



1 PKI Gemalto Smartcard

Erstellt am 25.01.2021

Inhalt:

1.1	PKI Zertifikat beantragen (grüne Gemalto Karte)	2
1.2	PKI-Zertifikat verlängern	2
1.3	PKI-Zertifikat löschen	2
	1.3.1 Bei Stellenaustritt	2
	1.3.2 Bei Verlust oder Defekt der PKI-Karte	2
1.4	Wichtige Informationen zum PIN	3
1.5	PIN ändern	3
1.6	PIN entsperren	4
	1.6.1 Schritt 1: E-Mail an Service Desk	4
	1.6.2 Schritt 2: PRU aufsuchen	4
	1.6.3 Der PRU führt folgende Schritte aus	5
	1.6.4 PIN Reset Dokumente	7
1.7	Karten- und Zertifikatsinformationen	8
	1.7.1 Suffix und Gültigkeit	8
	1.7.2 Gültigkeit, Seriennummer, Suffix (über Taskleiste)	9
1.8	Hinweise für Gemeinden und Kantonsspital	10
	1.8.1 Gemeinden	10
	1.8.2 Kantonsspital	10
1.9	PKI Voraussetzungen und Software	11
	1.9.1 Software für das Lesen der grünen Gemalto-Karten	11
	1.9.2 EJPD SSO-Portal	11
1.10	Infos für PIN Reset Superuser (Abraxas Service Desk, IT VD)	12
	1.10.1 Voraussetzungen	12
	1.10.2 Online-Ticket beim BIT erfassen	12



1.1 PKI Zertifikat beantragen (grüne Gemalto Karte)

Beantragen Sie ein neues Zertifikat

- falls Sie noch kein PKI-Zertifikat besitzen
- falls Sie Ihren Namen geändert haben
- falls Sie eine neue E-Mail-Adresse haben
- falls Sie eine weisse Atos-Karte besitzen und Ihr Zertifikat verlängert werden muss:
siehe 1.2 PKI-Zertifikat verlängern

Weitere Informationen sowie das Antrags- und Terminvereinbarungsformular finden Sie im Internet. Folgen Sie bitte den Anweisungen "Ein PKI-Zertifikat beantragen" unter diesem Link:

<https://www.sg.ch/wirtschaft-arbeit/pki/zertifikat-beantragen-verlaengern-loeschen.html>

1.2 PKI-Zertifikat verlängern

Keine Verlängerung von PKI-Zertifikaten auf weissen Atos-Karten

Ab dem 01.02.2021 werden PKI-Zertifikate ausschliesslich auf grünen Gemalto-Karten ausgestellt. Falls Sie eine weisse Atos-Karte besitzen, dürfen Ihre PKI-Zertifikate nicht verlängert werden, sondern es muss eine neue grüne Gemalto-Karte beantragt werden.

Beantragen Sie die Karte frühzeitig vor Ablauf Ihrer PKI-Zertifikate, d.h. gleich nach Erhalt der Systemmeldung: siehe 1.1 PKI Zertifikat beantragen (grüne Gemalto Karte).

1.3 PKI-Zertifikat löschen

1.3.1 Bei Stellenaustritt

Bei einem Stellenaustritt werden die Zertifikate von der PKI-Stelle nach dem letzten Arbeitstag gelöscht.

Retournieren Sie die PKI-Karte entweder persönlich oder über Ihren Vorgesetzten an die PKI-Stelle zusammen mit dem [Revokationsformular](#).

1.3.2 Bei Verlust oder Defekt der PKI-Karte

Informieren Sie bei Verlust oder Defekt der PKI-Karte unverzüglich die PKI-Stelle und reichen Sie einen Antrag zur Ausstellung einer neuen PKI-Karte ein. Folgen Sie bitte den Anweisungen "Ein PKI-Zertifikat beantragen" unter diesem Link:

<https://www.sg.ch/wirtschaft-arbeit/pki/zertifikat-beantragen-verlaengern-loeschen.html>

Die PKI-Stelle wird die Zertifikate auf der vermissten oder defekten PKI-Karte löschen und einen Termin für die Ausstellung der neuen Karte mit Ihnen festlegen.



