Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

Internal

Class B: RIO Application for the issuance of Class B certificates

Form for the transmission of the applicant information to the LRAO

V1.3, 23.02.2024

1 Applicant details (to be completed by the applicant and sent to the RIO)

The applicant hereby orders a prepared smartcard for the issuance of class B certificates of the Swiss Government PKI:

Last name, first name:

Departement/Office: First card ○ Replacement ○

FDFA email address: FDFA

Phone number:

2 Identification and card allocation (to be completed by RIO together with the applicant and sent to the LRAO).

The applicant receives a smartcard from the RIO, which can be unsealed using the S-PIN they have been notified of/sent after the LRA officer approves the application.

The RIO hands out to the applicant the smart card with
the following identification number: **Serial number** (mandatory): ___________________________

The RIO and the applicant confirm with their signature that a personal meeting, the handing over of the smart card with the above mentioned serial number and the identification by means of a valid travel document have taken place:

RIO:	**Applicant:**
Name, first name: ____________________________ (in block letters)	S/N of ID/passport ____________________
Place, date	Place/Date: ___________________________
Signature: _________________________________	Signature: ____________________________

3 Terms and conditions of use

The RIO ensures that the applicant has understood and received a copy of the Subscriber agreement and conditions of use for Class B. The applicant must sign a second copy, which the RIO submits to the LRA officer together with the current document (duly completed) and a copy of the applicant’s travel document.

4 Copy of travel document

A copy of the applicant's valid travel document must be made on the reverse side of this document. Identity cards must necessarily be copied on both sides. Passport copies please always with the pages of the photo, signature and validity date. The reverse side, as well as any additional pages required, must be marked with the place, date and signature of both parties. The back of this document serves as a template for the copies.

[Original travel/identity documents to be copied here].

RIO:	**Applicant:**
Place, date: ________________________________	Place, date: ___________________________
Signature: _________________________________	Signature: ___________________________

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Departement of Finance FDF

Federal Office of Information Technology, Systems and Telecommunication FOITT
Swiss Government PKI

NOT CLASSIFIED

Subscriber agreement and conditions of use for Class B

For Swiss Government PKI personal advanced certificates for federal authorities of the Swiss Confederation

V1.1, 31.03.2017

In its role as certification service provider (CSP), the Swiss Government PKI operates the PKI (public key infrastructure) of the federal authorities of the Swiss Confederation on behalf of the Federal IT Steering Unit (FITSU). Class B certificates are defined as part of the "SD005 - Standard Service Market Model: Identity and Access Management (IAM)". The acquisition and use of Swiss Government PKI Class B certificates are subject to the provisions of this document. These are adjusted annually by the Swiss Government PKI (SG-PKI) in line with the valid legal and normative requirements applying to Public Key Infrastructures. The guidelines are an integral component of these terms of agreement and use. The currently valid version is published on www.pki.admin.ch. All holders are notified by e-mail of the publication of an updated version of this document.

The "Guidelines on Swiss Government PKI Class B certificates" must also be observed. These must be accepted separately when obtaining a Class B certificate.

Completeness and accuracy of information

The holder of Swiss Government PKI Class B certificates (hereinafter referred to as the "holder"[1]) undertakes to supply the CSP at all times with correct and complete information required for the process of issuing them and for their content. Before the certificates are issued, the client must be identified in person on the basis of a valid travel document. The certificates are inseparably associated with this client.

The client's first name(s), surname(s), Admin-Directory suffix and e-mail address are always listed in the certificates. Additional personal details of the holder such as his revocation passphrases and a scan of his valid travel document are recorded by the Swiss Government PKI.

The client is required to notify the CSP without delay of any change in his personal data, especially his first name, surname, suffix (his entry in the federal government's Admin-Directory) and e-mail address.

Protection of private keys and certificates

The holder also undertakes to take all appropriate precautions to ensure that he retains sole control of his private keys and any activation data (e.g. PIN/PUK) and media (e.g. Smartcard) associated with them, and that they are kept confidential and protected from loss and misuse. The certificate's private keys can and may only be used in connection with the certificates and only for the purpose set out in the certificates (signature, authentication, encryption). They may be made accessible on no account to unauthorised third parties. The holder is liable for any damage arising from the disclosure to third parties of the private keys and any activation data and media associated with them.

