



17.10.2024

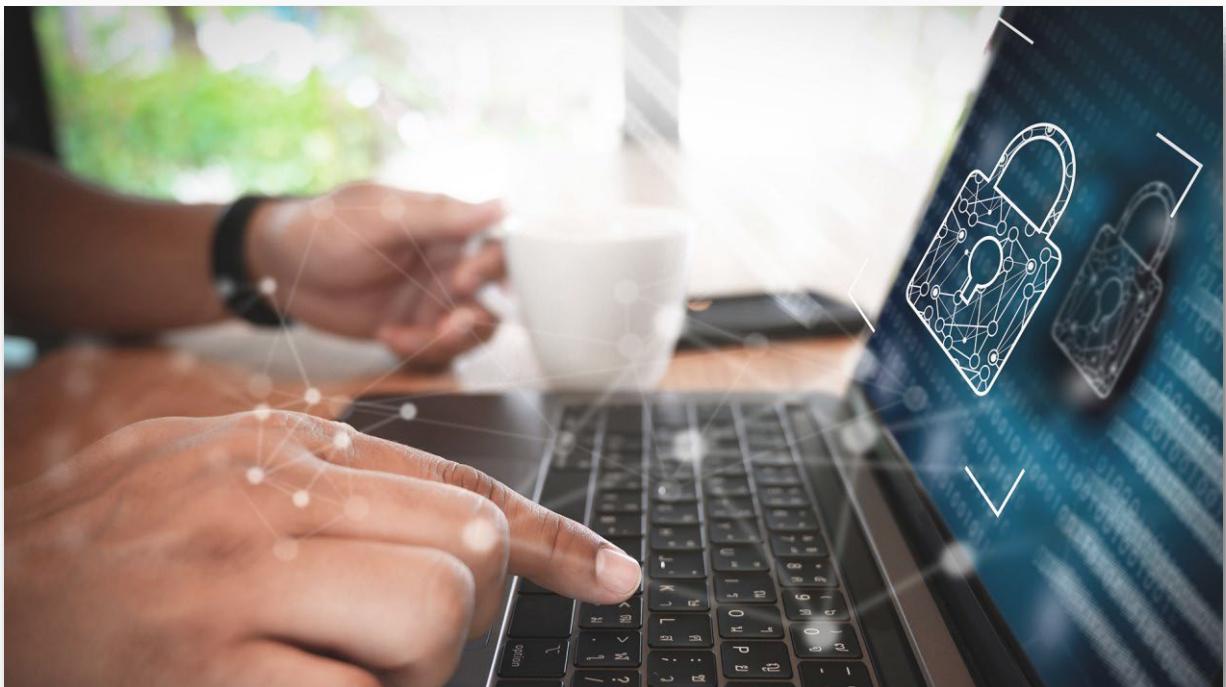
Quick Guide

Key Recovery Wizard

Wiederherstellung von Verschlüsselungszertifikaten

Status: Freigegeben

V2.0



Die zertifikatsinhabende Person bemerkt, dass sie eine alte verschlüsselte E-Mail nicht mehr lesen kann, weil der zugehörige private Schlüssel nicht mehr auf seiner gegenwärtigen Smartcard gespeichert ist.

Sie ruft in seinem Browser die Anwendung «Key Recovery» auf und erstellt damit ein eTicket im zentralen PKI-System.

