NICHT KLASSIFIZIERT

Key Recovery Klasse B

Prozessdefinition

V1.0, 25.05.2016

Prozess	**Key Recovery Klasse B** Wiederherstellen eines alten Encryption Keys auf die aktuelle Smartcard	**ID**	SGPKI-CLB-M13
Klassifizierung *	Nicht klassifiziert		
Status **	Freigegeben		
Autor	Daniel Stich		
Genehmigende (Eigner)	Swiss Government PKI Management Board		
Operative Verantwortung	BIT-BTR-BFS-BFO		
Doc_ID	0013-PD-SGPKI-CLB-M13.docx		
Ablageort	Trustcenter PKI		
Beschreibung	Der Zertifikatsinhaber bemerkt, dass er eine alte verschlüsselte E-Mail nicht mehr lesen kann, weil der zugehörige private Schlüssel nicht mehr auf seiner gegenwärtigen Smartcard gespeichert ist. Er ruft in seinem Browser die Anwendung ‚Key Recovery' auf und erstellt damit ein eTicket im zentralen PKI System. Sofern seine Verwaltungseinheit so aufgesetzt ist, dass für einen Key Recovery Request keine zusätzliche Autorisierung vorlegen muss, erhält er sofort die Nummer des erzeugten eTickets. Ansonsten wird das eTicket einem zuständigen KRO (Key Recovery Officer) zur Bewilligung vorgelegt. Wird der Request bewilligt, wird die eTicket-Nummer an den Zertifikatsinhaber geschickt. Mit der eTicket-Nummer und seiner Smartcard begibt sich der Zertifikatsinhaber zu seinem zuständigen LRA Officer. Nachdem er vom LRA Officer identifiziert wurde, startet dieser den Key Recovery Wizard und gibt die eTicket-Nummer ein. Der Wizard zeigt darauf alle für diesen Zertifikatsinhaber je ausgestellten Encryption Zertifikate an. Der Zertifikatsinhaber gibt dem LRA Officer diejenigen Schlüssel an, die er wiederherstellen möchte. Nach Eingabe seiner persönlichen PIN, schreibt der Wizard die gewählten Encryption Keys auf die Smartcard des Zertifikatinhabers.		
Prozessmodel	Kollaboration		
Teilnehmer	-Zertifikatsinhaber -Service Desk -Key Recovery Officer KRO -LRA Officer		
Input (Anfangszustand)	Der Schlüssel eines (abgelaufenen) Verschlüsselungszertifikats ist nicht mehr auf der Smartcard gespeichert.		
Output (Endzustand)	Der benötigte Schlüssel ist wieder auf der Smartcard nutzbar.		
Bemerkungen	Dieser Prozess gilt für Prestaged Smartcards.		

1 Detailmodell (DM)

Prozessmodell (Ablaufdefinition)

