Guidelines on Swiss Government PKI class B certificates

Explanations on obtaining and using Swiss Government PKI class B certificates

V1.0, 09.03.2017

1 Purpose of class B certificates

Purpose

Class B certificates are defined as part of "SD005 – Standard Service Market Model: Identity and Access Management (IAM)". Class B certificates can be used for the following purposes:

- Trusted data signatures, which ensure that data is authentic and intact
- Data encryption, which ensures that data is confidential
- Authentication of individuals, whereby the certificate reliably identifies the holder for identification components such as entry portals

The identity of the certificate holder is established at a high security level by means of extended verification and security mechanisms during the issuing process for class B certificates. Class B certificates are always issued in person and only after the holder has been identified by means of a valid travel document that authorises entry into Switzerland.

Excluded purpose

Class B certificates serve only the purposes mentioned above. They provide no other information, assurances or guarantees. In particular, class B certificates do not guarantee correct and legal use of the certificate by the holder.
Furthermore, class B certificates do not guarantee that:

- the holder named in the certificate is actively involved in business activities;
- the holder named in the certificate is compliant with the applicable statutory provisions;
- the holder named in the certificate is trustworthy and acts professionally in the business environment; or
- the holder named in the certificate has the specialist, technical, organisational or other skills to use this certificate correctly.

2 Quality of class B certificates

When a class B certificate is issued for the first time, the SG PKI LRA officer follows the processes set out in the registration guidelines, which define the steps that are necessary and appropriate in order to confirm the following facts:

- **Legally valid existence:** the holder named in the class B certificate exists as a natural person and has a personal entry in AdminDir.
- **Identity:** the name of the holder named in the class B certificate is the same as the name in their valid travel document.
- **Authorisation:** the holder named in the class B certificate is authorised to obtain the certificate.
- **Data accuracy:** all of the data and information contained in the certificate are correct.
- **Agreement/terms of use:** the holder named in the class B certificate has been notified by the LRAO (local registration authority officer) of the rights and obligations described in the "Class B user agreement and terms of

use". The LRAO has answered any questions in this regard in a comprehensible manner. The holder has read, accepted and signed the "Class B user agreement and terms of use".

- **Status:** the SG PKI makes the status of the certificate and information on its validity/revocation available online.
- **Revocation:** the SG PKI can revoke the class B certificate immediately for the reasons set out in the "Class B user agreement and terms of use".

3 Policies

All valid statutory requirements, policies (including CP/CPS) and guidelines for class B certificates are published online on the SG PKI website: www.pki.admin.ch.

4 Content and validity of class B certificates

Content

The SG PKI class B certificate contains:

- the publisher and issuing CA
- information about the issuing CA's root CA
- information about the policy applied
- the certificate's date of issue and expiry
- the certificate's serial number
- the intended purpose of the certificate
- information about the CRL and the OCSP
- information about the CA's auditors
- information about the holder of the certificate according to their entry in AdminDir when the certificate was first issued:
    - the common name of the holder
    - email address
    - UPN

Validity

SG PKI class B certificates are valid for a maximum of three years. The holder can renew the certificate a maximum of two times for a further three years each time before the three-year period in question expires. The holder can use the Rekeying Wizard to renew the certificate. After the third period of validity expires, a new certificate must be issued by the LRA officer. The process is the same as that for when a certificate is first issued.

5 Obtaining class B certificates

Procedure

The following documents and/or registrations are required in order to obtain SG PKI class B certificates:

- a valid travel document (ID/passport) issued to the applicant and entitling them to enter Switzerland
- a completed and (electronically) signed application form for Swiss Government PKI class B certificates, or an application through the office's line management or the prescribed internal HR process
- the signed "Class B user agreement and terms of use" (printed out by the LRA officer together with this document at the end of every class B certificate issue process)
- a personal entry in AdminDir, including surname(s), first name(s) (according to the travel document), a valid email address and optionally a UPN (user principal name) entry

Identification

The applicant is personally identified by the SG PKI class B LRAOs when the certificate is first issued, and again when its third period of validity expires, at the latest. When class B certificates are issued in a decentralised manner, applicants are personally identified by the RIO (registration identification officer), a delegate of the LRAO, who confirms to the LRAO that identification has taken place for the approval of the application.

In order to identify the applicant, their travel document is checked to ensure that it is valid, correct and genuine. LRAOs are also required to ensure that the photo on the document is that of the applicant. Before a personal certificate is issued, the application is plausibility-tested. Does the applicant really work at the organisational unit indicated in AdminDir, do they need the certificate in their day-to-day work, and are they entitled to apply for a certificate?

Binding character

The application or the internal process for submitting an application must be approved by the competent units. These guidelines and the "Class B user agreement and terms of use" must be accepted and (digitally) signed by the applicant.

6 Protecting the private key and certificate

Transferability

Class B certificates are always personal and non-transferable. The holder's personal details are stored both in the certificate and with the SG PKI.

PIN/PUK

The PIN must be different from other passwords and may not be accessible to third parties. It need not be changed regularly unless there are definite suspicions that a third party has become aware of it.

The certificate (and thus the certificate carrier – smartcard, USB flash drive, etc.) must be secured with a PIN of at least six characters. PINs may be purely numeric or mixed. In order to prevent the misuse of their personal electronic identities, holders may never disclose the PIN to third parties.

The smartcard PUK must comprise at least eight characters. The foregoing PIN rules also apply to the PUK.

Notification duty

The holder must immediately report the loss of the smartcard to the competent LRAO or the IT service organisation. The certificates affected will then be blocked (revoked) and the block will be published on a public electronic blocking list. Even if the smartcard is found again, the certificates will remain blocked and invalid. As soon as the block is in place, a new class B certificate can be requested from the competent LRAO. The process for issuing a new class B certificate is the same as the process for issuing the first one.

A change of organisation, a name change (e.g. due to marriage) or changes to your email address require a new certificate to be issued (first issue).

7 Revocation

Revocation requests must be submitted to the LRAO. Authorised persons (see full list below) have access to a form on the SG PKI website www.pki.admin.ch. If the revocation is requested by telephone, the LRAO will identify the applicant using their revocation passphrase and personal details (date and place of birth, etc.). Only applicants themselves are authorised to request revocation by telephone. Other persons who may apply for revocation must do so in writing.

Authorised persons are as follows:

- certificate holder
- SG PKI manager

- SG PKI security officer
- the following persons with responsibility for the certificate holder:
  - Human Resources staff
  - line managers
  - LRA officer
  - ISBO
  - ISBD
  - organisation's PKI manager

8 Certificate content

Authentication key
Fingerprint (SHA-1):
Certificate validity:
Serial #:

Encryption key
Fingerprint (SHA-1):
Certificate validity:
Serial #:

Signing key
Fingerprint (SHA-1):
Certificate validity:
Serial #:

9 Acceptance/confirmation of receipt of the smartcard

By signing, the certificate holder confirms that:

- the data stored in the certificate is correct
- they have received the smartcard
- they have read these guidelines and discussed them with the LRAO, and any questions have been answered by the LRAO in a comprehensible manner
- they understand and accept the rights and obligations arising from these guidelines
- they will implement the guidelines described herein

Additional questions may be emailed to the Swiss Government PKI at pki-info@bit.admin.ch[1].

Common name (CN):

Date of issue: **Signature:** _____

[1] You should also read the *user agreement and terms of use for Swiss Government PKI class B certificates*. A signed copy of this document is required when ordering your class B certificate. www.pki.admin.ch