Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Finance FDF

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

25.06.2025

# User Agreement and Terms and Conditions for Advanced Class B Certificates (for natural person) of the Swiss Government PKI

Entry into force: 01.08.2025 V2.0

The Swiss Government PKI of the Federal Office of Information Technology, Systems and Telecommunication (FOITT), in its role as trust service provider (TSP), operates the PKI (public key infrastructure) of the federal authorities of the Swiss Confederation on behalf of the DTI (Digital Transformation and ICT Steering). The class B certificates for the advanced signature in accordance with the ESigA, for authentication and for encryption are issued as part of the standard service "SD005 – Standard Service Market Model: Identity and Access Management (IAM)".

The acquisition and use of these Swiss Government PKI (SG PKI) certificates are subject to the provisions of this document. These are reviewed annually by the SG PKI and, if necessary, adapted to the applicable legal requirements and the normative requirements for public key infrastructures.

The version currently in force is published at Swiss Government PKI. All holders of such certificates will be informed of the publication of an updated version of this document by email. The new version is deemed to have been tacitly accepted 30 days after this information is sent, unless an order for immediate revocation of the certificates is made during this period.

**Note:** The glossary can be found on the PKI homepage.

## Contents

## 1. Completeness and accuracy of information

The natural person holding Swiss Government PKI class B certificates (hereinafter referred to as the "holder"[1]) undertakes to provide the TSP with the correct and complete information required for the issuing process, and for the content of the certificate, at all times. The identity of the person requesting the certificate (hereinafter referred to as the "requester[2]") is set at a high security level by means of extended verification and security mechanisms during the certificate issuing process. For example, before the certificate is issued, the requester must be identified in person by means of a travel document valid for entry into Switzerland. The certificate is inseparably linked to the holder.

The holder's first name(s)/last name(s), suffix and email address are always listed in the certificate (entry in the federal Admin Directory). Further personal details such as date of birth and revocation passphrases, as well as the scan of the valid identification document are recorded and stored by the SG PKI.

The holder is obliged to inform the TSP as soon as the data stored in the certificate changes.

## 2. Protection of private keys and certificates

The private keys of the class B certificates are stored on a personal smartcard. In order to activate the private keys to generate an electronic signature, and for authentication and/or decryption purposes, the holder must use the class B smartcard PIN. The smartcard PIN can be changed independently by the holder in the Safenet Authentication Client (SAC) if required. A PIN may be used for only one smartcard; if a smartcard is replaced, a new PIN must be chosen. This PIN should not be used for any other purpose (e.g. Postcard). The PIN must not be passed on to anyone else and must be changed as soon as there is any suspicion that another person has obtained access to it. The certificates (and therefore the certificate carrier: smartcard, USB stick, etc.) must be secured with a PIN of at least 6 characters (max. 14 characters), whereby purely numeric PINs and mixed PINs are permitted. Special characters are explicitly not permitted in class B certificate PINs. The holder undertakes to take all reasonable precautions to ensure sole control, confidentiality and protection against loss and misuse of the private keys and any associated activation data (PIN) and smartcard. The private keys for the certificates can and may only be used in connection with the certificates and only for the purposes specified in the certificates (signature, authentication, encryption).

If the holder forgets the PIN or enters it incorrectly several times, the holder can set a new PIN by contacting a PIN reset superuser authorised by the SG PKI and having them identify the holder. This identification can be carried out with a passphrase defined at the time of issue and the appropriate answer. The PIN reset superuser releases an eTicket and the holder can set a new PIN after re-identification with a PIN reset user (PRU) specified by the organisation.

Private keys of class B certificates are not transferable and must not be made accessible to unauthorised[3] third parties under any circumstances. The private keys of class B certificates are labelled as non-exportable on the certificate carrier (e.g. smartcard).

[1] The term "holder" describes the natural person to whom the certificate was issued.

[2] The term ‘applicant’ describes the natural person applying for the certificate.

[3] In the context of this document, the term "unauthorised third party" includes any other person who has not been authorised to recover information on the certificate due to death or judicial proceedings.

The holder is liable for any damage caused by the disclosure to third parties of the private keys, the key access data or any associated activation data or smartcard.

The smartcards used fulfil the requirements of the ESigA. All components must also have been approved by the FOITT. A list of approved components is published on Class B - Standards, rules and legal basis.