1.4 Wichtige Informationen zum PIN

Zu Ihrer PKI-Karte gehört immer auch ein PIN (Passwort), mit dem Sie die Karte aktivieren. Nach fünfmaliger Falscheingabe des PINs wird die Karte gesperrt. Sie können die Karte nur noch durch einen PIN Reset entsperren: siehe 1.6 PIN entsperren.

Beachten Sie, dass laut Vorgaben des Bundesamtes für Informatik und Telekommunikation (BIT) der PIN absolut vertraulich zu behandeln ist. Er darf anderen Personen nicht zugänglich gemacht werden. Insbesondere ist es auf gar keinen Fall gestattet, den PIN auf der Karte zu notieren. Auch das Sammeln und Verwalten der PINs aller Mitarbeitenden in einer Dienststelle ist nicht erlaubt.

Details regeln die Guidelines zu Klasse B Zertifikaten der Swiss Government PKI.

1.5 PIN ändern

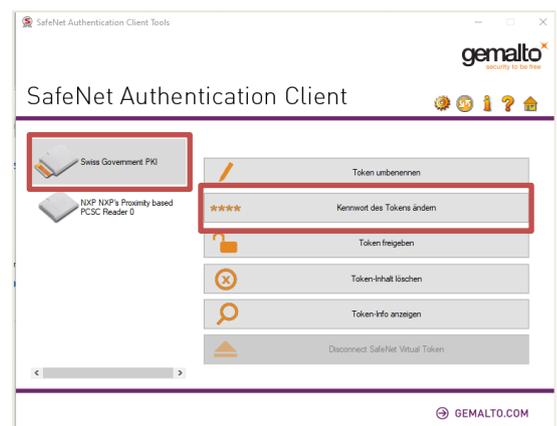
Informationen zur Software unter 1.9 PKI Voraussetzungen und Software.

Über Start, Programme den "SafeNet Authentication Client" öffnen.



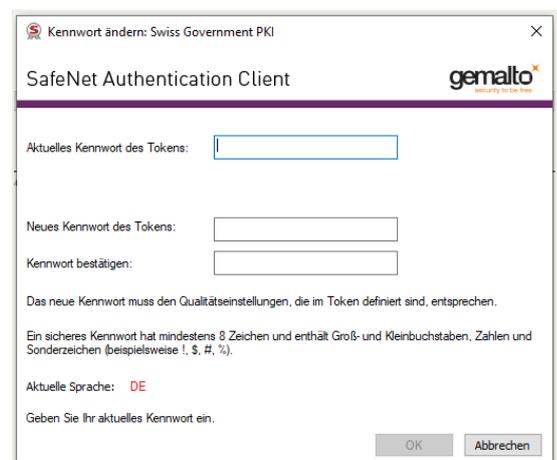
Auf der linken Seite "Swiss Government PKI" wählen.

Rechts auf die Schaltfläche "Kennwort des Tokens ändern" klicken.



1. Geben Sie Ihr aktuelles Passwort ein.
2. Geben Sie Ihr neues Passwort ein. Entgegen den Angaben auf der Eingabemaske sind keine Sonderzeichen möglich.
3. Geben Sie nochmals Ihr neues Passwort ein.
4. Bestätigen Sie Ihre Eingabe mit "OK".

Ein erfolgreicher Passwortwechsel wird bestätigt. Falls Sie das neue Passwort nicht zweimal identisch erfassen oder falls das Passwort nicht den Regeln entspricht, wird eine Fehlermeldung angezeigt. Korrigieren Sie in diesem Fall Ihre Eingaben.





1.6 PIN entsperren

Informationen zur Software unter 1.9 PKI Voraussetzungen und Software.

Nach einer fünfmaligen Fehleingabe des Benutzer-PIN ist die PKI-Karte gesperrt. Um sie zu entsperren, muss ein PIN Reset in zwei Schritten durchgeführt werden.

