Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Finance FDF

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

31.07.2025

Swiss Government PKI
Class B registration guidelines

Registration guidelines of the Swiss Government PKI for the LRA

Status: approved V7.0

Classification *	Unclassified
Status **	Approved
Owner	Swiss Government PKI
Author	TRF
Processed by	SG-PKI FOITT
Checked by	Beatrice Metaj, Sébastien Farquet, Cornelia Enke
Approved by	PKI Management Board
Distribution	LRAO, RIO, auditors
Storage location	PKI SharePoint
Entry into force	01.08.2025

* Unclassified, Internal, Confidential

** Being processed, Under review, Completed, Approved

Change management, review, approval

Version	Date	Name or role	Description, comments
2.91	23.07.2010	Andreas Zürcher	Replaces versions 2.x, which deal with classes A and B in a single document
2.92		Daniel Stich	Tightening and ensuring consistency with CP/CPS, checklists with links to the guidelines
2.93		Daniel Stich	Integration of findings from A. Zürcher's review
2.94		Daniel Stich	Integration of LZPPS feedback
3.00	23.02.2012	Daniel Stich	Final
3.01	23.04.2012	Daniel Stich	Changes to PIN rules
3.02	30.01.2013	Daniel Stich	PDF in RIO processes and certificate issuance, signed electronic document transmission for RIO process, changes to two-factor login on federal clients
3.03	22.04.2013	Tomaso Vasella	Integration of function certificates Change AdminPKI -> Swiss Government PKI Change of organisational unit following ON FOITT
3.04	11.09.2013	Daniel Stich	
3.05	15.01.2015	Daniel Stich	More detail on identification using ID documents
4.00	24.03.2015	Daniel Stich	Use of new template, integration into document management system
4.1	22.09.2016	Daniel Stich	Adaptation to new wizards, processes and prestaged smartcards
4.2	24.05.2017	Daniel Stich	Integration of new forms and checklists
4.3	29.08.2017	Daniel Stich	General rules on electronic archiving of logs and receipts
5.0	08.11.2017	Daniel Stich	Refined and approved new version
5.1	15.05.2019	Daniel Stich	Change to PSP requirement Identification of requesters according to "F permit" exemption
5.2	03.09.2019	Beatrice Metaj	Various changes in response to internal audit findings
5.2	20.09.2019	Beatrice Metaj	Changes to Annex B "Forms and user agreements", and guidelines inserted
5.3	14.10.2019	Cornelia Enke, Daniel Stich, Beatrice Metaj	Input In&Out/annual review
6.0	01.11.2019	PKI Management Board	Approval of new version
6.1	29.11.2023	Andreas Ruckstuhl, Adrian Bärlocher	Revisions for review by TRF
6.3	25.04.2024	Beatrice Metaj, Jürgen Weber	TRF review and preparation for review/approval
6.4	01.05.2024	Beatrice Metaj	Additions and corrections from the Management Board, esp. section 5.2.3.6 (Plausibility check), inserted
6.5	02.07.2024	Sébastien Farquet	Revisions regarding neutral wording
6.6	29.07.2024	Stephanie Schäfer, Silvio Pelli, Beatrice Metaj, Sébastien Farquet, Adrian Bärlocher	Additions and corrections from the review
6.7	14.01.2025	Beatrice Metaj, Sébastien Farquet, Cornelia Enke	Final review before publication
7.0	14.01.2025	Beatrice Metaj	Version approved for publication

Definitions, acronyms, abbreviations and references

- Glossary
- Reference list

Note

The LRA and at least one LRAO will be audited on the basis of this document, among other things.

Contents

Tables

1. General

Contents of this document

This documents contains and describes the guidelines and rules that apply to the issuance and administration of class B certificates of the Swiss Government PKI.

1.1 Target audience

The document is aimed primarily at trained class B LRAOs of the offices and cantons.

1.2 Terms and abbreviations used

Special terms and abbreviations used in this document are listed in the table "Definitions, acronyms and abbreviations" on Swiss Government PKI together with a brief explanation.

1.3 Reference documents

Reference documents will be marked with square brackets – for example [KLB001].

The reference document version in force at the time of publication of these guidelines is shown. If more recent versions are available, these can be found online and must be used.

1.4 Purpose of the document

The Certificate Policy and Certification Practice Statement of the Swiss Government Root CA (hereafter referred to by the abbreviation CP/CPS) [KLB001] are the regulations governing class B certificates. The aim of these registration guidelines is to define the CP/CPS's requirements for the LRA in more detail.

1.5 Scope

These guidelines apply to all persons whose work involves the class B LRA (Local Registration Authority). The Swiss Government PKI may delegate the tasks of the class B LRA to other organisational units. These, in turn, designate persons to carry out the tasks.

1.6 Swiss Government PKI – class B certificates

Class B certificates are stored on a security token (smartcard or USB token with on-device cryptochip), and are only issued after the personal registration of the requester.

The holder of a class B certificate is a natural person (not an organisation, group or function) and usually holds three key pairs with the associated certificates: depending on the type of certificate (class B certificate or class B function certificate), one for signature, one for authentication and one for key and data encryption, or only one for authentication. For class B certificates, smartcards are equipped with three sets of three key pairs right from the start, although only one set is linked to active certificates at a time.

When prestaged cards are renewed, the next key triplet in line is signed by the CA. Subsequently, only the old keys and certificates for signature and authentication are deleted from the smartcard. The old key pair for key and data encryption is left on the smartcard for later decryption.

Holders may own one class A, one class B and one or more class B function certificates. Class A, class B and function certificates must not be stored on the same security token, although a security token may contain more than one function certificate. The person's first name and surname are clearly identifiable and visible in the certificate.

1.7 Security tokens

A list of supported security tokens and related details can be found in the "A006 – smartcard" [BV002] standard approved by the Digital Transformation and ICT Steering Sector (DTI), and its annexes.

2 Tasks of LRAOs and RIOs

2.1 Required profile for LRAOs

- High degree of personal integrity
- Precise working in accordance with the Swiss Government PKI regulations
- Reliability
- Someone who enjoys customer contact
- Willingness to perform an activity while having regard to traceability
- Willingness to undergo an official assessment of trustworthiness, e.g. personnel security screening in accordance with Article 10 of the Ordinance on Personnel Security Screening (PSSO; SR 128.31 [GV005]) or similar (see section 2.5).
- LRAOs must not be authorised to create or change Admin Directory entries, subject to written exemptions confirmed by the relevant head of office and the relevant SG PKI security officer.

2.2 Tasks and duties of LRAOs

LRAOs have the following tasks:

- Check the request and any necessary additional forms and documentation (see section 5.2.3.2)
- Confirm the identity of requesters (see section 5.2.3.5)
- Verify information in the Admin Directory
- Issue certificates
- Revoke certificates
- Instruct and inform requesters about:
  - activation data
  - protection of activation data
  - their rights and obligations
  - the user agreement and terms of use for advanced class B certificates (for natural persons) [KLB021]
- Fill in and file checklists where necessary
- Keep a log of activities relating to the certificates and the LRA
- Maintain and store dossiers of the certificate holders
- Manage, and where necessary procure, smartcards
- Ensure training, qualification and support of RIOs
- Provide the RIOs with copies of the RIO class B request form, the user agreement and terms of use for advanced class B certificates [KLB021] and the checklist for RIOs
- Manage the list of RIOs
- Approve certificate requests as part of the RIO process
- Proactively maintain an up-to-date knowledge of regulations, processes and technical equipment relating to class B certificates
- Securely store and manage LRA material
- Comply with data protection rules (FADP)

2.3 Required profile for RIOs

- High degree of personal integrity
- Precise working in accordance with the SG PKI regulations and the instructing LRAO
- Basic understanding of the term "traceability" and appreciation of the need for its implementation in RIOs' activities
- Reliability
- Someone who enjoys customer contact
- RIOs must not be authorised to create or change Admin Directory entries, subject to written exemptions confirmed by the relevant head of office and the relevant SG PKI security officer.

