by Member States.

2 Implementation regulations

A log of all activity must to be kept regarding the CSCA and the S3 Servers.

2.1 Regulations regarding the CSCA

2.1.1 Generation of the CA key and certificate

The generation of pairs of CA keys has to occur in the context of a ‘root key ceremony’ in a controlled environment under the supervision of an auditor. The CSCA private key (CA key) is to be stored in a Hardware Security Module (HSM) certified to at least FIPS 140-2 Level 3.

The key generation algorithms are to be disclosed at the request of the contracting authority. As source/input for the algorithm, random bits from an HSM certified to at least FIPS 140-2 Level 3 are to be used.

The CSCA certificate is to be created immediately following the ceremony, to be signed with the CA key and to be published in the Federal Admin-Directory service.

In addition the CSCA certificate is to be submitted by the FOITT to the contracting authority, which will then distribute it to further recipients.

2.1.2 Splitting or storing the CA key

The CA key must not be distributed to multiple persons (m out of n entities) and must not be stored.

2.1.3 CA key backup

Implementing the root key ceremony, the CSCA’s private key material must be secured once only according to the standard back up procedure of the HSM on at least three back-up tokens certified to FIPS-140-2 Level 3.

From an organisational point of view it must be ensured that when carrying out the back-up procedure, more than one party is present with their corresponding credentials. No one party may be in complete possession of the necessary credentials for this process.

These back-up tokens are to be kept in geographically separate locations.

2.1.4 CA key restore

The CSCA’s private key material must, in an emergency and on written instructions from the contracting authority, be restored using the standard restore procedure from the HSM by one of the above-mentioned back-up tokens.

From an organisational point of view, it must be ensured that when carrying out the restore procedure, more than one party is present with their corresponding credentials. No one party may be in complete possession of the necessary credentials for this process.

2.1.5 Use of the CA key

Access to the CA key is to be protected by the HSM authentication and authorisation procedures as well as by physical access control.

The CSCA may use its private signature key only to sign its own certificate or document signer certificates and CRLs.

2.1.6 Archiving the CA key

The CA key must not to be archived, other than by means of the above-mentioned back-up.

2.1.7 Deleting the CA key

After its usage period has expired the CA key must be deleted, respectively, the HSM and the backup tokens must be initialised. A new key must be generated in a new ceremony.

2.1.8 Suspension or revocation of the CSCA certificate

It is not intended that the CSCA certificate should be suspended or revoked. If this were, however, to happen, the procedure must be agreed upon by the service provider and the contracting authority within one working day of the event having been ascertained.

2.1.9 Compromised CA key

Were the CA key to be compromised or if there were good reason to suspect that this had occurred, the contracting authority must be informed immediately. Further action will be decided by the contracting authority. The contracting authority and service provider will ensure, within their areas of responsibility, that time limits and specifications are adhered to.

2.1.10 Generation of private document signer keys and certificates

After being generated, private document signer keys (DS keys) must be transferred directly to the secure signature server (S3) and deleted on the CSCA.

Immediately after being generated, the corresponding certificates must be published in the Federal Admin-Directory service, which at the same time functions as an archive.

2.1.11 Suspension or revocation of a document signer certificate

As soon as an order for the revocation of a certificate has been received, the certificate must be revoked by the CSCA. Thereupon a new certificate revocation list (CRL) must be generated and published in the Federal Admin-Directory service.

The contracting authority is immediately to be made aware of the new CRL and will set in motion the further necessary procedures. The contracting authority and service provider will ensure that, in their respective areas of responsibility, time limits and specifications are adhered to.

2.2 Secure signature server (S3) regulations

2.2.1 Use of the DS key

When a document signer key (DS key) is received, it must be immediately stored in a FIPS-140-2 Level 3 certified HSM.

Access to a DS key is to be protected by the HSM authentication and authorisation procedures as well as by physical access controls.

Before the use of a DS key, the S3 must verify the trustworthiness of the data source (cf. origin of the request). The S3 must neither interpret nor verify the data content that is to be signed.

A DS key is to be used exclusively for signing data in biometric passports.

2.2.2 Compromised DS key

Were a DS key to be compromised, or if there were good reason to suspect that this had occurred, the contracting authority must be informed immediately. Further action will be decided by the contracting authority. The contracting authority and service provider will ensure, within their respective areas of responsibility, that time limits and specifications are adhered to.

2.2.3 Backup & restore of DS keys

No backup or restore of DS keys is to be carried out.