1.6.1 Schritt 1: E-Mail an Service Desk

Beauftragen Sie den Abraxas Service Desk per E-Mail einen PIN Reset zu starten. Für Gemeinde- und Kantonsspitalmitarbeitende ist das PKI-Team zuständig.

Verwenden Sie bitte ausschliesslich diese E-Mail-Vorlage für Ihren Auftrag und ergänzen Sie die nötigen Informationen: [Zu den Mail-Vorlagen](#).

Nach Eingang Ihres Auftrages wird der Service Desk, respektive das PKI-Team für Sie ein Online-Ticket beim Bundesamt für Informatik und Telekommunikation (BIT) eröffnen und Ihnen mitteilen, wann Sie den nächsten Schritt vornehmen können.

1.6.2 Schritt 2: PRU aufsuchen

Begeben Sie sich mit Ihrer gesperrten PKI-Karte zum PIN Reset User (PRU).

Wenn Sie den PRU nicht persönlich kennen, nehmen Sie Ihre gültige ID oder Ihren gültigen Reisepass mit.

Wer ist PRU?

PRU kann jeder Mitarbeitende mit einer weissen oder grünen PKI-Karte sein. Wichtig ist, dass seine Zertifikate noch gültig sind.

Es müssen für den PIN Reset zwei Kartenlesegeräte zur Verfügung stehen.

Die Software "PIN Reset" und "SafeNet Authentication Client" müssen auf dem Gerät des PRU installiert sein (Standard im Kanton, weitere Informationen unter 1.9 PKI Voraussetzungen und Software).

PIN Reset beim PRU:

Der PRU und Sie, der Inhaber der gesperrten Karte, werden mittels PIN Reset Wizard durch den Prozess geführt.

Das zweite Kartelesegerät muss angeschlossen sein.

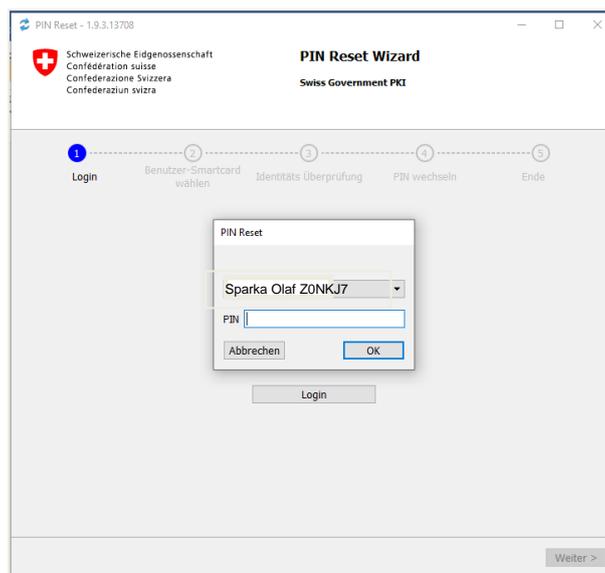


1.6.3 Der PRU führt folgende Schritte aus

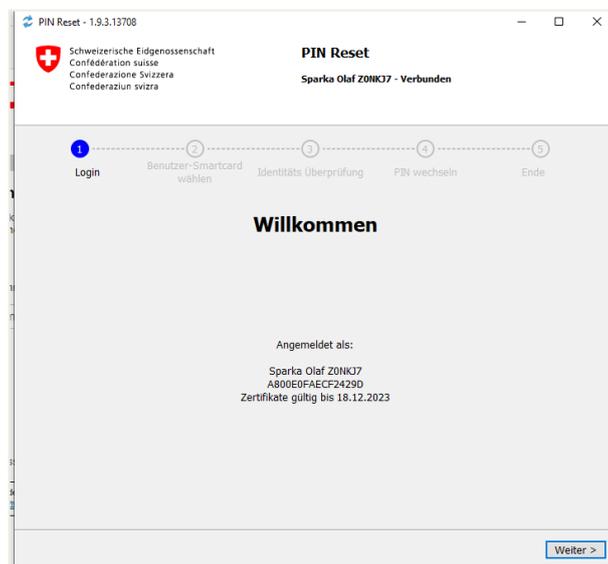
- prüft Ihre ID oder Ihren Pass (falls er Sie nicht persönlich kennt).
- öffnet die App "PIN Reset" über Start / Programme, um den PIN Reset Wizard zu starten



