



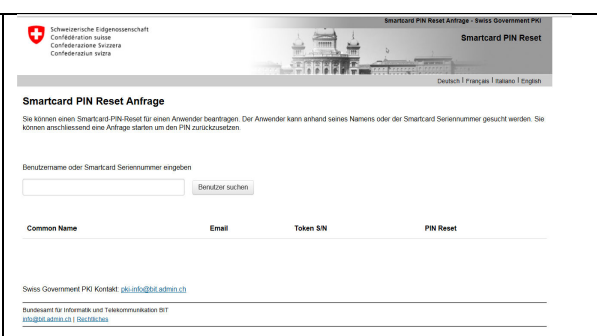
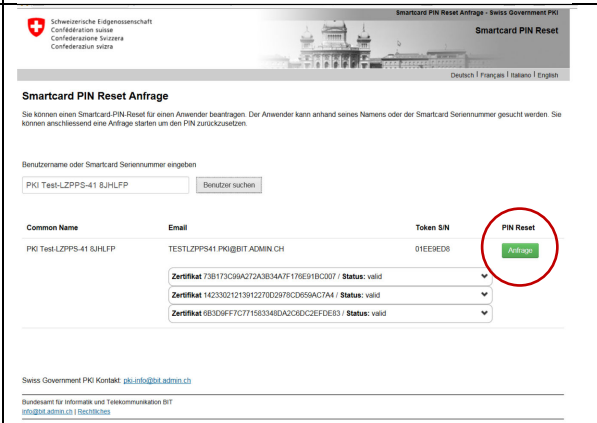
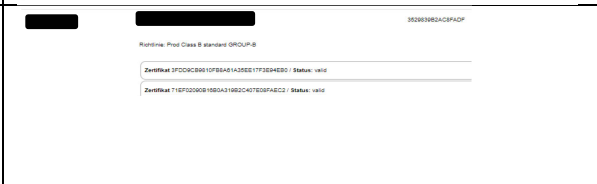
NICHT KLASSIFIZIERT

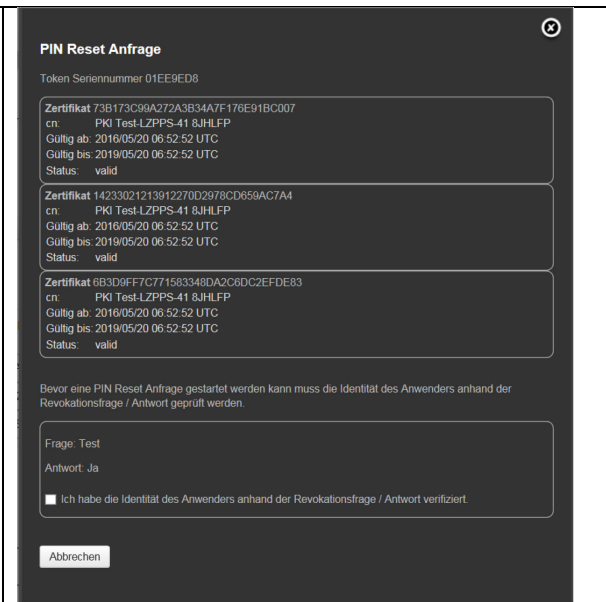
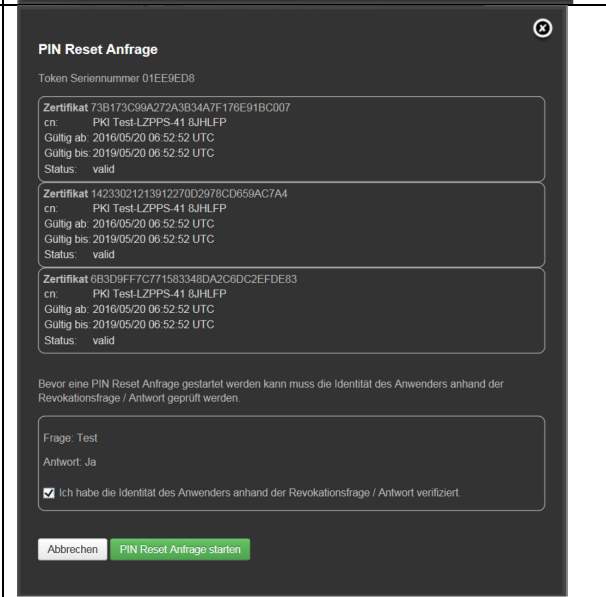
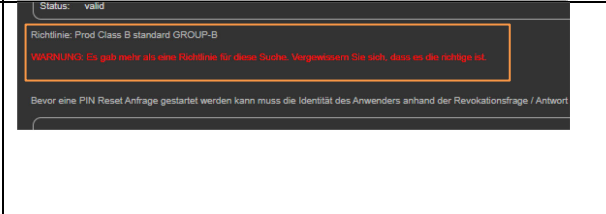