The CSP reserves the right to revoke the certificates without notifying the holder in advance if there are specific suspicions of misuse or unauthorised access to the private keys.

[1] Terms used in this document denoting one gender also cover the other.

Use of the certificates

The holder declares that he is familiar with the content, purpose and effect of the use of the Class B certificates. He undertakes to use the Class B certificates and their private keys only for authorised transactions and in compliance with all valid legal requirements and the provisions of this document.

Reporting and revocation

The holder also undertakes immediately to stop using the certificates and the associated private keys and ask the CSP to revoke them:

- in the event of specific suspicions that the certificates have been used for dubious activities (misuse of the activation data, the signature certificate or the encryption certificate)
- if the information in the certificates is no longer correct or accurate, or it will no longer be in the near future.

The CSP's instructions must be followed immediately where it is suspected that a certificate has been misused or compromised.

The CSP can transfer data relating to the holder, the certificates and other directly connected information to other responsible agencies, CSPs, companies and industrial groups if the certificates or the person using them is identified as the source of misuse if this is necessary for reasons of security and permitted by data protection law.

In the interest of traceability, all information concerning revocation will be archived by the CSP.

Termination of certificates usage

The holder also undertakes immediately to stop using the certificates once they have expired or been revoked (especially because they have been compromised).

Responsibility and liability

The holder is responsible for ensuring that the Class B certificates and their private keys are only used in compliance with the provisions of this document in the section on "Using the certificates". Any breach of this requirement will result in revocation and further administrative and possibly legal measures. The holder bears the responsibility for all signatures, authentications and encryptions carried out by him, and also for any resulting damage and its consequences.

Declaration of acknowledgement and consent

The holder notes that the CSP will revoke the certificates without delay in the event of a specific suspicion of misuse, a breach of the provisions of this document or a breach of any other valid legal provisions.

By appending his signature, the holder declares that he has read and understood the present document "Class B subscriber agreement and terms of use", and that he accepts the provisions listed herein.

Place, date: ______________________________ Signature: ________________________________

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department for Foreign Affairs FDFA
Directorate for Resources / Information Technology FDFA
Swiss Government PKI

Checklist for the RIO

V 2.1, 20.09.2019

No.	Description of the task	Result (OK / NOK)	**Date**
1	Check application and verify plausibility (this person is authorised to obtain Swiss Government PKI Class B certificates and is registered in the Admin Directory of the Confederation)		
2	Verify identity by comparing the valid travel document with the application form (only valid identity card or passport accepted).		
	Name:		
	Type of travel document according to the application form (only valid identity card or valid passport) Serial number of the document: Validity of the travel document:	□ ID □ Pass	
	Compare face of applicant with facial image in travel document.		
3	Hand over the SmartCard to the User and make him aware that from this moment on he must always keep the card under his sole control. Serial number of the SmartCard		
4	Fill in part 2 of the application form, including signatures		
5	"User Agreement and Usage Guidelines" and "Guidelines Class B Certificates of the Swiss Government PKI" to the Customers explain		
6	"User Agreement and Usage Guidelines" and "Guidelines Class B Certificates of the Swiss Government PKI" in duplicate to the customer, have a copy of the User Agreement signed and collect it again.		
7	Copy ID document on back of application (ID on both sides!)		
8	Sign all pages with copies of documents and have them countersigned by the customer		
9	For foreign identity cards from non-EU/EFTA countries and if required (clarify in advance in case of doubt): The site manager confirms the following facts about the identity document used: -It is a proof of identity accepted in the relevant country. - The identity document is issued by a government agency. - The identity document was sufficient to verify the identity of the person to carry out the intended work.	Name & Signature CFPA / Operations Manager	
10	Sign the checklist.		
11	Sending the documents to the LRAO (Helpdesk): "User Agreement and Usage Guidelines", Completed Application Form, this Checklist RIO In case of electronic transmission: send the signed documents with a signed and encrypted e-mail to the responsible LRA officer.		

RIO Name/First Name:	Organizational Unit:	Place, date:

Signature RIO: ____________________________________