- meldet sich mit seiner PKI-Karte durch die Eingabe des PINs und den OK-Button beim PIN Reset Programm an

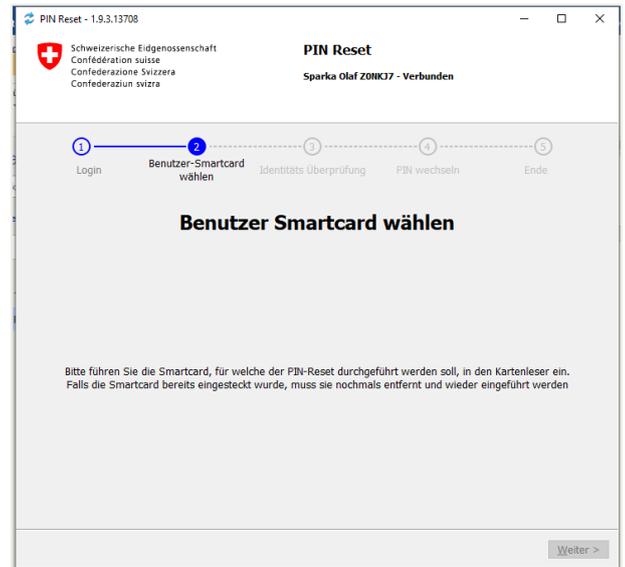


- klickt nach Bestätigung der Anmeldung auf "Weiter"

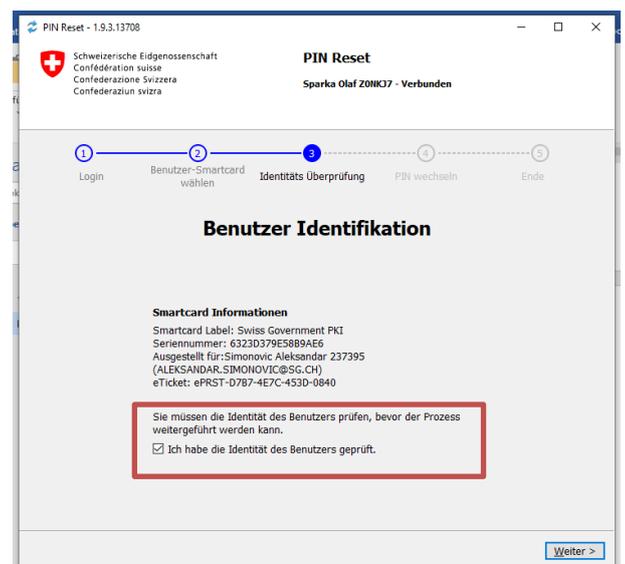




- führt die gesperrte Karte in das zweite Kartenlesegerät ein
- klickt auf "Weiter"



- identifiziert Sie mittels ID oder Pass, falls er Sie nicht persönlich kennt
- setzt ganz unten das Häkchen zur Bestätigung der Identifikation
- klickt auf "Weiter"