Diese Seite wurde absichtlich noch nicht erarbeitet

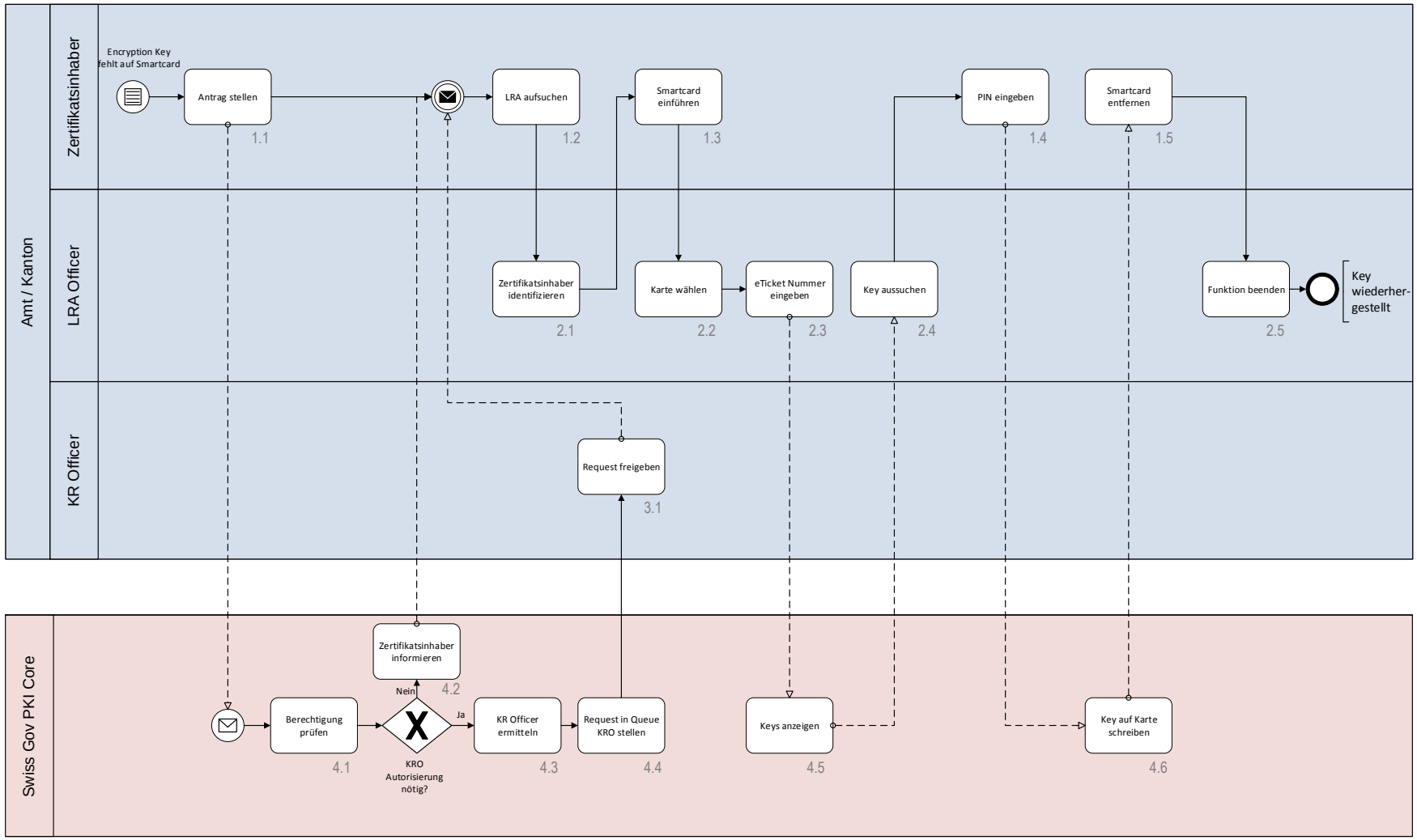
Erläuterungen

Nr.	Element	Erläuterung	Verweis, Hilfsmittel

2 Betriebsmodell (BM)

Prozessmodell (Ablaufdefinition)