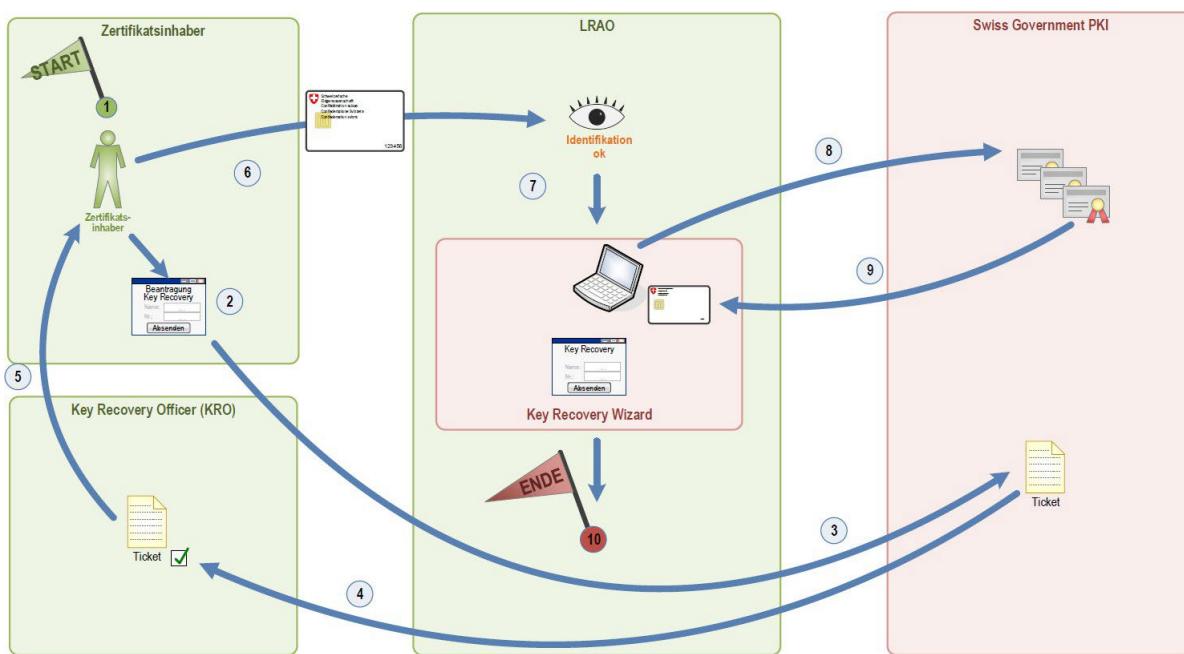
Ein [Lernvideo](#) und die [Prozessbeschreibung](#) finden Sie auf unserer [PKI Homepage](#).

Prozess

Die zertifikatsinhabende Person ruft in ihrem Browser die Anwendung «Key Recovery» auf und erstellt damit ein eTicket im zentralen PKI System.

Mit der eTicket-Nummer und seiner Smartcard begibt sie sich zu seinem zuständigen LRA-Officer. Nachdem sie vom LRA-Officer identifiziert wurde, startet der LRAO den Key Recovery Wizard und gibt die eTicket-Nummer ein. Der Wizard zeigt darauf alle für diese Person je ausgestellten Encryption Zertifikate an.

Die zertifikatsinhabende Person gibt dem LRA-Officer diejenigen Schlüssel an, die sie wiederherstellen möchte. Nach Eingabe ihrer persönlichen PIN, schreibt der Wizard die gewählten Encryption Keys auf die Smartcard der Person.



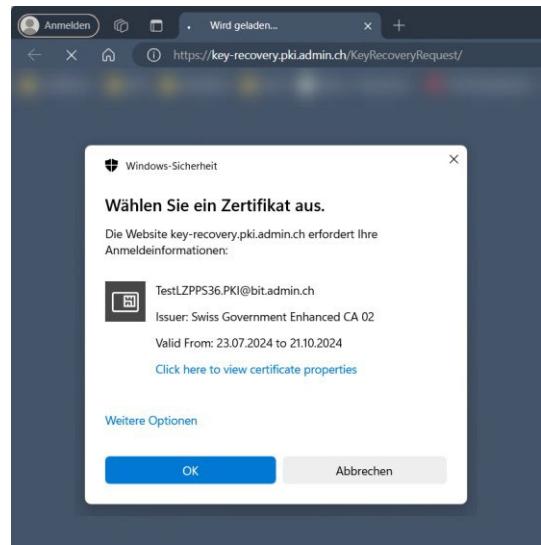
Erläuterung

Nr.	Element	Erläuterung
1	1	Die zertifikatsinhabende Person stellt fest, dass sie eine E-Mail nicht entschlüsseln kann, weil ihr der entsprechende private Encryption Key fehlt.
2	2,3	Mit dem Web-Tool 'KeyRecoveryRequest' öffnet sie ein eTicket für das Key Recovery.
3	4	Der KRO (Key Recovery Officer) erhält vom System die Aufforderung, den Key Recovery Request zu bewilligen (nur in bestimmten Ämtern)
4	5	Nach der Bewilligung des Requests durch den KRO wird der Zertifikats Inhabenden Person die eTicket-Nummer mitgeteilt.
5	6	Mit der eTicket-Nummer sucht sie ihren zuständigen LRA-Officer auf.
6	7,8,9	Der LRA-Officer startet den Recovery Wizard und wählt mit der zertifikatinhabende Person die wiederherzustellenden Schlüssel aus. Diese werden vom Wizard auf die Smartcard geschrieben.