The trust service provider (TSP) reserves the right to revoke the certificates immediately in the event of specific suspicion of misuse or unauthorised access to the private key without prior notification.

## 3. Acceptance of the certificate

The certificate holder checks the content of the certificate on receipt and ensures that it is correct for the entire period of validity.

## 4. Use of the certificates

Advanced class B certificates for natural persons can be used for the following purposes:

- Trusted data signatures. This ensures the authenticity and integrity of the data.
- Data encryption. Ensures that data remains confidential.
- Authentication of individuals. The certificate reliably identifies the holder to identification equipment such as entry portals.

The holder ensures that they are aware of the content, purpose and effect of the use of the class B certificates. They undertake to use the class B certificates and their private keys only for authorised transactions and in compliance with the applicable legal requirements (see section Legal basis, validity of the documents and contractual elements8 Legal basis, validity of the documents and contractual elements) and the provisions of this document.

Advanced class B certificates fulfil exclusively the above-mentioned purpose and do not provide any further information, assurances or guarantees. In particular, advanced class B certificates do not guarantee that the holder will act correctly and legally when using the certificate.

Furthermore, advanced class B certificates do not guarantee that:

- the holder named in the certificate is actively involved in the business activities;
- the holder named in the certificate complies with the applicable legal requirements;
- the holder named in the certificate is trustworthy and acts with integrity in the business environment; or
- the holder named in the certificate has the professional, technical, organisational or other expertise to use this certificate correctly.

The Swiss Government PKI confirms the following facts at the time of initial issue of an advanced class B certificate:

- *Legally valid existence:* The holder named in the certificate exists as a natural person and has a personal entry in the federal Admin Directory.
- *Identity:* The holder's name stated in the certificate matches the name in their valid identification document.
- *Authorisation:* The SG PKI has taken all necessary and reasonable steps to verify that the holder named in the certificate is authorised to obtain the certificate.
- *Accuracy of the data:* The SG PKI has taken all necessary and reasonable steps to ensure that all data and information contained in the certificate are correct.
- *Status:* The SG PKI makes the status of the certificate and information about its validity/revocation available online 24/7 and thus fulfils the legal requirements.

If you have any questions or problems using the certificates, you can contact your local service desk or the FOITT Service Desk (Tel.: +41 (0)58 465 88 88). For a complaints procedure or questions about this document, the SG PKI can be contacted by email at pki-info@bit.admin.ch.

## 5. Reporting and revocation

- The holder undertakes to immediately stop using the certificates and the associated private keys, and to immediately request the revocation (invalidation) of the certificates from the TSP (e.g. local registration authority officer/LRAO of the SG PKI in the holder's organisation) if:
- there is a definite suspicion that suspicious activities (compromise/abuse of the activation data, the authentication certificate, the signature certificate or the encryption certificate) have been performed with a certificate;
- the information in the certificates is no longer correct or is inaccurate, or will no longer be in the near future;
- a possible loss of the smartcard is discovered.

The instructions of the TSP must be followed without delay, particularly in the event of suspected compromise or misuse of the certificates.

The holder can request a revocation in person or by telephone. The TSP or the person authorised by the TSP (e.g. LRAO) will identify the holder.

Other persons authorised to request a revocation must submit the request in writing using the (electronic) revocation form. Authorised persons are:

- the holder themselves
- the holder's line manager(s)
- the SG PKI manager
- the SG PKI security officer
- the responsible LRAO of the SG PKI
- the IT security officer of the organisational unit (ITSOO) or the department (ITSOD)
- employees of the Human Resources (HR) department responsible for the holder

As soon as the certificate has been revoked, a request can be made to the TSP for new certificates to be issued. The process for issuing new certificates is the same as for the initial issue.

Information relating to identification, the issuance of certificates and revocation is recorded by the TSP for reasons of traceability, and processed and stored in accordance with the legal requirements. The retention period of 11 years begins when the certificates expire or are declared invalid.

If required for security reasons and permitted under data protection law, the TSP may forward data about the holder, the certificates and other directly related information to other competent bodies, TSPs, companies and industrial groups if the certificates or the holder using the certificates are identified as a source of misuse.

## 6. Termination of the use of the certificates

The holder undertakes to cease using the certificates immediately after their expiry or revocation (in particular due to a compromise).