2.2.4 Archiving DS keys

DS keys are not to be archived.

2.2.5 Deleting DS keys

After the prescribed period of use (in terms of number of signatures or validity period) DS keys are to be deleted on the HSM of the S3.

3 CSCA Certificates

3.1 Certificate hierarchy

The certificate hierarchy is comprised of a self-signed root CA, which immediately issues the document signing certificates. These document signing certificates all have the same purpose and belong to the same class (issuing process, security features).

3.2 Certificate types

3.2.1 General information

All certificates issued by the CSCA are based on the X.509v3 standard. Only certificates based on cryptographic procedures for elliptic curves over prime fields shall be issued.

SHA-1 is a hash algorithm.

3.2.2 CA certificate

The CA certificate is signed (i.e. self-signed) with the corresponding private key (CA key). Verification of the CA certificate is effected by comparing the hash value (fingerprint) of the CA certificate with the value published by the Federal Office of Information Technology, Systems and Telecommunication (FOITT), noted in this document (see 3.2.2.6 below).

3.2.2.1 Nomenclature

The CA certificate has the following subject and issuer DN:

RDN	Description
C	CH
O	Admin
OU	Services
OU	Certification Authorities
CN	csca-switzerland-1

3.2.2.2 Validity

The validity period of the CA certificate is composed of the maximum lead-in time plus the maximum period of use of a CSCA key plus the validity period of a document signer certificate.

The validity period of a CA certificate is set at 4,082 days.

3.2.2.3 Usage period of the CSCA key (Private Key Usage Period)

The recommended usage period of the CA key is 1,461 days. Start and finish of the usage period are stipulated in the CA certificate in the certificate renewal private key usage period.

The usage period of the CA key is set at 1,827 days.

3.2.2.4 CA key lead-in time

The lead-in time of the CA key is designated as the period of time between the beginning of the validity period and the beginning of the usage period. The lead-in time comprises at least 0 days and at most 31 days.

The lead-in time of the CA key is set at 0 days.

3.2.2.5 Number of biometric identity documents to be issued

The maximum number of biometric identity documents signed with document signer keys from the same CA is set at 5,000,000.

3.2.2.6 Fingerprint

Hash alg.	Fingerprint
SHA-1	A2B6 D663 B233 6191 4D30 B020 0B88 6816 761B DC11
MD5	8ee6 9e68 ba31 435c d8c9 7af1 f428 f601

3.2.2.7 Signature procedure

The CA certificate is signed with ECDSA (self-signed). The CA key is used exclusively for ECDSA signatures.

3.2.2.8 EC parameters

The CA key is based on elliptic curve P-384 in line with [FIPS 186-2]. The EC parameters are given explicitly in the CA certificate, including cofactor.

3.2.2.9 Extensions

The CA certificate contains the following X.509v3 –compatible extensions.

Name	Critical	Value
Private Key Usage Period	No	See paragraph 3.2.2.3.
Certificate Policies	No	Policy: 2.16.756.1.17.3.52.1 CPS: http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_52_1.pdf
Subject Key Identifier	No	4EC8 9D98 C9B4 E090 F52B 5B85 9750 56BF E824 EB76
Key Usage	Yes	Certificate Sign, CRL Sign
Basic Constraints	Yes	CA:TRUE, pathlen:0

3.2.3 Document signer certificates

3.2.3.1 Nomenclature

The document signer certificates have the following subject DN:

RDN	Description
C	CH
O	Admin
OU	Services
OU	Signature-Server
OU	Pass06
CN	ds-001

The issuer DN of the document signer certificates is the subject DN of the CA certificate, in line with paragraph 3.2.2.1.

3.2.3.2 Validity

The validity period of the document signer certificate is composed of the maximum lead-in time plus the maximum validity period of a biometric identity document plus the maximum lead-in time plus the maximum usage period of a document signer key.

The validity period of a document signer certificate is set at 2,224 days.

3.2.3.3 Usage period of a DS key (Private Key Usage Period)

The maximum usage period of a DS key is 366 days. Start and finish of the usage period are stipulated in the document certificate in the certificate renewal private key usage period.

The usage period of a DS key is set at 93 days.

3.2.3.4 DS key lead-in time

The lead-in time of the DS key is designated as the period of time between the beginning of the validity period and the beginning of the usage period. The lead-in time comprises at least 0 days and at most 31 days.

The lead-in time of the DS key is set at 0 days.