SGPKI-CLB-M13: Key Recovery

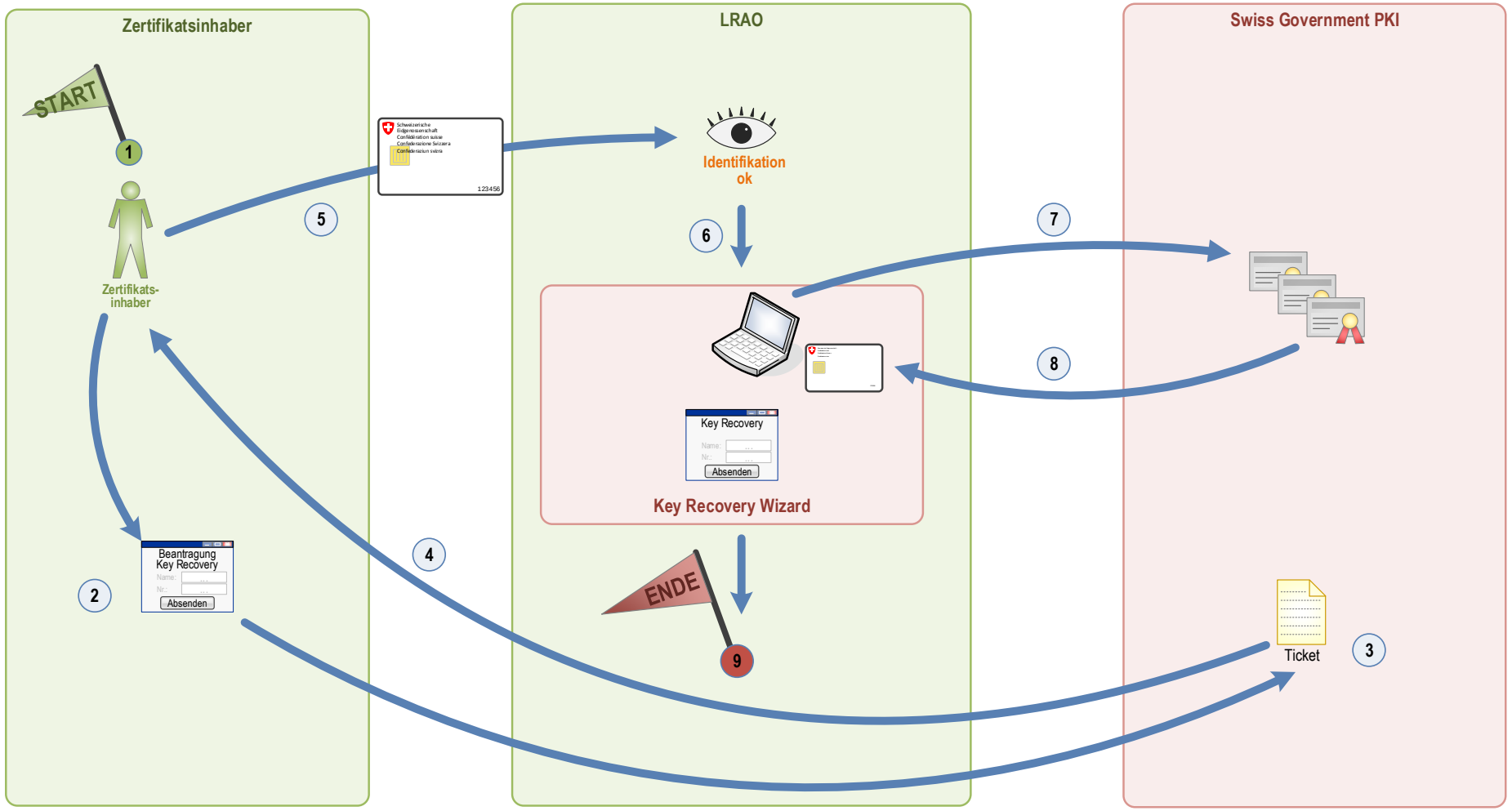


Erläuterungen

Nr.	Element	Erläuterung	Verweis, Hilfsmittel
1	1.1	Jeder Besitzer mit einer gültigen Prestaged Klasse B Smartcard kann mit dem Web-Tool ‚KeyRecoveryRequest' einen Antrag (ein eTicket) für Key Recovery eröffnen.	
2	4.1	Je nach Einstellung des Amtes kann die zusätzlich Autorisierung des Antrags durch einen Key Recovery Officer (KRO) verlangt sein.	
3	1.2	Um den Key Recovery Wizard starten zu können, wird eine spezifische Berechtigung benötigt. Diese wird in der Regel den LRA Officer zugeteilt.	
4	2.3	Die Nummer des eTickets, welches vom Zertifikatsinhaber beim Aufsetzen des Antrags erzeugt wurde.	
5	1.4	Für die Recovery-Aktion wird die gültige PIN der Karte benötigt, auf welche der Schlüssel geschrieben wird.	