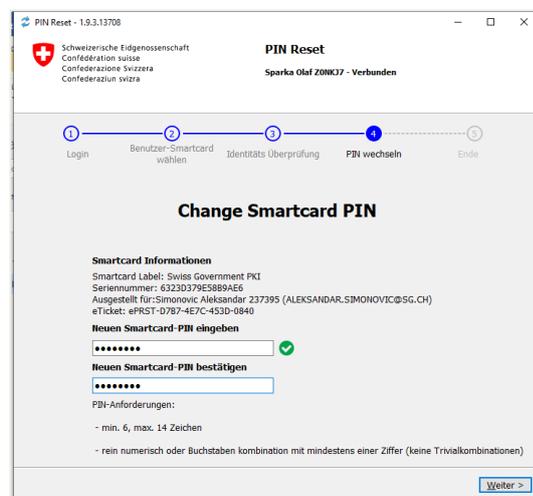
- überlässt Ihnen das Arbeitsgerät



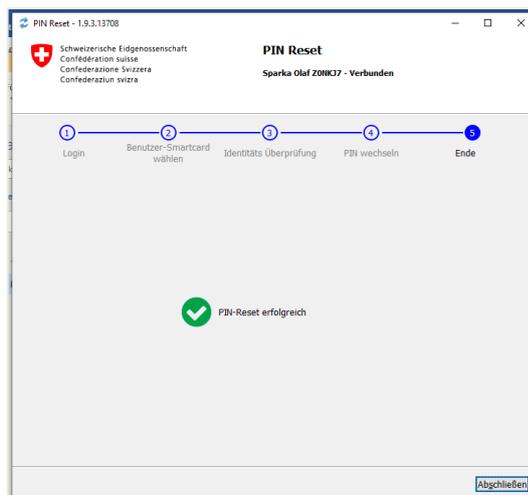
Neuen PIN erfassen

Sie, der Inhaber der gesperrten Karte:

- geben zweimal den neuen PIN ein:
Abweichend von den Angaben auf der Erfassungsmaske sind keine rein numerischen PINs möglich, auch keine Sonderzeichen
- klicken auf "Weiter"



- schliessen nach dem erfolgreichen PIN-Reset den Wizard mit Klick auf "Abschliessen"
- können nun mit Ihrer Karte zurück zu Ihrem Arbeitsplatz



1.6.4 PIN Reset Dokumente

[Quickguide](#)

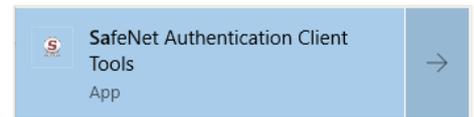
[Prozessbeschreibung](#)

1.7 Karten- und Zertifikatsinformationen

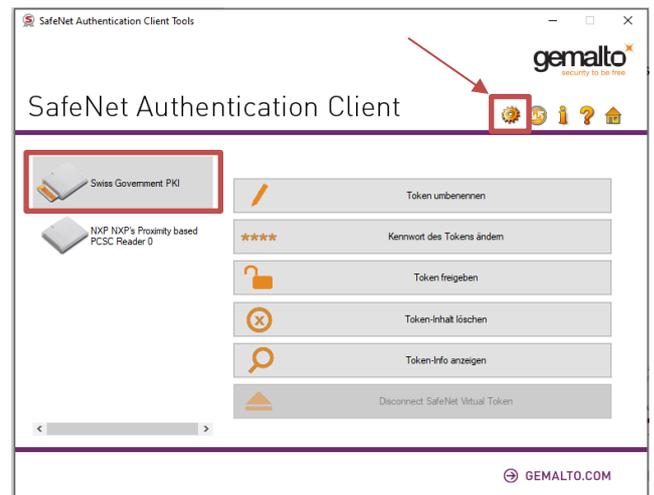
Über den Gemalto Authentication Client lassen sich verschiedene Informationen zu Ihren Zertifikaten und zur PKI-Karte anzeigen wie das Suffix, die Gültigkeit oder die Seriennummer.

1.7.1 Suffix und Gültigkeit

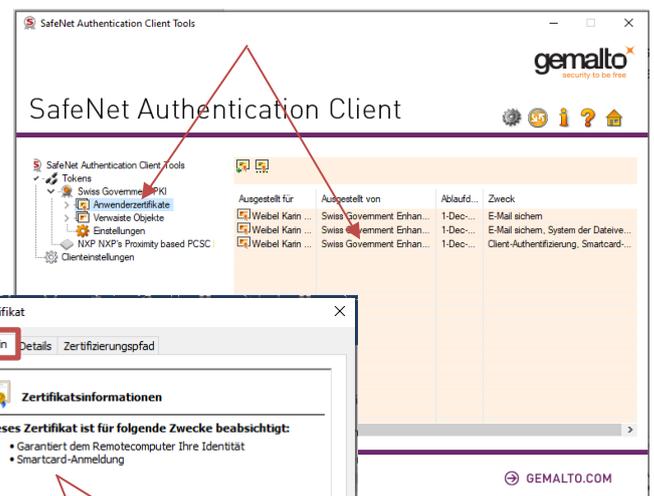
- Anwendung "SafeNet Authentication Client" öffnen