2.4 Tasks of RIOs

The RIO deals with requests for class B certificates in accordance with the Guidelines for Registration Identification Officers (RIOs). RIOs have the following tasks:

- Confirm the identity of requesters
- Instruct and inform requesters about:
  - activation data
  - protection of activation data
  - their rights and obligations
  - the user agreement and terms of use for advanced class B certificates [KLB021]
- Check the request and any necessary additional forms and documentation (see section 5.2.3.2)
- Copy the ID document and request
- Fill in the checklist
- Securely transmit the completed checklist, any additional forms, the signed request accompanied by a copy of the valid ID document, as well as the signed *user agreement and terms of use for advanced class B certificates* [KLB021] to the instructing LRAO by post, courier or electronic means. If electronic transmission is chosen: scan the above-mentioned documents as PDF files, sign the files digitally with their personal class B certificate and send to the LRAO by encrypted email. All data saved for transmission purposes must be deleted from the RIO's own system after submission.
- Securely store and manage prestaged smartcards
- RIOs are **not** authorised to store, in any way, datasets of people for whom they have carried out the identification on behalf of an LRAO. All personal information must be transmitted to the relevant LRAO or deleted/shredded.

An LRAO may assume the role of RIO, but not vice versa.

2.5 Trustworthiness assessment for LRAOs

Before appointing someone as an LRAO, the authority shall take such measures as are reasonable and allowed under law to check their trustworthiness and integrity. The SG PKI recommends that the authority take the following measures:

- Personnel security screening in accordance with Article 10 of the Ordinance on Personnel Security Screening [GV005]) by the PSS specialist office of the DDPS

and/or

- Its own measures to check the person's trustworthiness, such as:
  - Identity check (passport or ID card);
  - Checking of professional and/or private references;
  - Verification of the completeness and consistency of the CV;
  - Checking of referenced academic and professional qualifications;
  - Checking of extracts from the debt collection register and the register of criminal convictions.

The authorised signatory from the authority then confirms to the SG PKI that the person's trustworthiness has been checked in accordance with the above recommendation or by similar means. The authorised signatory determines that the person is trustworthy and has integrity, and confirms that they have the necessary skills to perform their future activity as an LRAO.

2.6 Confidentiality, data protection

LRAOs must sign a confidentiality agreement. This is integrated into the class B request for LRAOs.

The acts and ordinances on data protection (FADP) [GV015, GV016] and information security (ISA, ISO) [GV003, GV004] are to be complied with. LRAO activities are carried out on behalf of the SG PKI. LRAOs are personally responsible for compliance during their activities.

In particular, care should be taken to ensure that information relating to customer data or important data of the LRA is transmitted in encrypted form and is not made available to unauthorised third parties.

2.7 Staff training

All LRAOs must undergo training. At the end of the training, a written test is held to determine whether the participants have sufficient knowledge and skills to act as class B LRAOs.

If the aspiring LRAO does not pass the test, they are not assigned LRAO credentials. They can attend the course again and resit the test to demonstrate that they have the necessary aptitude and skills. If LRAOs discover a gap in their knowledge or skills, or have queries which they are unable to resolve themselves, they are required to inform the Swiss Government PKI. The Swiss Government PKI will seek a solution together with the LRAO.

RIOs must also undergo training, with a reduced scope. Training is generally given by the instructing LRAO. Training may also be carried out by the Swiss Government PKI. The training must cover at least the referenced documents "*Verification of applicant's identity, class B*" [KLB003], the "*Guidelines for Registration Identification Officers (RIOs)*" [KLB027] and the *user agreement and terms of use for advanced class B certificates* [KLB021].

2.8 Refresher training

LRAOs are required to maintain their personal knowledge up to date, especially with regard to the registration guidelines. For this purpose, the Swiss Government PKI provides the up-to-date documents and information in the client area of its website Swiss Government PKI. The Swiss Government PKI undertakes to announce important information by email. LRAOs are required to read the corresponding information upon receiving the associated email from the Swiss Government PKI.

Moreover, each LRAO is required to collect a total of 20 training points within a 24-month observation period. The table below shows examples of how to collect points from certain activities:

Activity	Number of points
LRAO basic course (participation)	10
Successfully passed test for LRAO basic course	10
LRAO Summit (1/2 day, participation and feedback)	10
Briefing event (virtual, max. 1 hour, feedback)	5
Personalised LRAO workshop (min. 4 participants, in person)	5 to 10 (depending on content)
E-learning module (incl. test)	max. 5
LRA audit (participation)	5
Q&A sessions (virtual, max. 1 hour, feedback)	2

Table 1: Number of points per LRAO event

The Swiss Government PKI offers regular training and refresher courses for LRAOs (LRAO workshops or the LRAO Summit). LRAOs with an insufficient number of points may be required to attend, otherwise their LRAO credentials may be withdrawn. The current personal points score can be requested from the SG PKI at pki-info@bit.admin.ch. The SG PKI does not publish lists of scores.

3 General operational aspects

3.1 Service hours for the LRA

The service hours for the LRA are set by the relevant responsible organisational unit. They should be designed to allow urgent tasks to be performed within an appropriate period (e.g. revocations to be carried out immediately, within a maximum of one working day).

3.2 Support for LRAOs

3.2.1 Support

LRAOs who require support can contact the operating team of the SG PKI as set out in the service and product catalogue or applicable service level agreement. Details are also published on the Swiss Government PKI.

3.2.2 Malfunction

In the event of a malfunction, the operating team can be contacted via the FOITT Service Desk (+41 (0)58 465 88 88), or the LRAO can create their own ticket via the RoBIT In urgent cases during service hours, LRAOs can ask to be connected to the Swiss Government PKI via the FOITT Service Desk (+41 (0)58 465 88 88).

Malfunctions in the federal workstation client should also be reported to the FOITT Service Desk.

3.2.3 Security

In the event of urgent security-related announcements and questions, a Swiss Government PKI security officer should be contacted via the FOITT Service Desk (+41 (0)58 465 88 88).
For less time-critical announcements and questions regarding security, the pki-secoff@bit.admin.ch email box is available.

3.2.4 Orders

Orders and general questions can be sent as a MAC (Move/Add/Change) request to the FOITT MAC management team, either directly or as a service request to the FOITT Service Desk (+41 (0)58 465 88 88). The pki-info@bit.admin.ch email box should no longer be used for such matters.

3.3 Entrance controls

The LRA's equipment may be housed in a single-occupancy office. However, the use of, for example, meeting rooms, first-aid rooms, or similar spaces to which unauthorised people have access, is not permitted. The rooms should be easily accessible for requesters and provide sufficient privacy for entering the personal PIN and the revocation passphrase. If open-plan offices are shared with people who do not have an LRA function, the room must contain a protected or segregated area for LRA tasks. The room must have enough places in which to lock away LRA material, such as forms and customer data, and must offer sufficient privacy for issuing certificates.

3.4 Access controls

Access to the federal workstation client with LRA functions is protected by two-factor authentication. The federal workstation client is equipped with disk encryption. The LRA applications can be accessed only by people with LRAO credentials on a class B authentication certificate. Access by other people, even other LRAOs, to personal smartcards with LRAO credentials is strictly forbidden. The smartcard must either always be carried or be locked away separately. If the LRAO is not working on the federal workstation, the smartcard must always be removed and stored safely, or carried. The PIN required for the smartcard must only be written down if it is locked away and stored separately from the smartcard. If it is suspected that somebody else knows the PIN, the PIN should be changed immediately. If the smartcard is lost, the corresponding certificates must be blocked without delay. This can usually be

done by an LRAO from the same unit. In addition, the loss must be reported immediately to the FOITT Service Desk and the Swiss Government PKI.