## 7. Responsibility and liability

The holder is responsible for ensuring that their class B certificates and the associated private keys are only used in compliance with the provisions in the section Use of the certificatesUse of the certificates (section 4) of this document. Failure to comply with this requirement will result in revocation of the certificates and, if necessary, further administrative and legal measures. The holder is responsible for all

signatures, authentications and encryptions performed by them, as well as for any damage resulting from improper use and the associated consequences.

## 8. Legal basis, validity of the documents and contractual elements

The following legal bases and other requirements form an integral part of this user agreement. They are listed in the applicable order of precedence:

1. Federal Act on Certification Services in relation to Electronic Signatures and other Uses of Digital Certificates ESigA, SR 943.03
2. Ordinance on Certification Services for Electronic Signatures and other Uses of Digital Certificates CertESO, SR 943.032
3. OFCOM Ordinance on Certification Services for Electronic Signatures and other Uses of Digital Certificates SR 943.032.1
4. CP/CPS root CA I of the SG PKI
5. « Convention et conditions d'utilisation des certificats avancés de classe B (pour les personnes physiques) de Swiss Government PKI » (present document)
6. Normative requirements for public key infrastructures

The applicable legal requirements, policies and guidelines for regulated and advanced class B certificates are published or linked on the Swiss Government PKI website Class B - Standards, rules and legal basis.

## 9. Content and validity of advanced class B certificates

The SG PKI certificates contain information concerning:

- Publisher (TSP) and issuing certificate authority (CA)
- Information about the issuing CA's root CA
- Information about the applicable policy
- Certificate's date of issue and expiry
- Certificate serial number
- Information about the CRL and the OCSP
- Information about the certificate holder at the time of initial issue:
- First name(s), surname(s) and suffix from the Admin Directory (holder's common name (CN))
- Holder's email address
- User principal name (UPN) (optional)
- Public key

The certificates are valid for a maximum of three years. Before the three-year period expires, the certificates can be renewed a maximum of two times by the holder for a further three years. The certificate holder can use the Renewal Wizard to renew the certificate. After the third period of validity expires, a new certificate must be issued by the LRAO, using the process for an initial issue. In such cases, the issue procedure remains the same as for an initial issue. A personal appointment involving a re-identification and the necessary documents is required.

## 10. Requesing and obtaining class B certificates

The following documents and registrations are required to obtain advanced class B certificates from the SG PKI:

- A travel document (ID/passport) valid for entry into Switzerland, issued to the future holder. The expiry date must not have elapsed.
- Completed and signed (electronically, min. with class B) request form for SG PKI class B certificates or a written request through the organisation's line management or via the internally defined HR process.
- Personal entry in the federal Admin Directory, with surname(s), first name(s) (as per travel document), valid email address and optionally a user principal name (so-called UPN entry).
- The signed "[Titel]" (present document)

The requester is personally identified by the SG PKI class B local registration authority officer (LRAO) when the certificate is first issued and at the latest after the third period of validity has expired. When class B certificates are issued in a decentralised manner, requesters are personally identified by the RIO (registration identification officer), a person delegated by the LRAO, who confirms to the LRAO that identification has taken place for the approval of the request. The requester must appear in person for the certificate to be issued. In order to verify and identify the requester, the LRAO or RIO will check the validity, accuracy and authenticity of the travel document when the certificate is issued. The LRAO and RIO are also required to ensure that the photo on the document is that of the requester. Before an advanced certificate is issued, the request is plausibility-tested. Does the requester really work at the organisational unit indicated, do they need the certificate in their day-to-day work, and are they entitled to request a certificate?

If additional information is required for the request, the requester has 10 days to submit it to the SG PKI. After this period, the request will expire automatically.

## 11. Declaration of acknowledgement and consent

The requester notes that the TSP will revoke the certificates without delay in the event of a definite suspicion of misuse, a breach of the provisions of this document or a breach of any other applicable legal provisions.

By signing, the requester confirms that they have read and understood this document “Convention et conditions d’utilisation des certificats avancés de classe B (pour les personnes physiques) de Swiss Government PKI” and that they accept the provisions set out therein.

| | |
|---|---|
| Full name (requester): | (electronic cl. B) Requester's signature: |
| Place, date: | |