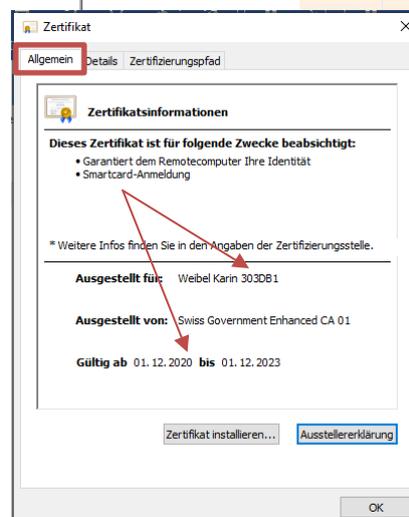
- Auf der linken Seite "Swiss Government PKI" wählen und rechts oben über das Zahnrad zu den Einstellungen



- Auf der linken Menüleiste Klick auf "Anwenderzertifikate": Die bestehenden Zertifikate werden rechts aufgelistet
- Klick auf eines der Zertifikate



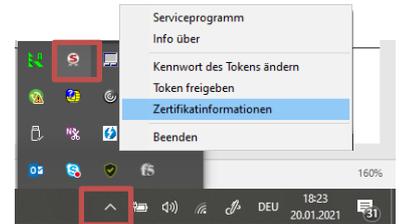
- Die Informationen werden im Fenster "Zertifikat" angezeigt. Das Suffix sowie die Gültigkeit des Zertifikates sind unter dem Register "Allgemein" ablesbar.



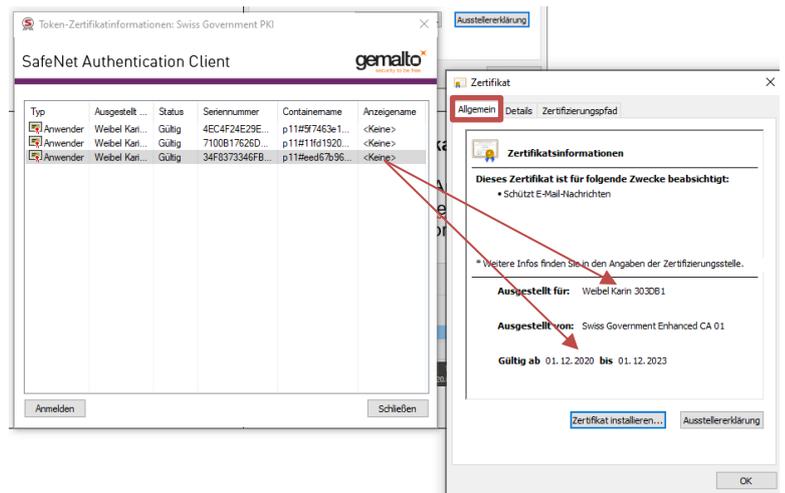


1.7.2 Gültigkeit, Seriennummer, Suffix (über Taskleiste)

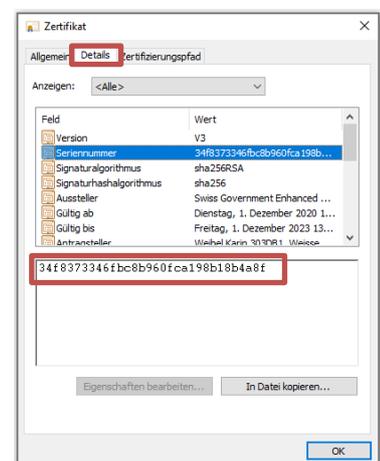
- Taskleiste unten links: Ausgeblendete Symbole anzeigen lassen
- Rechtsklick auf SafeNetClient-Symbol
- Zertifikationsinformationen wählen



- Auf der angezeigten Zertifikatsliste Doppelklick auf ein Element
- Unter Register "Allgemein" wird das Suffix und die Gültigkeit angezeigt



- Unter Register "Details" wird die Seriennummer durch Markieren der Zeile im unteren Bereich komplett angezeigt.