3.5 Policy regarding the federal workstation client with LRA functions

Use of the federal workstation client with LRA functions is governed by strict security regulations, as well as the Information Security Act [GV003], the Information Security Ordinance [GV004] and E026 – Deployment guideline for workplace system [BV003]. It is strictly forbidden to:

- use the federal workstation client for tasks (LRA function) other than those explicitly intended,
- install/order your own software,
- make changes to hardware and software configurations.

The federal workstation client with LRA functions must be protected from access by third parties.

3.6 Forms and customer data

The forms issued by the Swiss Government PKI must be used and filed in the customer dossier, unless explicit reference is made to permitted alternatives (in paper or electronic form). For reasons of traceability, other forms or electronic solutions are not permitted. The current versions of the forms are published online and must be used.

Customer dossiers (request forms, information sheets, revocation requests, etc.) must be locked away for storage (clean desk policy). Either the room must be locked, with access only for LRAOs, or the documents must be locked away in a cupboard which is likewise only accessible for LRAOs. Each LRAO of an LRA must have access to all the LRA's customer dossiers.

With regard to the maintenance of electronic dossiers, the data must be saved in a folder to which only authorised persons, i.e. LRAOs and auditors, have access. In addition, compliance with the conditions set out in section 3.8 must be ensured. All filed receipts must be available as PDF/A documents and validly signed with the class B certificate of the responsible LRAO or instructing RIO.

3.7 Logs

The LRAO performing the issuance and revocation of certificates records all related activities of the LRA or other significant events in the log. Significant LRA activities and events include:

- certificate issuance
- certificate revocation
- key recovery
- receipt of new prestaged smartcards
- internal request number (e.g. ticket number of the request management system), where applicable
- LRAO changes (new etc.)
- change of LRAO location(s)
- major changes to processes (new forms, new workflow, new archive, etc.)
- errors, problems and special features of the above processes

LRAO logs can either be handwritten (see class B: LRAO log of the Swiss Government PKI) or electronic. If logs are electronic, the daily logs must be printed out at the end of each day, signed by the executing LRAO and filed. Alternatively, the electronic logs can be exported daily to PDF/A format, signed with the LRAO's class B certificate and marked with the time stamp of the SG PKI TSA. The PDF log template with the digitally signable entries for each line may also be used. In principle, several

logs may be maintained for each LRA (e.g. for each LRAO, each office, each month, etc.), provided that the chronology and completeness remain assured. In addition, all LRAOs must have access to all logs.

With regard to the maintenance of electronic logs, the data must be saved in a folder to which only authorised persons, i.e. LRAOs and auditors, have access. In addition, compliance with the conditions set out in section 3.8.

The minimum information which a log entry must contain is:

1. Serial number of the entry
2. Date
3. Customer (requester/certificate holder)
4. Activity (prefix: SZ: standard certificate, FZA: admin certificate, FZT: test certificate, A: issued, R: revoked, K: key recovery)
5. In the case of revocation: old smartcard withdrawn yes/no
6. Signature of executing LRAO

3.8 Retention periods

Forms, customer data and logs must in any case be archived for at least 11 years after the certificate has expired, in accordance with section 3.6 and 3.7. During this period, LRAOs must be able to access the archive, and the SG PKI must be able to view it. Access protection for this data must also be ensured for electronically managed customer dossiers (no access to data for non-LRAOs).

LRAOs who give up their position are required to hand over all customer dossiers, logs and other LRA material to their successor within the organisation, or to the SG PKI.

For archiving purposes, existing paper documents may be scanned, saved as PDF/A files, signed and marked with the time stamp of the SG PKI TSA. Individual documents need only be signed with the class B certificate of the original executing LRAO. If several documents are digitalised (e.g. documents for an entire month or year in a single PDF/A file), two LRAOs must digitally sign the PDF/A file, thereby confirming the seamless and correct migration from paper to electronic form. It must be ensured that individual documents remain locatable. Electronically archived items must be protected from access by non-LRAOs. Once the paper documents have been digitalised in accordance with these requirements, they may be destroyed.

3.9 Storage of prestaged smartcards

Prestaged smartcards and other sensitive data carriers must be stored safely. Either the room must be locked, with access only for LRAOs, or the smartcards must be locked away in a cupboard whose keys are held only by LRAOs.

3.10 Use and protection of certificates with LRAO credentials

Certificates with LRAO credentials may only be used for the intended purposes and must not be passed on to someone else. LRAOs are also required to protect the private keys and certificates on their smartcard with activation data in accordance with section 3.4.

3.11 Disposal

3.11.1 Clean desk policy

Paper documents relating to the LRA (guidelines, checklists, notes, etc.) or customers (certificate requests, lists, etc.) that are no longer required must be disposed of by means of a shredder or security box. Smartcards that are no longer required must be rendered unusable with a hole punch or shredded prior to disposal.

Documents that are still required must be filed in a way that is not visible to all/not out in the open on a desk or not in publicly accessible storage, and must be safely archived.

3.11.2 Federal workstation

The federal workstation will be disposed of by FOITT Support (Service Desk).

3.11.3 Smartcards

Smartcards must be rendered unusable (e.g. by punching a hole in the chip) before disposal.

3.12 Rules for PINs

Certificate holders use PINs (passwords) to activate their security token or private keys. The PIN is fundamentally different from the password, which is used for logging in to applications, for example "Quick Guide: PIN rules for smart cards" under "Certificate issuance (Issuing)"]. Each certificate holder chooses their own PIN. The rules with regard to smartcard PINs are:

- *Length:* The PIN must be at least six characters long.
- *Number of attempts:* The smartcard must lock itself after five failed attempts, at the latest.
- *Complexity:* The composition of the PIN can be freely chosen (even a purely numerical code is permitted). Trivial PINs (e.g. User-ID or 123456) must not be used.
- *Validity:* The PIN must be changed as soon as there is any suspicion that another person has obtained access to it. If a smartcard reaches the end of its life cycle, the new smartcard must be assigned a new PIN.
- *Uniqueness:* A PIN may only be used for one smartcard.

Special characters should not be used, due to the different keyboard layouts in different languages.

3.13 Revocation passphrase

The revocation passphrase comprises a general question with the associated personal answer.

The information in the passphrase should be selected such that it cannot be inferred or easily guessed by third parties. At the same time, it should be familiar enough to the requester that they never have a problem or doubt about answering the question.

The revocation passphrase is used to identify the certificate holder to the LRAO during a phone conversation, e.g. when the holder requests the revocation of their certificates, or to the relevant Service Desk during the PIN reset process.

3.14 PIN reset and PUK handling

The SG PKI has developed an electronic centralised system with PUK management for its prestaged smartcards, in which the PUK is stored in encrypted form on one of the SG PKI servers and is made available to the smartcard in the background during the unlocking process. At no time is the PUK displayed to anyone.

The following principles apply for support staff or LRAOs:

- In order to perform a PIN reset, a PIN reset superuser is needed. The PIN superuser can use a web application to create an internal ticket for a smartcard if they are able to successfully identify the person as the PIN holder. The identification can also take place by phone, using the revocation passphrase. Only then can the PIN holder reset their PIN with a so-called PRU.
- A PRU (PIN reset user) is needed to unlock the smartcard. The PRU launches the PIN Reset Wizard and confirms that they have clearly identified the person present as the PIN holder for the locked smartcard, and allows them to reset the PIN.
- The PRU has the job of "lending" the PIN holder their PC (as the PIN holder cannot perform two-factor authentication on their own PC at this time, owing to their smartcard being locked). The affected user must be at the same location as the PRU and insert their smartcard into a second card reader at the PRU's PC.
- The functions of PIN reset superuser and PRU must not be performed by the same person simultaneously. The credentials for these functions are mutually exclusive, in order to comply with the multiple-control principle for PIN reset processes.

The PIN reset process for prestaged smartcards is described in detail in the "PIN reset" quick guide.

4 Conformity check

The SG PKI is required to check the implementation of the CP/CPS [KLB001]. This includes, in particular, checking compliance with these registration guidelines by the LRAOs. The conformity check can be performed by the SG PKI itself or by an external unit commissioned by the SG PKI. LRAOs are required to cooperate with these checks, and to allow access to processes and documents.