PIN-Reset Wizard

Quickguide zur Rücksetzung der Benutzer-SmartCard PIN

V1.2, 15.01.2024

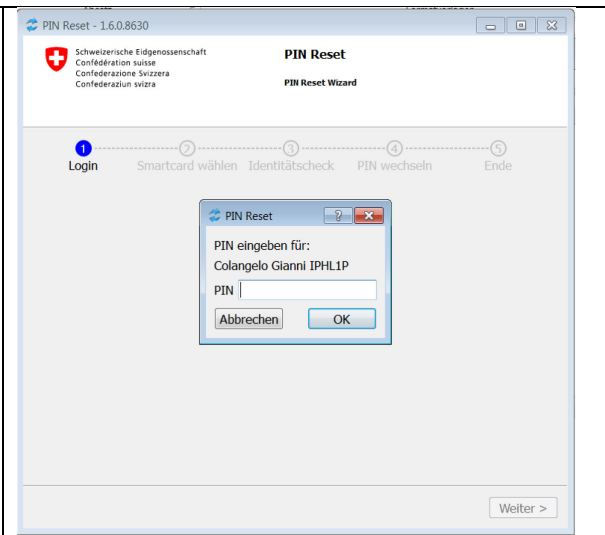
1 Ablauf für den Servicedesk/ Superuser

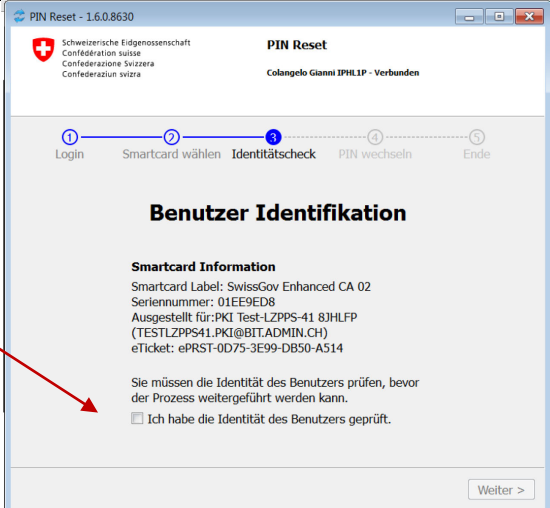
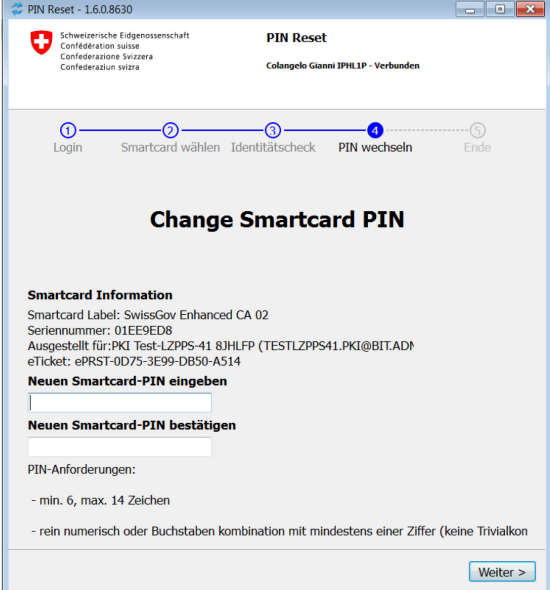
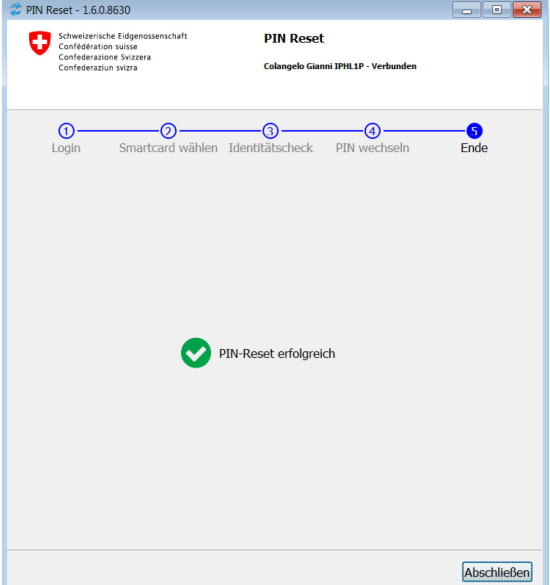
<p>Die Berechtigung auf die URL https://ra.pki.admin.ch/PINResetRequest/ wird von der SG-PKI auf das persönliche Klasse B Zertifikat erteilt (mittels Formular: <i>Antragsformular für PIN Reset für Superuser/ Servicedesks</i> auf der PKI Homepage www.pki.admin.ch unter <i>Zertifikats-typen</i> → <i>Klasse B</i> → <i>Prestaged</i>)</p> <p>Starten Sie die URL für die Ticketerstellung.</p>	
<p>Suchen Sie den Benutzer mit „Namen*“ oder mit der Seriennummer der Smartcard des Benutzers.</p> <p>Klicken Sie bei mehreren Möglichkeiten den richtigen Benutzer an und starten Sie die Anfrage mit dem Button „Anfrage“.</p>	
<p>Mit der neuen Version 2024 der Seite wird eine zusätzliche Information angezeigt, der Name der Policy für die Zertifikaten. Dies kann Ihnen helfen, den richtigen Benutzer auszuwählen, wenn die Suche mehrere Homonyme zurückgibt.</p>	