1.8 Hinweise für Gemeinden und Kantonsspital

1.8.1 Gemeinden

Die genauen Prozesse der Gemeinden sind durch deren Informatikverantwortliche definiert. Bei Fragen kontaktieren Sie daher bitte immer zuerst diese Stelle.

Zertifikat beantragen

Eintrag im PKI-System veranlassen:

Der Informatikverantwortliche der Gemeinde muss einen Standard Account bei Abraxas bestellen und das Flag „DIP PKI Angebot“ setzen. Eine Anleitung ist hier abrufbar:

[Hinweise für Gemeinden / Kantonsspital | sg.ch](#)

Der Eintrag wird über Nacht nach Bern übertragen, d.h. frühestens am Folgetag können die Zertifikate ausgestellt werden.

Von Vorteil ist es, wenn der Informatikverantwortliche prüft, ob die Übertragung auch wirklich stattgefunden hat.

Wichtig: Jede neue Karte muss durch den Mitarbeitenden zuerst beim Service Desk des ISC-EJPDs freigeschalten werden, damit die Verbindung mit Infostar möglich ist.

Kontakt: servicedesk@isc-ejpd.admin.ch oder Tel. 058 463 78 78.

Weitere Informationen unter 1.9 PKI Voraussetzungen und Software.

1.8.2 Kantonsspital

Für die Ausstellung der Zertifikate ist die PKI-Stelle im Volkswirtschaftsdepartement zuständig.

Kontaktperson für alle anderen Fragen ist Herr Christian Cossu, christian.cossu@kssg.ch.

Weitere Informationen unter 1.9 PKI Voraussetzungen und Software.



1.9 PKI Voraussetzungen und Software

1.9.1 Software für das Lesen der grünen Gemalto-Karten

Ab dem 01.02.2021 werden die PKI-Zertifikate ausschliesslich auf Gemalto-Karten ausgestellt. Die Karten sind grün und unterscheiden sich damit optisch von den bisherigen weissen Atos-Karten.

Zum Verwenden der Karte muss der "Gemalto SafeNet Authentication Client" installiert sein. Für einen PIN-Reset der grünen Karte muss beim PIN Reset User (PRU) der "Gemalto SafeNet Authentication Client" und die Software "PIN Reset" installiert sein (siehe 1.6 PIN entsperren).

Auf den Geräten des Kantons sind diese Voraussetzungen gegeben. Sollte die Anwendung "Gemalte Safe Net Authentication Client" fehlen, kann sie über das Abraxas Serviceportal bestellt werden: UG-264-C SafeNetAthenticationClient (Gemalto).

Kontaktstelle für Gemeinden bei Fragen zur Software ist der Informatikverantwortliche der Gemeinde. Für das Kantonsspital ist Christian Cossu zuständig, christian.cossu@kssg.ch. Sollten hier nicht alle Fragen geklärt werden können, wenden Sie sich an das PKI-Team пки@sg.ch.

1.9.2 EJPD SSO-Portal

Eine Anleitung für die Umstellung (Switch) auf dem LocalProxy des EJPD SSO-Portals von der weissen Atos-Karte auf die grüne Gemalto-Karte ist hier abrufbar:

[Hinweis für Benutzer EJPD SSO-Portal | sg.ch](#)



1.10 Infos für PIN Reset Superuser (Abraxas Service Desk, IT VD)

1.10.1 Voraussetzungen

Der PIN Reset Superuser verfügt über die Berechtigung vom Bundesamt für Informatik und Telekommunikation (BIT) zur Online-Ticketerstellung für PIN Resets.