If someone does not pass the conformity check, their LRAO credentials can be withdrawn. In the case of particularly serious contraventions, all the user certificates issued by the non-compliant LRAO may also be revoked.

5 Processes for Swiss Government PKI class B

5.1 Overview

For class B, there are different specifications of certificate. The table below provides an overview of which processes can be used for which type of certificate:

Class B for U accounts or X accounts (user accounts)
Smartcard initialisation is performed by the SG PKI during the prestaging process
During prestaging, three sets of three key pairs (signature, authentication, encryption) are generated externally and written onto the smartcard
During issuance, three certificates – for signature, authentication and encryption – are written onto the smartcard
Key recovery on a third-party card (delegation) is not possible
Key recovery for the private encryption key is possible
RIO process possible
Renewal possible up to two times

Table 2: Process for class B

Class B function certificate for A accounts (admin accounts)
Smartcard initialisation is performed by the SG PKI during the prestaging process
During prestaging, three sets of three key pairs (signature, authentication, encryption) are generated externally and written onto the smartcard
During issuance, only the certificate for authentication is written onto the smartcard
Key recovery on a third-party card (delegation) is not possible
Key recovery for the private authentication key is not possible
No RIO process planned
Renewal not permitted

Table 3: Process for A accounts

Class B function certificate for T accounts (test accounts)
Smartcard initialisation is performed by the SG PKI during the prestaging process
During prestaging, three sets of three key pairs (signature, authentication, encryption) are generated externally and written onto the smartcard
During issuance, three certificates – for signature, authentication and encryption – are written onto the smartcard
Key recovery on a third-party card (delegation) is not possible
Key recovery for the private encryption key is possible
RIO process possible
Renewal possible up to two times

Table 4: Process for T accounts

5.2 Certificate issuance process

A distinction should be made between two specifications for the issuance process:

- Issuance process without a RIO
- Issuance process with a RIO

Below, the process without a RIO is referred to as "issuance without RIO", and that with a RIO as "issuance with RIO".

The differences between the processes with and without a RIO are listed in the following table:

Process without RIO	Process with RIO
Direct personal identification of the requester by the LRAO. As proof, the LRAO scans the requester's valid travel document and other documents if necessary.	Personal identification of the requester by the RIO. As proof, the RIO copies the valid travel document and the correctly completed request form and other documents if necessary. The RIO fills in the checklist and transmits these documents and the signed user agreement and terms of use for advanced class B certificates [KLB021] to the responsible LRAO.
The LRAO checks the requester in the Admin Directory.	The RIO checks the requester in the Admin Directory.
The LRAO informs the requester about activation data and the protection thereof.	The RIO informs the requester about activation data and the protection thereof.
The LRAO issues the certificate for the requester in the Walk-in Wizard.	Check/approval of the request, then request for issuance of the certificate by the LRAO in the Walk-in Wizard and dispatch of the "unseal ticket number" (S-PIN) to the requester or the RIO.
The requester records the personal PIN and the data for revocation by phone (revocation passphrase) as the last step in the Walk-in Wizard.	The requester records the personal PIN and the data for revocation by phone (revocation passphrase) when unsealing the smartcard with the Unseal Wizard.

Table 5: Difference between processes with and without RIO

5.2.1 Who can request a certificate?

In the request for LRAO credentials, the line manager specifies the organisational units and staff for which/whom certificates may be issued. The requester's allocation to an organisational unit must match the LRAO's credentials. Specifically, this means that the entry for the requester must be in the same directory path in the Admin Directory as the one approved for the LRAO, or that the authorised directory paths must be stored in the LRAO's account.

Minors (i.e. apprentices) can also request class B certificates, in which case the LRAO must perform their duty to inform particularly diligently during issuance.

An LRAO's class B certificates must be requested from, and issued by, another LRAO. Under no circumstances may an LRAO issue a class B certificate to themselves.

5.2.2 How can a certificate be requested?

The LRAO or the PKI manager decides how a certificate can be requested (in writing by filling in a form, via MAC remedy, etc.). As a general rule, the request process must be traceable for up to 11 years after the certificate has expired. The SG PKI provides a form containing all the data required for registration (class B: request for personal class B certificates of the Swiss Government PKI).

If certificates for exemptions are requested (e.g. if the requester can only provide an F permit), the SG PKI's additional forms for the relevant exemption must in all cases be filled in and attached to the registration.

5.2.3 Issuance without RIO

Use of the LRA client is governed by the LRAO training documentation and the quick guides on the individual wizards. Where the rules are contradictory, these guidelines shall take precedence.

The LRAO shall act in accordance with the "*Checklist: Issuance of class B certificates*".

5.2.3.1 Checking the request in the Admin Directory

The requester must be entered in the Admin Directory in order for a certificate to be issued.

The following conditions must be met:

1. Is a complete, plausible email address specified in the "Mail" field?
   In the case of function certificates for A accounts: the email address of the A account must be clearly labelled with the add-on "Admin", "ADM" or similar.
   In the case of function certificates for T accounts: the email address of the T account must be clearly labelled with the add-on "Test", "TST" or similar.
2. If there is more than one entry (same first name and surname): can the entry for which the certificate was issued be clearly identified from the name suffix?

If the requester is not entered in the Admin Directory, or not correctly, the change must be made by the Admin Directory administrator for that office. The process cannot be continued until the requester is correctly entered in the Admin Directory (replication of the data generally takes at least one night). The LRAO can check the Admin Directory entry in the Walk-in Wizard, for example.

5.2.3.2 Checking the request form

The request form should be checked for completeness and correctness.

1. Is the requester authorised to submit a request to this LRAO in accordance with section 5.2.1
2. Do the requester's details on the form match those in the Admin Directory entry?
3. Is the form correctly dated and signed?
   Instead of individual requests, the relevant HR unit can also send a list of newly hired staff to the responsible LRAO. The list must contain at least the same details for the staff as the mandatory fields in the request form. Within the FOITT, a MAC remedy is available for ordering class B certificates.

A request form is required for both a first issue and a subsequent reissue.

In addition, the request form must not be filled in and signed until the day of issue.

5.2.3.3 Arranging an appointment

An appointment to issue the certificate must be arranged with the requester. For this purpose, an email is sent to the email address specified in the request (exception: ADM accounts without a mailbox). This email should contain the following:

1. Proposed date(s) for certificate issuance.
2. An instruction to the requester to bring a valid travel document with them. The travel document must not have expired at the time of registration. In the case of exemptions, the requester must also bring the additional forms and documents specified for the relevant exemption (see section 5.2.3.5).
3. An instruction to the requester to create a PIN. The requester should be reminded of the rules governing the PIN, as set out in section 3.12.
4. An instruction to the requester to prepare a revocation passphrase.

5. Contact details of the LRAO for questions and for resolving clashes of dates.

For new hires, the appointment can also be arranged with the relevant HR unit or the future line manager. The above information must in any case be communicated to the requester in advance.

5.2.3.4 Starting the issuance process

After the requester has arrived, the LRAO launches the Walk-in Wizard on the LRA client and selects the appropriate policy (for function certificates of A accounts, the policy for creating an individual authentication certificate must be selected). The LRAO then searches for the requester in the issuance application by entering their name or email address, and the correct entry is selected. The Admin Directory acts as a data source in this regard.

5.2.3.5 Checking the requester's identity

For identity checking purposes, the requester must appear in person before the LRAO. A valid passport or an ID card which is valid for entering Switzerland must be used for the identification. The check of the requester's identity is a three-stage process:

1. Checking the authenticity of the travel document (ID card/passport) provided. For example, a (corporate) staff ID or driving licence is not sufficient for identification purposes. The document should be checked for the following points:
    a. Is the travel document still valid (not expired at the time of registration)?
    b. Are the known security features present? (At least four of the ID's official security features must be verified.)
2. Personal identification of the requester through comparison with the identification document:
    a. Does the person match the photograph in the travel document?
    b. Do their age and height match the details in the document?
    c. Does the signature in the travel document match that on the request form?
3. Checking whether the details in the travel document match those in the request and in the Admin Directory. In particular, the surname(s) and first name(s) in the document must be matched with those in the Admin Directory, according to the following criteria.