<p>Überprüfen Sie zuerst die Angaben: Token Seriennummer CN Status</p> <p>Identifizieren Sie Ihren Kunden anhand der Telefonnummer Face-To-Face mit ID/Pass Evtl. kennen Sie die Person</p> <p>UND: Mit der Revokationspassphrase (Frage stellen) im Kasten.</p> <p>Klicken Sie das Kästchen bei erfolgreicher Identifikation an,</p> <p>Oder brechen Sie bei nicht Erfolg den Prozess ab.</p>	
<p>Ist die Identifikation erfolgreich, erscheint nach dem Setzen des Häkchens der Button „PIN Reset Anfrage starten“ (in grün).</p> <p>Klicken Sie auf den Button um das Ticket zu eröffnen.</p>	
<p>Mit der neuen Version 2024 der Seite wird der Name der Policy des Zertifikats zurückgerufen. Es kann sein, dass Sie eine Warnmeldung erhalten, wenn der gesuchte Benutzer Zertifikate von mehreren verschiedenen Policy ausgestellt hat. So können Sie überprüfen, ob es sich um den richtigen Benutzer handelt.</p>	
<p>Verlassen Sie den Browser oder fahren Sie mit einem weiteren Userticket fort.</p>	

2 Ablauf für den PIN Reset User (PRU)

Wer ist PRU? Die Funktion PRU wird von der jeweiligen Organisation ausgewählten Benutzern zugeteilt. Dazu wird keine spezielle Berechtigung im PKI-System benötigt. Ein Merkblatt für den PRU ist im Kap.3 beigefügt.

<p>Öffnen Sie den PIN Reset Wizard und loggen Sie sich mit Ihrem Klasse B Zertifikat und dem dazugehörigem PIN ein.</p>	
<p>Klicken Sie auf „Weiter“.</p>	
<p>Führen Sie nun die gesperrte Karte in den Reader.</p>	

<p>Identifizieren Sie die Person, die den PIN-Reset durchführen möchte.</p> <p>Die Identität wird mittels ID/ Pass geprüft, oder Sie kennen die Person persönlich.</p> <p>Setzen Sie bei erfolgreicher Identifikation zu-unterst das Häkchen zur Bestätigung.</p> <p>Die „Weiter“-Taste wird aktiviert. Fahren Sie damit fort.</p>	
<p>Die Smartcard Information wird angezeigt. Nun kann der Benutzer eine neue PIN eingeben und bestätigen.</p> <p>Klicken Sie danach auf „Weiter“.</p>	
<p>Die PIN wurde geändert, schliessen Sie die Applikation mit dem letzten „Abschliessen“ Knopf ab.</p>	