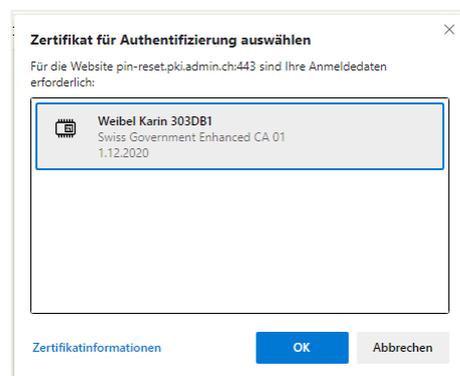
[Link zum Antragsformular](#)

1.10.2 Online-Ticket beim BIT erfassen

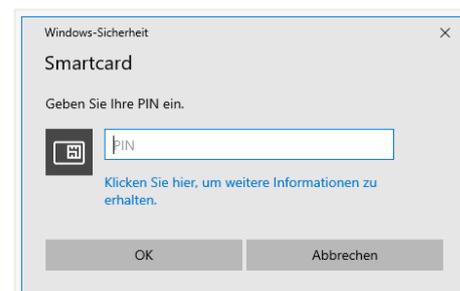
Der PIN Reset Superuser / Abraxas Service Desk

– meldet sich mit seiner PKI-Karte unter diesem Link an:
<https://pin-reset.pki.admin.ch/PINResetRequest/>

– bestätigt die Auswahl des Zertifikates mit OK



– gibt den PIN seiner PKI-Karte ein und bestätigt mit OK





- startet die Smartcard PIN Reset Anfrage mit Eingabe der Benutzerdaten im Suchfeld in dieser Form:

Nachname Vorname Suffix

Swiss Government PKI Kontakt: csi-info@bit.admin.ch

Bundesamt für Informatik und Telekommunikation BIT
info@bit.admin.ch | [Rechtliches](#)

- falls der Benutzer seine Suffix nicht weiss, kann es über das AdminDir-Adressbuch in Outlook angezeigt werden:

Namen auswählen: admindir.admin.ch

Suchen: Nur Name Mehr Spalten

Simonovic Aleksandar

Adressbuch
admindir.admin.ch - Weitere Adressbücher

Name	E-Mail-Adresse	E-...	Telefon geschä
Simonovic Aleksandar 237395	Aleksandar.Simonovic@sg.ch		SMTP

- startet die Anfrage mit dem Button "Anfrage"

Swiss Government PKI Kontakt: csi-info@bit.admin.ch

Bundesamt für Informatik und Telekommunikation BIT
info@bit.admin.ch | [Rechtliches](#)

Common Name	Email	Token S/N	PIN Reset
Simonovic Aleksandar 237395	ALEKSANDAR.SIMONOVIC@SG.CH	6323D379E58B9AE6	<input type="button" value="Anfrage"/>

Zertifikat 20675952E2136F2ABB324E481EE403BB / Status: valid
Zertifikat 145A7016C45A97FD9C69A1A626C28A0E / Status: valid
Zertifikat 5D495427EF325E6AF55D13147C712F1 / Status: valid



- bestätigt die erfolgreiche Identifikation durch Setzen des entsprechenden Häkchens oder bricht den Prozess ab, wenn die Person nicht eindeutig identifiziert werden kann.

Status: valid

Zertifikat 145A7016C45A97FD9C69A1A626C28A0E
cn: Simonovic Aleksandar 237395
Gültig ab: 2021/01/11 09:53:31 UTC
Gültig bis: 2024/01/11 09:53:31 UTC
Status: valid

Zertifikat 5D4954277EF325E6AF55D13147C712F1
cn: Simonovic Aleksandar 237395
Gültig ab: 2021/01/11 09:53:31 UTC
Gültig bis: 2024/01/11 09:53:31 UTC
Status: valid

Bevor eine PIN Reset Anfrage gestartet werden kann muss die Identität des Anwenders anhand der Revokationsfrage / Antwort geprüft werden.

Frage: Wie heisst meine Lieblingsband?
Antwort: Delfones

Ich habe die Identität des Anwenders anhand der Revokationsfrage / Antwort verifiziert.

Abbrechen

- startet nach Setzen des Häkchens die Anfrage ans BIT über den grünen Button.
- informiert den Benutzer mit der gesperrten Karte, dass er einen PIN Reset User aufsuchen kann.

Ich habe die Identität des Anwenders anhand der Revokationsfrage / Antwort verifiziert.

Abbrechen PIN Reset Anfrage starten