    Since 1 January 2014, for new hires in the Federal Administration, the responsible HR unit has entered the fields "Surname according to ID" and "First name according to ID" in addition to the name fields "Surname" and "First name". The content of these fields is displayed in the Walk-in Wizard. The check must be performed according to the rules below, depending on the content of these four fields. The rule applied must be selected on the relevant page of the Walk-in Wizard. The applicable rules are:

    Rule 1: Both the fields "Surname according to ID" and "First name according to ID" have been filled in and are identical to the surname(s) and first name(s) on the ID document presented. On the screen, the option "Identified with <Surname according to ID>/<First name according to ID> according to ID" should be selected.

    Rule 2: The fields "Surname according to ID" and "First name according to ID" have been filled in, but they do not match the travel document presented. On the screen, the option "Field <Surname according to ID>/<First name according to ID> not valid" should be selected. No certificate is issued.

    Rule 3: The fields "Surname according to ID" and "First name according to ID" have not been filled in. However, "Surname" and "First name" do match the travel document presented, taking account of the requirements in the document "Identity check for class B requesters" [KLB003]. On the screen, the option "Identified with <Surname>/<First name>" should be selected.

Rule 4: The fields "Surname according to ID" and "First name according to ID" have not been filled in. "Surname" and "First name" do not match the travel document presented, even when taking account of the requirements in the document "Identity check for class B requesters" [KLB003], but they are plausible. The requester already holds a certificate with this surname and first name, i.e. this is a card replacement or the issuance of a follow-up card. In this case, a data entry request for the fields "Surname according to ID" and "First name according to ID" must be sent to the responsible HR unit. The requester must be entered in a list of provisionally issued certificates. The certificate may be issued. On the screen, the option "Provisional issuance with 'surname'/'first name'" should be selected. The change by HR in the IPDM (formerly BV+) must be tracked by the LRAO.

Rule 5: The fields "Surname according to ID" and "First name according to ID" have not been filled in. "Surname" and "First name" do not match the travel document. No earlier certificate exists for the requester.
No new certificate may be issued. A data entry request for the fields "Surname according to ID" and "First name according to ID" must be sent to the responsible HR unit. On the screen, the option "<Surname>/<First name> invalid" should be selected.

Exemption for F permits

In exceptional cases, identification can also be performed with a valid F permit. The checking of the ID must comply with the rules on checking a travel document as described above. With requests based on an F permit, the additional forms and documents below must be provided (and then filed in the customer dossier):

- A completed "Additional form for requesters with F permit", signed by the relevant ITSOO. On this form, the ITSOO confirms that the requester cannot be clearly identified on the basis of the ID document provided, and accepts the associated risk for the organisation.
- The work permit issued by the relevant canton or federal authority.

5.2.3.6 Plausibility check of the request

Points to bear in mind include:

- Can the requester be identified?
- Do they work for the specified organisation?
- Is the HR unit or the line manager responsible for the requester?

The LRAO may refuse a request if it can be assumed that the requester does not know how to use the certificates. The same applies if the conversation indicates that they are unlikely to comply with the provisions of the user guidelines.

5.2.3.7 Preparing the smartcard

Prestaged smartcards are used. These smartcards are prepared centrally by the SG PKI and therefore do not need to be staged separately.

5.2.3.8 Digitalising documents

The documents used for the identification, especially passports, must be digitalised and saved in the system during the issuance process. An integrated scanning process is available in the Walk-in Wizard.

With ID cards, the front and back should be scanned; with passports, the double page with photo and signature should be scanned. Other documents that are needed for identification purposes should also be scanned. The scan must be clearly legible.

To achieve a high-quality result when scanning, you should use the following settings:

- **Resolution:** 200 x 200 or 300 x 300 dpi (depending on scanner options)
- **File format:** JPEG (file extension: .jpg)
  PDF/A (file extension: .pdf) for double-sided scan of both ID pages

If no scanner is connected to the LRA client, scanning can be performed on a multifunction device and the scanned ID documents may be sent to the LRAO's personal email address. If possible, the transmission must be encrypted.

Normally, the scanning result is A4 size. Before you save the travel document, crop out the travel document so that only this is saved.
Save the document in a private drive on your client. After the certificate has been issued, you are required to delete these files and any emails, and then to empty the Recycle Bin/Deleted Items in the client and in Outlook.

5.2.3.9 Instructing the requester about the PIN and the revocation passphrase

The requester is reminded about the purpose of the revocation passphrase and, if they have not yet set up a passphrase, requested to think of one in accordance with the requirements in section 3.13. The requester is also reminded of the rules for creating a PIN, as set out in section 3.12.

5.2.3.10 Requesting certificates and saving them on the smartcard

The requester's smartcard is inserted into the second card reader. Standard certificates must not be issued on the same smartcard as class A or class B certificates. However, more than one class B function certificate (e.g. an administrator certificate and several test certificates) may be stored on the same smartcard.

In the next step, all required and previously digitalised documents are saved in the system. At a minimum, this should be a copy of the valid travel document. All documents needed for clear identification and registration, e.g. marriage certificates, letters of guarantee, other identification documents, etc., must be included. The process is described in section 5.2.3.8.

The Wizard then generates the request and sends it to the central system, where the certificate is created.

The requester is invited to enter their PIN and the revocation passphrase themselves. Then, the certificates are written onto the requester's smartcard, and the smartcard is secured with the user's PIN.

5.2.3.11 Confirming receipt/signing the user agreement

Once the certificate is issued, the "*Confirmation of smartcard receipt and handling*" is displayed with the "fingerprints" (unique ID number for the certificate). Printing and handover of this document is optional. Using the *user agreement and terms of use for advanced class B certificates* [KLB021], the requester must be verbally informed of their rights and obligations (purpose of the certificate, smartcard contents, certificate revocation, due diligence for PINs, revocation passphrase).

Finally, a copy of the *user agreement and terms of use for advanced class B certificates* [KLB021] must be signed by the requester (both for first issues and later reissues). They thus confirm that they have read and taken note of the information, and have received the smartcard with the certificates. The LRAO compares the signature on this form with that on the request form. The "*Confirmation of smartcard receipt and handling*" with the fingerprints is no longer needed and can be ignored. As an alternative to the paper copy, the LRAO may choose to provide the user agreement to the requester electronically. However, the LRAO must ensure that the document version that is signed with the class B certificate is received within five working days, and that it is archived electronically in accordance

with the requirements in section 3.8. If the signed user agreement is not returned to the LRAO, the corresponding certificates must be revoked immediately.

5.2.3.12 Completing the issuance process

At the end of the process, the requester receives the following:

- the new smartcard
- the unsigned copy of the user agreement and terms of use for advanced class B certificates [KLB021]
- their travel documents and any other documents required

.

5.2.3.13 Keeping the log

The activities performed must be recorded in the LRA log by the LRAO. The rules set out in section 3.7.

5.2.3.14 Deleting saved files from local systems

If travel documents are scanned outside the Walk-in Wizard and saved locally, they must be deleted after the certificates have been issued. Particular attention should be paid to ensuring that nothing remains stored in personal or corporate email accounts (see also section 5.2.3.8).

Note: This must be done because otherwise this would constitute an undisclosed data collection within the meaning of the Data Protection Act. The files are archived in the Swiss Government PKI database (which is disclosed in accordance with the FADP [GV015]) during the issuance process.

5.2.3.15 Filing the customer dossier

The actioned request and the signed copy of the *user agreement and terms of use for advanced class B certificates* [KLB021] are filed in the customer dossier. If additional forms (e.g. for issuance based on an F permit) or other documents are needed, these are also filed in the customer dossier.