3 Merkblatt für PRUs (PIN Reset User)

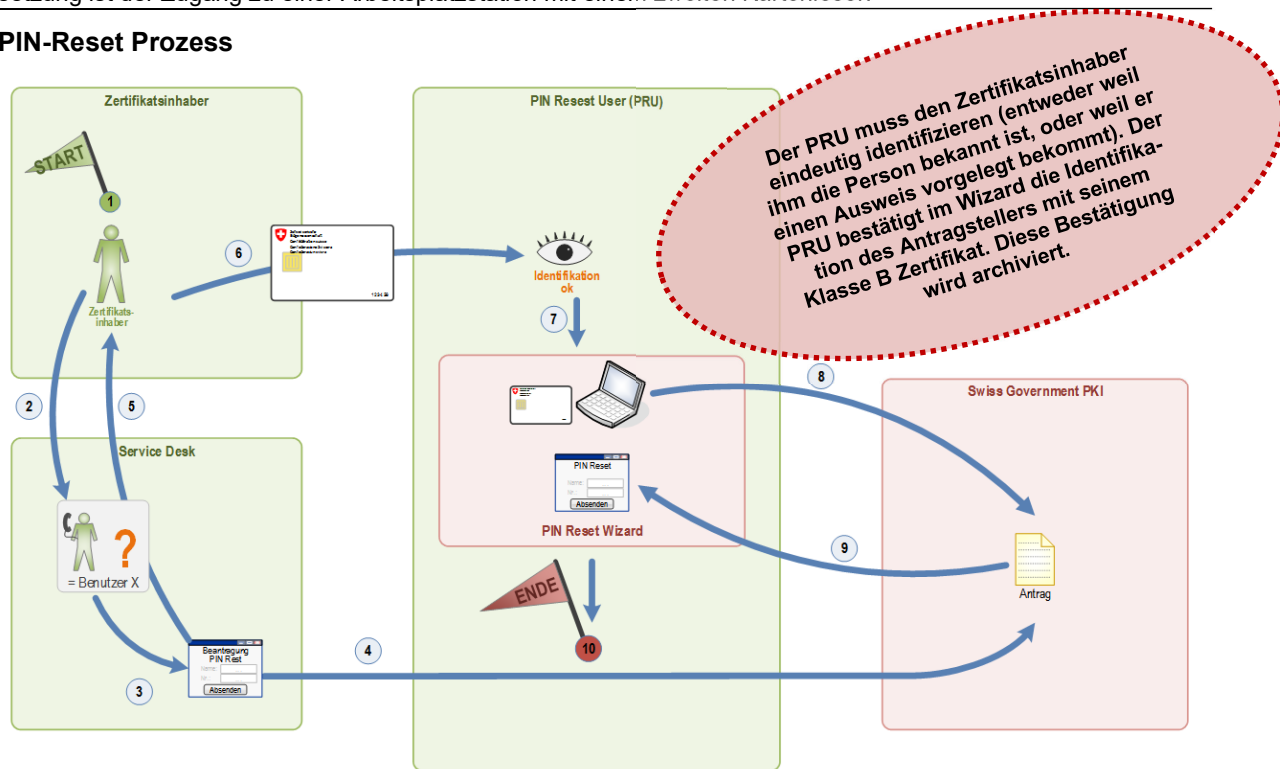
Was ist ein PRU? Ein PIN Reset User ist eine Person im Besitze eines Klasse B Zertifikats der Swiss Government PKI, die einer anderen Person der BV mit Hilfe des PIN Reset Wizards eine blockierte Smartcard entsperren kann.

Wer ist PRU? Die Funktion PRU wird von der jeweiligen Organisation ausgewählten Benutzern zugeteilt. Dazu wird keine spezielle Berechtigung im PKI-System benötigt.

Wann braucht man einen PRU? Ist der PIN der eigenen Smartcard einmal blockiert (z.B. weil man zu viele Fehlversuche bei der PIN-Eingabe hatte), muss das Service Desk kontaktiert werden und zusätzlich ein PRU aufgesucht werden.

Voraussetzungen: Jeder Benutzer mit einem gültigen Klasse B Zertifikat kann als PRU agieren. Weitere Voraussetzung ist der Zugang zu einer Arbeitsplatzstation mit einem zweiten Kartenleser.

PIN-Reset Prozess



Erläuterungen

Nr.	Element	Erläuterung
1	1	Smartcard des Zertifikatsinhabers ist gesperrt
2	2	Der Zertifikatsinhaber kontaktiert telefonisch das Service Desk
3	3	Das Service Desk plausibilisiert die Identität des Zertifikatsempfängers anhand der beim Service Desk hinterlegten persönlichen ‚Magic Questions‘
4	4	Das Service Desk eröffnet mit der WEB-Anwendung der PKI das PIN-Reset Ticket. Dabei muss die Seriennummer der gesperrten Smartcard eingefüllt werden.
5	5	Der Zertifikatsinhaber wird vom Service Desk instruiert, den nächstgelegenen PIN Reset User aufzusuchen.
6	6	Der Zertifikatsinhaber begibt sich mit der gesperrten Smartcard zum PIN Reset User
7	7	Der PRU identifiziert den Zertifikatsinhaber, entweder weil er diesen persönlich kennt oder dessen gültigen Ausweis kontrolliert hat.
8	8	Nach Einführung der gesperrten Smartcard sucht der Wizard nach dem entsprechenden Ticket im PKI-System
9	9	Der benötigte PUK wird vom PKI-System an den Wizard in verschlüsselter Form übermittelt. Der Zertifikatsinhaber gibt den neuen PIN ein und der Wizard entspermt die Karte mit dem PUK und setzt gleichzeitig den neuen PIN.
10	10	Die Karte ist entspermt und wieder einsatzbereit.