NICHT KLASSIFIZIERT

PIN Reset Klasse B

Prozessdefinition

V1.1, 10.01.2022

Prozess	**PIN Reset Klasse B** Eine nach mehr als 4 fehlerhaften PIN-Eingaben gesperrte Smartcard wird kontrolliert entsperrt und mit einem neuen PIN versehen.	**ID**	SGPKI-CLB-M12
Klassifizierung *	Nicht klassifiziert		
Status **	Freigegeben		
Autor	Daniel Stich / Gabrielle Lyoth		
Genehmigende (Eigner)	Swiss Government PKI Management Board		
Operative Verantwortung	BIT-BTR/BFS/BFO		
Doc_ID	0012-PD-SGPKI-CLB-M12_DE_2022-01-10.docx		
Ablageort	Certified PKI		
Beschreibung	Nach der viermaligen Fehleingabe der Benutzer-PIN ist die Smartcard für Klasse B Zertifikate gesperrt. In einem ersten Schritt meldet sich der Zertifikatsinhaber bei seinem Service Desk. Der Service Desk Mitarbeiter plausibilisiert den Anrufer mit Hilfe der hinterlegten ‚Magic Questions'. Ist die Plausibilisierung zufriedenstellend, eröffnet der Service Desk Mitarbeiter ein Ticket in der WEB-Anwendung der Swiss Government PKI. Die gesperrte Smartcard kann entweder über die Seriennummer oder den Namen des Zertifikatsinhabers gesucht werden. Nach Eröffnung des PIN-Reset Tickets muss sich dann der Zertifikatsinhaber zu einer Arbeitsstation mit zwei Kartenlesern begeben. An diesem Arbeitsplatz muss ein Benutzer angemeldet sein, der als PRU (PIN Reset User) agieren kann. Dazu startet er den PIN-Reset Wizard und meldet sich mit seinem gültigen Klasse B an. Danach steckt der Zertifikatsinhaber seine gesperrte Karte in den freien Leser. Der PIN-Wizard liest die Seriennummer der Karte und sucht im zentralen PKI-System nach einem Ticket zu dieser Sequenznummer. Als nächster Schritt muss der PRU den Zertifikatsinhaber eindeutig identifizieren. D.h. der PRU kennt entweder den Zertifikatsinhaber persönlich oder er identifiziert ihn mittels eines gültigen Ausweises. Der PRU muss die erfolgreiche Identifikation im Wizard bestätigen. Der Wizard erhält dann von den zentralen PKI-Komponenten eine verschlüsselte Version des Karten-PUK und der Zertifikatsinhaber wird aufgefordert, zwei Mal seinen neuen PIN einzugeben. Mit dieser Information und dem PUK führt der Wizard dann einen PIN-Reset auf der Karte durch. Die Smartcard ist nun entsperrt und einsatzbereit. Sie kann vom Leser entfernt werden. Bei der ganzen Transaktion wird auf einem Log festgehalten, welche Karte durch welchen PRU zum PIN-Reset freigegeben wurde.		
Prozessmodel	Kollaboration		
Teilnehmer	- Zertifikatsinhaber - Service Desk - PIN Reset User		
Input (Anfangszustand)	Die Smartcard des Zertifikatsinhabers ist gesperrt, nachdem die PIN mehr als fünf Mal inkorrekt eingegeben wurde und kann somit nicht mehr verwendet, bis sie wieder entsperrt ist.		
Output (Endzustand)	Die Smartcard ist entsperrt und mit einem neuen PIN versehen. Die Karte ist wieder einsatzfähig und die Zertifikate auf der Karte durch den Inhaber nutzbar.		
Bemerkungen	Dieser Prozess gilt für Prestaged Smartcards.		