If the customer dossier is managed electronically, the documents described above must be scanned, saved in PDF/A format, signed with the LRAO's personal class B certificate and then saved in such a way as to ensure that:

- a chronology and the certificate holder are identifiable
- the request can be found at any time
- any information from peripheral systems (such as ticket numbers, etc.) is available (associated tickets, etc. must be retrievable for at least 11 years after the certificate expires)

5.2.4 Issuance with RIO

In the "Issuance with RIO" process, the LRAO delegates the requester identification check and other tasks to the RIO. In this case, the requester and the RIO are not in the same location as the LRAO. This is also known as an asynchronous issuance process. Administration and test certificates must not be issued with this process.

Other documents to be complied with in connection with this process are the "*Guidelines for Registration Identification Officers (RIOs)*" [KLB027] and the "*Quick Guide Walk-In-Wizard - RIO*» (under «RIO (Registration Identification Officers)". Where provisions are contradictory, the present guidelines shall take precedence.

The entire document archiving process is carried out by the LRAO; RIOs do not maintain permanent archives.

In the interests of completeness, the entire process is described here, including the steps that requesters perform themselves to activate the smartcard at the end of the process.

5.2.4.1 Creating a request

The requester enters their personal data and their organisational and communication details in section 1 of the form "Class B: RIO request to issue class B certificates". They then date and sign this section.

5.2.4.2 Identification of the requester by the RIO

The requester must be clearly identified by the RIO. For this purpose, the requester must present themselves in person to the RIO. The steps below are used to perform the necessary checks and enter the additional details in the request form:

1. The requester goes in person to the RIO, taking with them their ID document (valid, unexpired passport or ID card valid for entry into Switzerland).
2. The RIO goes through the "RIO checklist" and fills it in.
3. Using the travel document, the RIO checks whether the requester's face matches the photo in the travel document. If it does not match, the RIO refuses to continue the identification process and reports the incident to the responsible LRAO. Alternative identification documents for exemptions and the processes used in such cases are listed in section 5.2.3.5. That list is definitive.
4. If it does match, the RIO hands over a new prestaged smartcard to the requester and notes down the serial number of the cryptochip in the relevant field of the form. If the serial number is not printed on the smartcard, it can be retrieved using either the card middleware or the Unseal Wizard. The RIO makes the requester aware that, from now on, the requester must keep the smartcard under their sole control.
5. The RIO and the requester sign section 2 of the form to confirm that a personal meeting and the identification with a valid travel document have taken place, and that the requester has received the specified smartcard.
6. The RIO makes sure that the requester has understood the contents of the *user agreement and terms of use for advanced class B certificates* [KLB021] and has received a copy. A second copy must be signed by the requester.
7. The RIO places page 2 of the request form on the photocopier together with the travel document, so that the travel document with visible photo appears on the copy in the relevant field of the request form.
   For ID cards, both sides must be copied; for passports, the double side with the photo and signature must be copied.
8. The RIO copies page 2 of the request form and the travel document, as well as all additional forms and documents needed for issuance purposes. The requester and the RIO sign page 2 and this, together with the previously completed page 1, is compiled to make the complete request form.
9. The RIO sends both signed documents (request form and signed user agreement [KLB021], the copies of any additional documents and the completed checklist to the responsible LRAO. The documents may be sent in one of the following ways:
   a. The signed documents are sent by post or courier to the responsible LRAO.

b. The RIO scans the documents in PDF/A format, signs them with their personal class B certificate and then sends them by encrypted email to the responsible LRAO. The prerequisites for this process are:

   i. The RIO is the holder of a valid class B certificate

   ii. The RIO has access to the LRAO's public encryption key

   iii. The RIO's workstation is scanning-enabled.

10. If the LRAO does not manage electronic customer dossiers in accordance with the specifications in section 5.2.4.3, and if the documents were sent electronically, the original paper documents must subsequently be sent by post to the LRAO for filing in the physical customer dossier. The LRAO must check and ensure that the documents have been received.

11. The originals of the documents used for identification purposes are returned to the requester. All copies and forms must be either sent to the LRAO or destroyed (shredded). Digital copies, for instance those in mailboxes, must be deleted and the Recycle Bin/Deleted Items emptied. The RIO does not retain any documents, and does not manage any customer dossiers.

5.2.4.3 Approval of requests by the LRAO and certificate issuance

After receiving and checking the documents provided in accordance with section 5.3.4.2, the LRAO can approve the request and release the generation of the certificates. For this purpose, the following steps from the "Issuance with RIO" checklist are performed:

1. The LRAO checks whether all documents are enclosed and the request form has been signed by an authorised RIO. The documents required are:
   - Request form "Class B: RIO request for issuance of class B certificates", with multiple signatures
   - Signed user agreement and terms of use for advanced class B certificates [KLB021]
   - Signed RIO checklist
   - Other documents and IDs needed in the case of exemptions
2. If the documents were sent electronically, the LRAO checks whether
   - the documents were sent in encrypted form and
   - the documents are electronically signed with the RIO's valid signature
3. Using their personal smartcard, the LRAO launches the Walk-in Wizard in RIO mode on the LRA client. The LRAO searches for the requester in the system by entering their name or email address.
4. The LRAO checks whether the details on the request form match those in the copy of the ID document and the requester's entry in the Admin Directory (see the requirements under No 3 in section 5.2.3.5). If the three sets of details match in accordance with the requirements, approval of the request can continue. Otherwise, the process must be stopped and a correction of the Admin Directory or the request form must be requested.
5. Documents received electronically can be directly entered in the Wizard.

   If the documents were sent on paper, the LRAO scans the completed and signed request form received from the RIO, the signed RIO checklist and any other documents and IDs needed in the case of an exemption.

   To achieve a high-quality result when scanning, the following settings should be used:

   - **Resolution:** 200 x 200 or 300 x 300 dpi (depending on scanner options)
   - **File format:** JPEG (file extension: .jpg) or PDF/A (file extension: pdf)

   The LRAO then uploads the documents to the Walk-in Wizard.

6. The LRAO enters the serial number of the smartcard issued to the requester and issues the certificate on the server (via the Walk-in Wizard).
7. The approved request is entered in a ticket in the background and sent to the CA for certification. The ticket number is held in a so-called unseal document (PDF format), which can be printed out.
8. The LRAO forwards the unseal document or unseal code (e-ticket number), either directly to the requester or to the RIO.
9. The LRAO records this action in the log.
10. The LRAO files the signed user agreement and terms of use for advanced class B certificates [KLB021] in the customer dossier. If the dossier is managed electronically, either the electronic version signed by the RIO must be saved, or the LRAO must create a PDF/A version from the paper documents. The document is then signed by the LRAO using their personal class B certificate before it is filed. With regard to storage security, data protection, retention periods and revisability, the electronic customer dossiers must meet the requirements in section 5.2.3.14 and 3.8 in these guidelines.
11. Both parties delete all digitalised copies of the ID card or passport from their personal storage areas (including copies in Sent Items, etc.).

5.2.4.4 Activating the smartcard by loading the certificates onto the smartcard

As the last step, the certificates must be loaded onto the requester's smartcard.

1. After a certificate has been successfully issued, the requester receives the unseal document with the e-ticket number, either by email or via the RIO.
2. The requester launches the Unseal Wizard on a client that is logged in to the network and inserts their smartcard into the card reader. If the client requires two-factor login for Windows, a second card reader must be installed for this step. The requester enters the ticket number they have received. The Wizard checks whether the smartcard specified in the ticket matches the smartcard in the second card reader.
3. If it matches, the requester is prompted to enter their PIN and the revocation passphrase.
4. The Wizard saves the revocation passphrase in the central database, loads the certificates onto the smartcard and secures the smartcard with the new personal PIN.

The smartcard is now activated and can only be used by the requester.