3.2.3.5 Number of signatures of a DS key

A DS signer key shall sign a maximum of 100,000 biometric identity documents. The recommended number is 25,000.

The number of signatures of a DS key is set at 25,000.

3.2.3.6 Signature procedure

The document signer certificates are signed by means of the CA key with ECDSA. The DS keys are used exclusively for ECDSA signatures.

3.2.3.7 EC parameters

The DS keys are based on elliptic curve P-256 in line with [FIPS 186-2]. The EC parameters are given explicitly in the document signer certificate, including cofactor.

3.2.3.8 Extensions

The document signer certificates contain the following X.509v3–compatible extensions.

Name	Critical	Value
Private Key Usage Period	No	See paragraph 3.2.2.3.
Certificate Policies	No	Policy: 2.16.756.1.17.3.52.1 CPS: http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_52_1.pdf
Authority Key Identifier	No	4EC8 9D98 C9B4 E090 F52B 5B85 9750 56BF E824 EB76
Key Usage	Yes	Digital Signature

4 CA infrastructure

The CSCA is not a public body; it is under the authority of the Federal Office of Police and is administered by the Federal Office of Information Technology, Systems and Telecommunication (FOITT).

4.1 Physical security

4.1.1 Locations

The CSCA is administered in the PKI area of Federal Office of Information Technology, Systems and Telecommunication (FOITT). This is a secure area, dedicated exclusively to public key infrastructures.

The secure signature servers (S3) are located in a special area of the Media Center Bund (MCB) within the Federal Office for Buildings and Logistics (FBL). The MCB is also a secure area with restricted access.

4.1.1.1 Access control

Only persons identifiable by name bearing special badges have access to the area housing the CSCA system. Other persons (e.g. maintenance staff) shall have access only if accompanied by authorised personnel; such access shall be logged.

Only a small number of persons identifiable by name shall have access to the area housing the S3. An additional key shall be kept in a safe, to which a small number of persons have access. Other persons have access only if accompanied by authorised personnel. In addition, the area housing the S3 shall be under video surveillance.

4.1.1.2 Power supply and air conditioning

The areas (housing the CSCA and the S3) shall be equipped with an air conditioning system to regulate temperature and humidity. All electrical components shall be connected to an interruption-free power supply.

4.1.1.3 Water damage

The areas (housing the CSCA and the S3) shall be equipped with water sensors which are directly linked to the building’s security centre. In the event of an alarm sounding, the aforementioned IT equipment will be automatically shut down and the power supply cut off.

4.1.1.4 Fire prevention and fire fighting

The areas (housing the CSCA and the S3) shall be equipped with smoke sensors which are directly linked to the building’s security centre. In the event of a fire alarm sounding, the aforementioned IT equipment will be automatically shut down and the power supply cut off.

4.1.1.5 Storage of data medium

Data medium containing information relating to the CSCA, including safety copies, shall be kept in the fireproof safe in the PKI area.

CSCA files meriting protection shall be kept in at least two separate buildings.

4.2 Personnel security

4.2.1 Security testing of personnel

CSCA personnel shall be drawn from FOITT staff. They shall possess the necessary qualifications and experience to provide PKI services and normally work full time for the PKI.

The employment contract of each staff member shall include a confidentiality clause. All FOITT PKI staff members shall have undergone, on commencing their service, a personnel security test in line with article 1, section 1, subsection a, of the regulations governing security tests in respect of persons.

4.2.2 Identification and authentication of each person

Technical access to individual IT systems shall be realised by means of user recognition and password or smartcard and password. Cryptographic devices such as HSMs and CA servers are subject to special authentication procedures.

4.2.3 Necessary number of persons for fulfilment of tasks

The fulfilment of the following processes requires the presence of at least two persons with different roles:

- Generating the CA key,
- Backup and Recovery of the CA key,
- Replacing the hardware containing the CA key or the DS key.

The two persons shall have equal responsibility for protecting the information and credentials necessary in sensitive transactions. Neither of these persons, alone, shall be in a position to use this information or have access to it.

All other tasks, including generating DS keys, may be carried out by a single authorised person.

4.3 Security regulations for the installed system

4.3.1 Special security requirements

The CSCA and the S3 shall be operated on a programmable Hardware Security Module (HSM). This HSM shall be certified to FIPS 140-2 Level 3 or higher. The applications shall run on specially reinforced systems (LINUX).

4.3.2 Software development

Software development for the CSCA and the S3 shall be carried out by qualified staff. Modified software shall be adopted on the productive systems only after a defined testing and acceptance procedure.