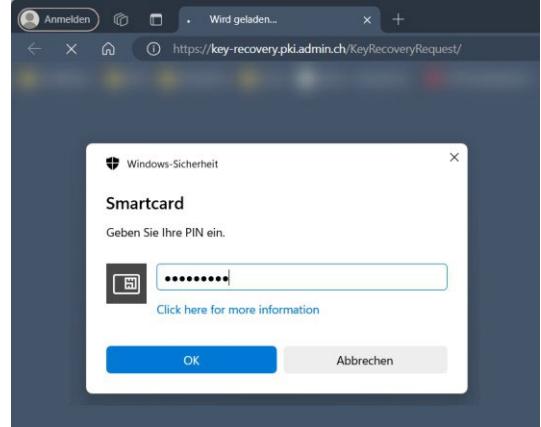
1 Starten des Key Recovery Antrags (zertifikatsinhabende Person)

Benutzen Sie Ihr aktuell gültiges Klasse B Zertifikat, um auf den [Antragslink](#) zu kommen:

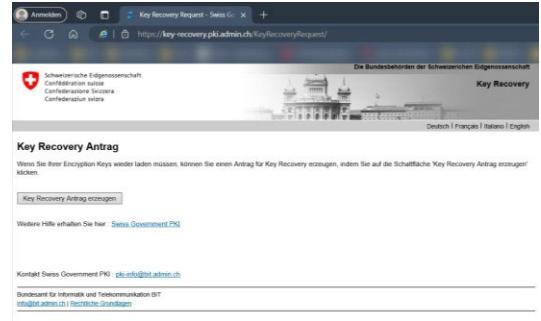
1. <https://key-recovery.pki.admin.ch/Key-RecoveryRequest>
2. Oder suchen Sie in der Windows-Suche nach «Key Recovery Request».



Geben Sie danach den PIN Ihrer SmartCard ein.



Klicken Sie auf Key Recovery Antrag erzeugen



Im Bestätigungsfeld der Antragsübergabe erhalten Sie eine Übersicht der archivierten Schlüssel.

Sie können den Internet-Browser nun verlassen.

The screenshot shows a web browser window titled "Key Recovery Request - Swiss G" with the URL "https://key-recovery.pk.admin.ch/KeyRecoveryRequest/". The page header includes the Swiss Government logo and the text "Die Bundesbehörden der Schweizerischen Eidgenossenschaft" and "Key Recovery". Below the header, there is a message: "Vielen Dank. Sie haben Ihren Antrag erfolgreich eingesetzt." A table titled "Archivierte Schlüssel" (Archived Keys) is displayed, showing two entries:

Seriennummer	Antragsteller CN	Aussteller CN	Gültig ab	Gültig bis	Anzahl erforderliche Genehmigungen
8500_7108	PKI Test LZPPS-36 BZK0.02	Swiss Government Enhanced CA 02	2024/07/23 09:05:16 UTC	2024/10/21 09:05:16 UTC	0
18AC_31A7	PKI Test LZPPS-36 BZK0.02	Swiss Government Enhanced CA 02	2022/07/08 09:34:23 UTC	2022/10/06 09:34:23 UTC	0

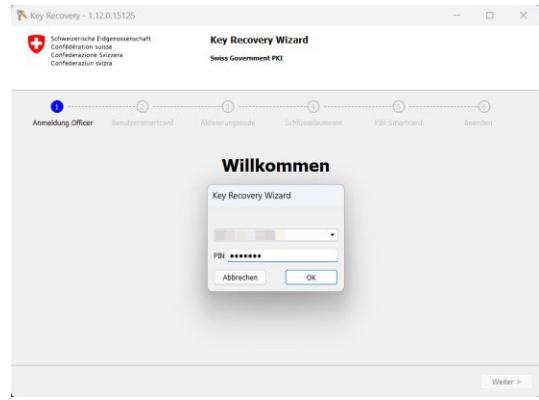
Im nächsten Schritt erhalten Sie ein Bestätigungsmaill auf Deutsch und Englisch in Ihrer Mailbox.

(Braucht es eine Genehmigung erfolgt die Mail nach der Freigabe des Auftrags durch eine dedizierte Person, die diese Funktion in Ihrem Amt ausübt).

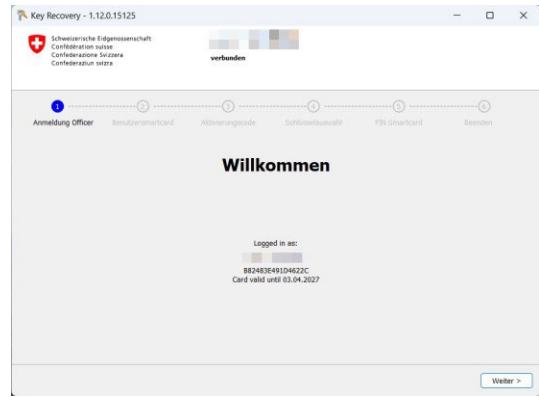
Die **eTicket-Nummer** in der Mail wird vom LRA-Officer für die Wiederherstellung des Schlüssels benötigt. Begeben Sie sich damit zu einem LRA-Officer oder einem berechtigten Key Recovery Officer.