5.3 Certificate revocation process

5.3.1 Who can request a revocation?

The following list is exhaustive, and shows all the roles that can request a certificate revocation:

- the requester themselves,
- the requester's line manager,
- the PKI manager,
- the SG PKI security officer,
- the responsible LRAO of the SG PKI,
- the organisation's ITSOO/ITSOD or IT security officer,
- employees of the HR unit responsible for the certificate holder.

5.3.2 How can a revocation be requested?

Certificate holders can request a revocation from the LRAO personally, via email or by phone. The LRAO identifies the requester using the revocation passphrase, for example, and checks the plausibility of the request.

The HR units and line managers can also send revocation requests to the LRAO as lists (e.g. Excel files). This is mainly the case where staff leave or change units. The revocation will need to be integrated into the relevant exit procedures. The LRAO checks the responsibilities. The LRAO may only accept revocation requests from third parties in writing (signed email, signed revocation requests). Only certificate holders are permitted to request a revocation by phone.

The LRAOs must be involved in the exit procedures for their unit. It must be ensured that certificates of departing staff are revoked in good time. Once the smartcard is returned, revocation must take place immediately, or at the latest on the first working day after departure.

The LRAO, the PKI security officer and the Swiss Government PKI manager can revoke a certificate directly in the Revoke Wizard.

5.3.3 Reasons for a revocation are, in particular:

What are the reason for a revocation?

- The smartcard has been stolen or cannot be located
- The smartcard is defective
- The smartcard is renewed
- The smartcard is returned (e.g. to the line manager, the LRAO, HR)
- The termination of the employment relationship
- Changes to the details on the certificate (name, email address, etc.)
- The suspicion that the private key has been compromised (revealed) and that someone else was able to use a service, e.g. sign an email
- Infringement of the guidelines (e.g. non-compliance with the user agreement [KLB021])
- The LRAO considers that revocation is appropriate for other reasons

5.3.4 Process

A revocation request should **always be processed immediately**. If there is uncertainly about the validity of a revocation request (e.g. in the case of a request by phone), the following must be borne in mind: the aim of a revocation is to protect the certificate holder and the organisation from possible damage as a result of their certificates being abused. However, a fraudulent revocation request and subsequent revocation may also cause damage by preventing services from being used by the customer, or an administrative act being carried out. Thus, the LRAO has to weigh up the potential damage from a non-revocation versus a fraudulent revocation.

The LRAO should proceed as follows:

5.3.4.1 Plausibility check of the request

Points to bear in mind are:

- Can the requester be identified (voice, phone number, revocation passphrase)?
- Is the HR unit or the line manager responsible for the certificate holder?
- Is this the responsible ITSOO or ITSOD?

5.3.4.2 Revocation form

If a revocation request is made by a third party (i.e. not the LRAO and not the certificate holder; see also section 5.3.1), the request must be made in writing using the *Revocation request for Swiss Government PKI class B certificates*. HR units and or line managers can also send revocation requests to the LRAO as lists (e.g. Excel files). If the request is not submitted on paper, care should be taken to ensure that the document or email with the attachment is signed by the requester.

A revocation form is also required if the information (reason, instructing authority) relating to the revocation is not entered in the Revoke Wizard, or if the official Revoke Wizard cannot be used for the revocation. In these cases, the form may also be filled in by the LRAO. This applies especially to revocations with the CMC console and revocation requests to the SG PKI.

5.3.4.3 Revocation

For the revocation, the Revoke Wizard is launched on the LRA client and a search for the certificate holder is performed. The certificates to be revoked are then selected. The LRAO sees a page showing the ID documents that are stored for the relevant certificate. The LRAO uses these documents to check the certificate holder's identity.

After the identification, the selected certificates are revoked. The certificate holder automatically receives an email notification about the revocation.

If possible, the smartcard is collected, destroyed and disposed of in accordance with section 3.11.

5.3.4.4 Administrative completion

If a revocation form is available, this is filed in the customer dossier. If the customer dossier is managed electronically, the requirements in section 3.8 and 5.2.3.15 apply. The revocation process is recorded in the log in accordance with section 3.7.

5.4 Certificate renewal process

Certificates can be renewed autonomously by the certificate holder up to twice during their validity period. The prerequisite is that the current version of the Renewal Wizard is installed on the user's client and there is still sufficient storage space on the smartcard. As prestaged smartcards already have three set of keys on them, this is usually the case for this type of card. The process is as follows:

- The still-valid class B certificate is used to launch the Renewal Wizard on the user's personal workstation.
- The smartcard that is inserted in the card reader is displayed
- The user confirms that this is the correct smartcard
- The Wizard then generates three new certificates and loads them onto the smartcard. The old signature certificate and authentication certificate are deleted. Old encryption certificates remain on the smartcard.

If the certificates have already expired, the renewal described above can no longer be performed. A new certificate will have to be issued by the LRAO. The process is the same as that for a first certificate issuance.

5.5 Process for recovering your own key

A certificate holder can autonomously request a key recovery for their own encryption key. The process is as follows:

Via the https://key-recovery.pki.admin.ch/KeyRecoveryRequest/ URL, the user can log in to the application with their personal, currently valid class B certificate and create an e-ticket for key recovery.

The user then takes the ticket number and their personal smartcard to the nearest responsible LRAO or key recovery agent (KRA).

They identify the smartcard holder and launch the Key Recovery Wizard. They insert the holder's smartcard into a free card reader and enter the e-ticket number. The smartcard holder's old encryption keys are then displayed on the screen. Once the relevant key has been selected, this is loaded onto the smartcard in addition to the existing encryption keys.

5.6 Process for recovering someone else's key

As a general rule, encryption keys may only be loaded onto the certificate holder's personal smartcard.

In exceptional cases, however, it may be necessary to pass on someone's encryption keys to an authorised person on a separate smartcard. The reasons for this could be:

- The certificate holder no longer works for that office
- The certificate holder has been on sick leave for a prolonged period
- The certificate holder has died
- Legal cases

As this would mean that all the certificate holder's encrypted emails and documents can also be read (in cases where the certificate holder is also the owner of the encrypted data), each of these cases must be assessed individually by the SG PKI and the FOITT's legal service. For this purpose, a detailed and substantiated request must be submitted to the responsible people at the SG PKI. The next steps will then be defined on a case-by-case basis, and always in consultation with the legal service.

6 Forms and checklists

The forms and checklists below were created for the processes outlined above. All forms and checklists can be downloaded as separate documents from the Swiss Government PKI.

6.1 Certificate request form

Before the certificate is issued via the "*Issuance without RIO*" process (see section 5.2.3), the requester must fill in the form *Class B: Request for personal class B certificates of the Swiss Government PKI*. The form can be downloaded from the Swiss Government PKI website. Customers may also choose to create their own form for their organisation. If so, the following data must be collected as a minimum:

- Surname, first name
- Organisational unit
- Email
- Unique staff number or suffix

In addition, the form should already notify users of the rules on creating a PIN and personal passphrase.

The form should be given to customers in advance, so that they have enough time to think of a PIN and the associated revocation passphrase. The customer signs the request form, thereby confirming that the information on it is correct.

Alternatively, offices can also request class B certificates via their internal request system (e.g. MAC remedy, Gever, etc.). It should be ensured that the requests can be clearly assigned to the issues, and that the request documentation and the proofs used can also be retrieved 11 years after the certificate has expired (see section 5.2.3.15 and 3.8).

At the Federal Administration, the first issuance of a standard certificate is usually integrated into the HR process for newly hired staff. The relevant HR unit can also inform the LRAO of new hires by means of lists. The data mentioned above must be provided for each new hire.
For the "*Issuance with RIO*" process (see section 5.2.4 the form *Class B: RIO request for issuance of class B certificates* is used.