4.3.3 Data protection and data security

Data protection, data security and risk analysis shall be handled in the context of the Information Security and Data Protection Plan (ISDS) established by the FOITT.

4.3.4 Network security

The CSCA and the S3 shall be protected against illegal access by several firewalls. Administrative access to the CSCA and the S3 shall be possible only from the Admin workstation over mutually authenticated SSH connections.

Access of the DPSS (passport production partner system) to the productive S3s shall be possible only over mutually authenticated HTTPS connections.

4.3.5 Faults/maintenance

The hardware used for the CSCA may only be removed from the PKI area with written consent and according to the requirements of the FOITT PKI security officer. In particular, no components may be introduced or exchanged. The contracting authority is to be informed immediately.

4.4 Directory services

4.4.1 Admin Directory

Certificates generated by the Passport06 Switzerland (PCH06) PKI shall be published in the electronic Admin-Directory service.

The Admin-Directory is an internal directory service of the federal government in compliance with the ITU-T’s X.500 standard. The service shall be accessible through HTTP protocol at www.verzeichnisse.admin.ch (for persons) and through LDAP protocol at admindir.admin.ch (port 389; for further objects such as CA or server certificates). The public part of the directory service, the Admin-Directory Public, is accessible via the Internet.

Note: the directory relevant to the operative processes of passport use is Public-Key Directory CH (PKD-CH). The corresponding information is copied there from the Admin Directory.

5 Further commercial and legal aspects

5.1 Cessation of activity

The Federal Office of Information Technology, Systems and Telecommunication (FOITT) shall inform the parties concerned in good time, but at least six months in advance, if a cessation of the activities of the CA infrastructure is foreseen.

Issued certificates and CA infrastructure log files shall be archived. The safe custody period is in line with the contracting authority's applicable archive regulations.

5.2 Certification and auditing

The contracting authority shall inform the operator as soon as possible of any certifications or audits that are to be carried out. The costs incurred shall be divided between the contracting authority and the service provider. The contracting authority shall bear 100% of the costs only if the costs or the profit can be attributed solely to the application or the processes in connection with the biometric passport.

5.3 Fees

Fees for FOITT services in respect of the CSCA are contained in the FOITT tender package for the maintenance and operation of the applications for the CSCA and the S3. Details are regulated in the corresponding service level agreement (SLA). The SLA shall be adjusted as necessary.

5.4 Insurance cover

Not applicable.

5.5 Confidentiality of commercial information

As CSCA and S3 operator, the FOITT bears the responsibility for measures to protect confidential information. Data may be handled only in the context of the provision of services and may only be passed on to third parties if a declaration of confidentiality has previously been signed, and personnel entrusted with the work have been bound to observe the legal requirements in respect of data protection.

For auditing and inspection purposes, confidential documents may be examined in the presence of the FOITT official responsible for operational security.

5.6 Obligation to produce documents

The service provider shall submit to the contracting authority on demand those documents, descriptive texts and regulations in respect of the 'Country Signing CA Switzerland' for examination.

5.7 Right of use

For further or other use of systems established in the context of the ‘biometric passport’ pilot project (CSCA or S3) or of any follow-on projects, the written consent of the contracting authority is to be sought.

Should the service provider cease operation or if the administration of ‘Country Signing CA Switzerland’ were to be transferred to another unit, the contracting authority can make available to the new unit the programs, applications and the components it has financed, including documentation. Allowance is to be made for the legitimate confidentiality interests of the service provider.

5.8 Confidentiality of personal data

In the context of the operation of the CSCA and the S3, personal data will be processed by the FOITT. These data shall neither be processed nor stored. Moreover, the provisions of the Data Protection Law apply.

5.9 Warranty exclusion

Not applicable.

5.10 Limitation of liability and compensation for damages

Not applicable.

5.11 Jurisdiction

Not applicable.

5.12 Mediation bodies

Mediation shall be at directorate level of the departments directly concerned, as indicated in 1.4 Points of contact.

5.13 Entry into force and cancellation

This document entered into force with its publication on the first day of production of biometric passports and is valid until it is replaced by another version. If a new version is published, this will replace all previous versions.

It is not anticipated that the CSCA will be terminated.

5.14 Area of applicability

All the regulations contained in this document apply to relations between the operator of the CSCA and the S3, the passport producer and the contracting authority.

5.15 Language

This document was originally written in the German language. In the case of discrepancies in translations, the German version is authoritative.