2 Schlüssel-Wiederherstellung (LRAO/Key Recovery Officer)

Loggen Sie sich mit Ihrer berechtigten LRAO-Karte im Key Recovery Wizard ein.



Der Wizard startet auf.



Fügen Sie nun die Benutzersmartcard im freien Kartenleser ein.

(Ist die Karte bereits im Leser so entfernen Sie diese und fügen Sie sie an dieser Stelle wieder ein.)

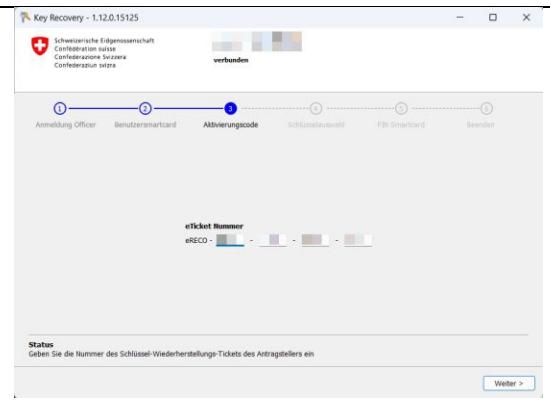


Die Benutzersmartcard wird automatisch erkannt. Klicken Sie auf «Weiter».

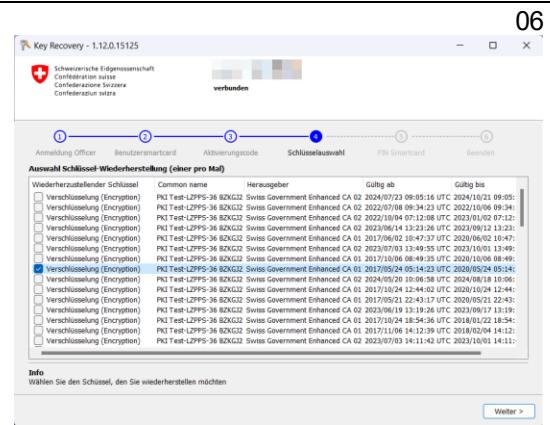


Nun muss die **eTicket-Nummer** eingegeben werden.
(Diese wurde dem Benutzer per Mail mitgeteilt.)

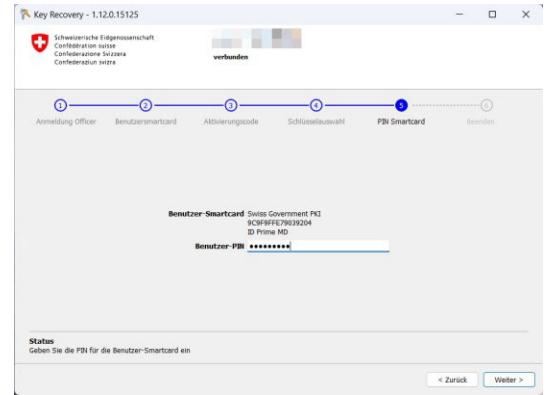
Tragen Sie die Nummer in den Feldern ein und klicken Sie auf «Weiter».



Der LRAO muss nun den gewünschten Schlüssel zur Wiederherstellung aus.



Nun muss die zertifikatsinhabende Person die PIN der Smartcard eingeben. Klicken Sie nach der Eingabe des Benutzers auf «Weiter».



Die Schlüssel werden nun auf die Karte geschrieben. Der Wizard kann mit dem «Abschliessen»-Knopf geschlossen werden.

Anmerkung:

Sollte die zertifikatsinhabende Person weitere Schlüssel benötigen, so können diese mittels des "zusätzliche Schlüssel wiederherstellen"-Knopf ebenfalls auf die Karte zurückgespielt werden. Es braucht keine weitere eReco-Ticketnummer, sofern Sie in der gleichen Session bleiben.

Haben Sie den Wizard mittels "Abschliessen" geschlossen, so muss für weitere Schlüssel der Antrag von der anfragenden Person neu gestellt werden. In diesem Fall würde die eReco-Nummer neu versendet werden.