6.1.1 Supplementary form for requesters with an F permit

If a request is submitted under the exemption for a user with an F permit, the *Supplementary form for requesters with F permit* must also be filled in and signed by the responsible ITSOO. By signing, the ITSOO confirms that they have taken note of the fact that the requester with F permit cannot be clearly identified, and that the SG PKI cannot therefore provide any guarantee that the requester has been correctly identified. The form is part of the audit-related documents for the relevant issuance processes.

6.2 User agreement and terms of use for advanced class B certificates

The form "User agreement and terms of use for advanced class B certificates" [KLB021] contains only the most important information; it was created specially for end users. The full information is contained in the CP/CPS [KLB001]. The form is part of the audit-related documents for an issuance process. The currently still available form "Confirmation of smartcard receipt and handling" contains the fingerprints for the certificates. At the end of the process, the smartcard number can be entered if available. This number may be useful in the event of problems with the smartcard (loss or damage). This confirmation is not part of the audit-related documents for an issuance process.

6.3 Form for revocations

When a revocation is performed with the Revocation Wizard, the instructing authority and the reasons for the revocation must be recorded in the Wizard. In such cases, the revocation form does not need to be filled in or filed. Otherwise, the form is part of the audit-related documents for a revocation process – see section 5.3.4.2.

6.4 Key recovery form for someone else's key

No specific form has been created for this process. The request, together with a detailed justification, must be submitted to the FOITT's PKI manager. The requisite documents are part of the audit-related documents for key recovery.

6.5 Checklist for issuing certificates without a RIO

The "Issuing class B certificates" checklist is used by the LRAO as an aid when issuing certificates, and does not need to be filled in or filed for each certificate issued.

6.6 Checklist for issuing certificates with a RIO

The "Issuance with RIO" checklist is used by the LRAO as an aid when issuing certificates, and does not need to be filled in or filed for each certificate issued.

6.7 RIO checklist

The RIO checklist is a mandatory element of the request for the "Issuance with RIO" process. For each request, the RIO must fill in the checklist and send it to the authorising LRAO, who must file it in the customer dossier. This checklist is part of the audit-related documents for an issuance process.

6.8 Checklist for revoking certificates

The "Revoking class B certificates" checklist is used by the LRAO as an aid when issuing certificates, and does not need to be filled in or filed for each revoked certificate.

7 Infringement of these guidelines

In the event of an infringement of these registration guidelines, the Swiss Government PKI can withdraw an LRAO's credentials and thus prevent them from issuing further end user certificates.

8 Escalation procedure

If you encounter things that need clarification, or have questions or problems relating to customers, the operation of the Swiss Government PKI or other organisational units, and you are unable to resolve them yourself, please contact the FOITT PKI manager.

9 Feedback/suggestions

Please send any feedback or suggestions for changes to this document or the forms to:

Trust Front End Product Owner
Federal Office of Information Technology, Systems and Telecommunication FOITT
Swiss Government PKI – Trust Front End (PS-PSC-TRU)
Eichenweg 3
CH-3052 Zollikofen
Email: pki-info@bit.admin.ch

Annex A: Document change history

Registr. Guide version	Topic	Section
V5.2	Definitions, acronyms and abbreviations – various additions and corrections	Definitions, acronyms and abbreviations
V5.2	Ref. [29]-[32] added	References
V5.2	Clarification: Class B certificates are only issued for natural persons	1.3
V5.2	Personnel security screening: A PSS or equivalent trustworthiness assessment is required by the hiring office	2.1 / 3.13
V5.2	Support for LRA now via the FOITT Service Desk or remedy ticket/MAC request	3.2 / 3.11 / 3.12
V5.2	Entrance controls: Requirements for LRA locations redefined	3.3
V5.2	Access controls: Requirements for protecting LRAO PCs changed to meet requirements for a federal client	3.4 / 3.5
V5.2	Forms and customer data: Clarification regarding storage	3.6
V5.2	Logs: New guidelines on keeping (electronic) logs, and access rights	3.7
V5.2	Clarifications on (electronic) access protection and retention periods for electronic documents	3.8 / 3.9
V5.2	Replacement of special LRAO certificates by the allocation of credentials on personal class B certificates	3.10
V5.2	Protecting the private key of the LRA station	Previously in section 3.10 – removed
V5.2	Replacement of the LRA station by federal workstation clients with LRAO functions	3.11 / 3.12
V5.2	Clarifications on the applicable laws on the protection of personal data	3.14
V5.2	Clarifications on the training and further education of LRAOs, correction and other information on the required points score	3.15 / 3.16
V5.2	PIN reset and PUK handling	New section 3.19
V5.2	Conformity check: Text revisions	4
V5.2	Process without RIO: Additions relating to the issuance process with F permits	5.2 / 5.2.3.2 / 5.2.3.7 / 5.2.4.2
V5.2	Entering an issuance request via request management systems (MAC, Gever) and approving identification with an F permit, including additional form	5.2.2 / 5.2.3.2
V5.2	Insertion of fields 4 and 5 ("adminGivenNameLong" and "adminSurNameLong") into AdminDir and LRAO tools, and the possible decision options for certificate issuance	5.2.3.1
V5.2	Inclusion of ID documents via scan	5.2.3.7
V5.2	Electronic data handling and archiving (scan files)	3.7/ 3.8 / 5.2.3.6 / 5.2.3.8 / 5.2.3.12 / 5.2.3.13
V5.2	Revocation: Clarification for requests by phone	5.3.2
V5.2	Revocation form: New guidelines for revocations using the Revocation Wizard	5.3.4.2 / 5.3.4.4 / 6.3
V5.2	Audit-related forms: Relevance added to the corresponding section	6.1 et seq.
V5.2	Request form: Requirements on requested data adjusted	6.1
V5.2	New guidelines on using the "*Confirmation of smartcard receipt*"	6.2
V5.2	Supplementary form for requesters with an F permit	New section 6.1.1
V5.2	Checklists – miscellaneous corrections	Annex A

Registr. Guide version	Topic	Section
V5.2	Forms – miscellaneous updates and corrections, new form for F permits	Annex B
V5.2	Forms – LRAO forms and FA and management added for completeness	Annex B
V5.2	Document change history, plus status and entry into force of the document	New annex: Annex C
V5.2	Checklists and forms changed	Annex B
V5.2	PIN reset superuser form and KRA request inserted in registration guidelines	Annex B
V5.9	Pre-approval version changes	V5.2 Registration guidelines
V5.9	Section 3.12: "Repair" deleted	Previously 3.12
V6.0	Post-approval version control	Version control
V6.1	LRA station replaced with LRA client or federal workstation client, only prestaged smartcards from now on	Miscellaneous sections
V6.1	Gender-neutral formulations	Entire document
V6.1	Unnecessary references removed, FADP, ISA and ISO inserted (instead of Federal Council directives and FITO)	References, section 3.13, miscellaneous sections
V6.1	Miscellaneous definitions, acronyms and abbreviations changed or added	Definitions, acronyms and abbreviations
V6.1	Annex A: Procedure for checklists and Annex B: Forms for class B certificates removed. The current documents can be found on the SG PKI website, references removed	Annex A, Annex B
V6.1	Guidelines in document removed (will be replaced by expanded user agreement)	Miscellaneous sections
V6.1	Support and availability of SG PKI changed	Section 3.2
V6.1	Example detailing required log entries expanded	Section 3.7
V6.1	Explanations on the subsequent electronic archiving of paper documents added	Section 3.8
V6.1	LRAO's liability extended	Section 3.13
V6.1	List of training points changed	Section 3.15
V6.1	Issuance process slightly changed/expanded	Section 5.2
V6.1	Need to involve LRAOs in the exit procedures added	Section 5.3.2.3
V6.4	Usage guidelines for workstation system (federal workstation client) added as new guideline to be complied with	Section 3.5
V6.4	Misc. changes to the RIO process, e.g. page 2 of request form must not be filed in the customer dossier	Section 5.2.4 et seq.
V7.0	New version of document following various changes and additions (acc. to change history) and gender neutrality of document	

Status of version 7.0: 14.01.2025

Entry into force of this version: 01.08.2025