3 Schaubild

Key Recovery ohne KRO (Key Recovery Officer) Funktion **ID: Zeichenblatt-1**

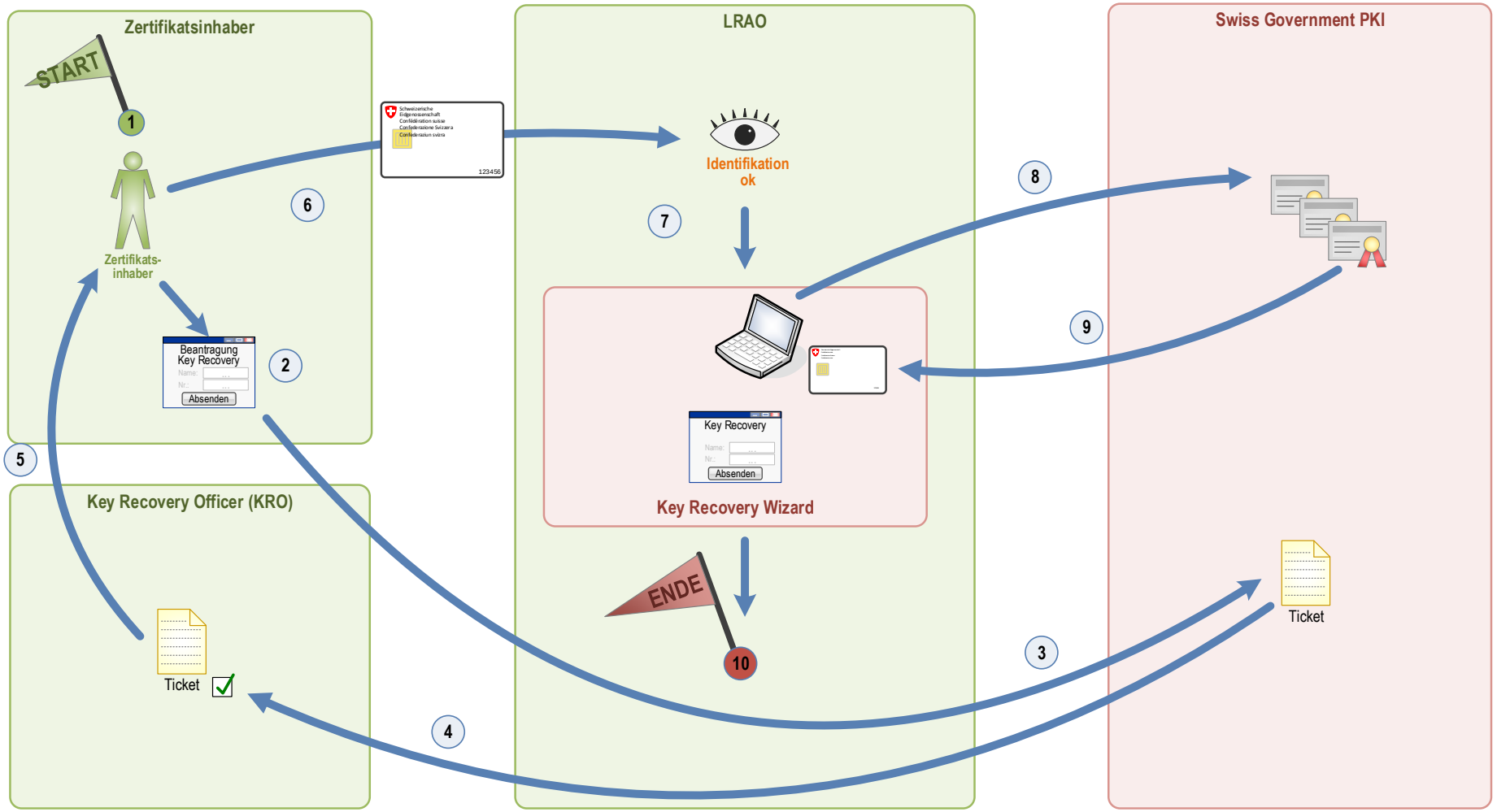


Erläuterungen

Nr.	Element	Erläuterung	Verweis, Hilfsmittel
1	1	Der Zertifikatsinhaber stellt fest, dass er eine E-Mail nicht entschlüsseln kann, weil ihn der entsprechende private Encryption Key fehlt.	
2	2,3	Mit dem Web-Tool ‚KeyRecoveryRequest' öffnet der Zertifikatsinhaber ein eTicket für Key Recovery.	
3	4	Dem Zertifikatsinhaber wird die eTicket-Nummer mitgeteilt.	
4	5	Mit der eTicket-Nummer sucht der Zertifikatsinhaber seinen zuständigen LRA Officer auf.	
5	6	Der LRA Officer startet den Recovery Wizard und wählt mit dem Zertifikatinhaber die wiederherzustellenden Schlüssel aus. Diese werden vom Wizard auf die Smartcard geschrieben.	

Key Recovery mit KRO (Key Recovery Officer) Funktion

ID: **Zeichenblatt-1**



Erläuterungen

Nr.	Element	Erläuterung	Verweis, Hilfsmittel
1	1	Der Zertifikatsinhaber stellt fest, dass er eine E-Mail nicht entschlüsseln kann, weil ihn der entsprechende private Encryption Key fehlt.	
2	2,3	Mit dem Web-Tool ‚KeyRecoveryRequest' öffnet der Zertifikatsinhaber ein eTicket für Key Recovery.	
3	4	Der KRO (Key Recovery Officer) erhält vom System die Aufforderung, den Key Recovery Request zu bewilligen	
4	5	Nach der Bewilligung des Requests durch den KRO wird dem Zertifikatsinhaber die eTicket-Nummer mitgeteilt.	
5	6	Mit der eTicket-Nummer sucht der Zertifikatsinhaber seinen zuständigen LRA Officer auf.	
6	7, 8 , 9	Der LRA Officer startet den Recovery Wizard und wählt mit dem Zertifikatinhaber die wiederherzustellenden Schlüssel aus. Diese werden vom Wizard auf die Smartcard geschrieben.	