1 Detailmodell (DM)

Prozessmodell (Ablaufdefinition)

Diese Seite wurde absichtlich noch nicht erarbeitet

Erläuterungen

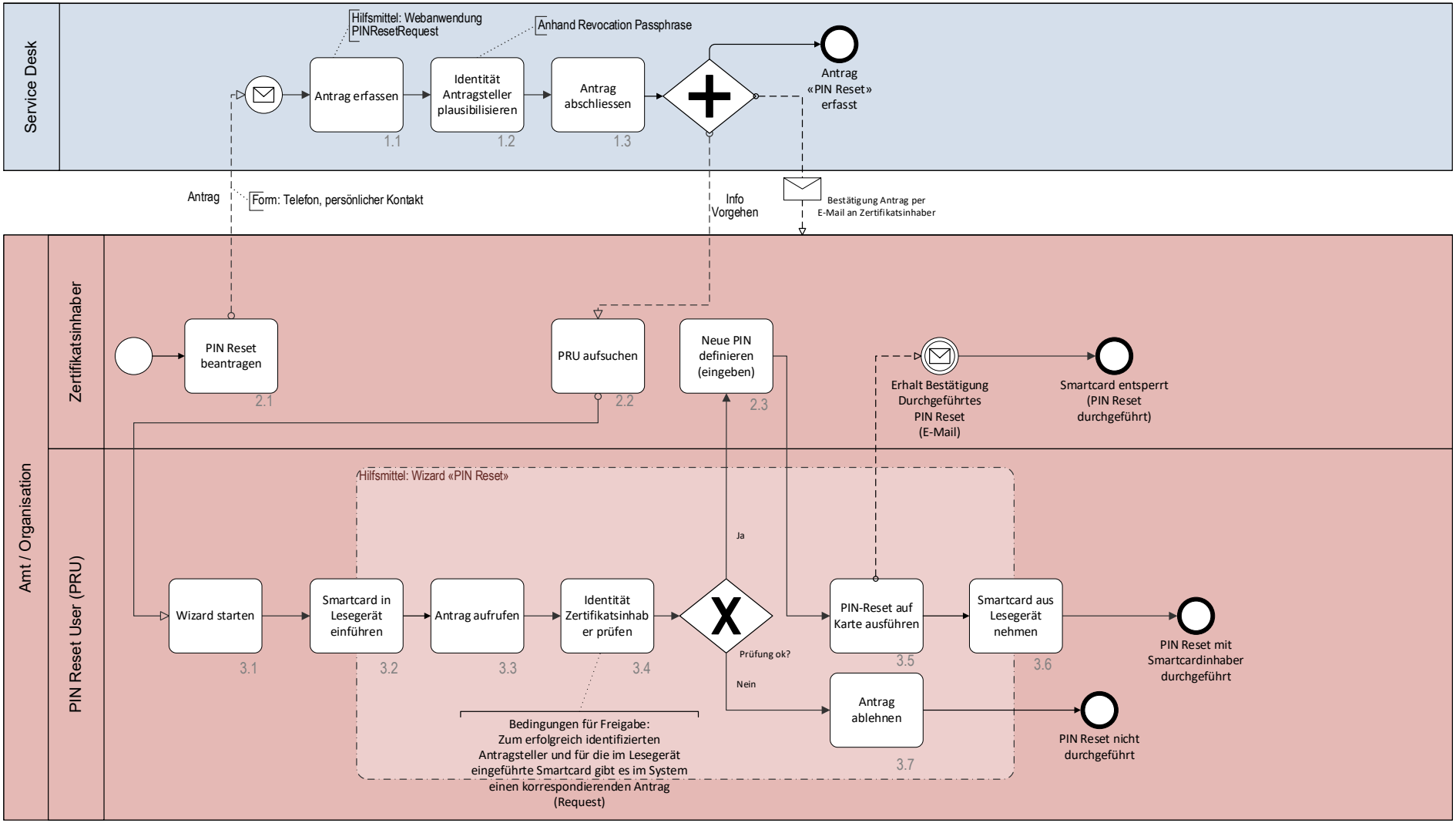
Nr.	Element	Erläuterung	Verweis, Hilfsmittel

2 Betriebsmodell (BM)

Prozessmodell (Ablaufdefinition)

SGPKI-CLB-M12: PIN Reset

Kategorie: Betriebsmodell
Blatt: 1 / 1

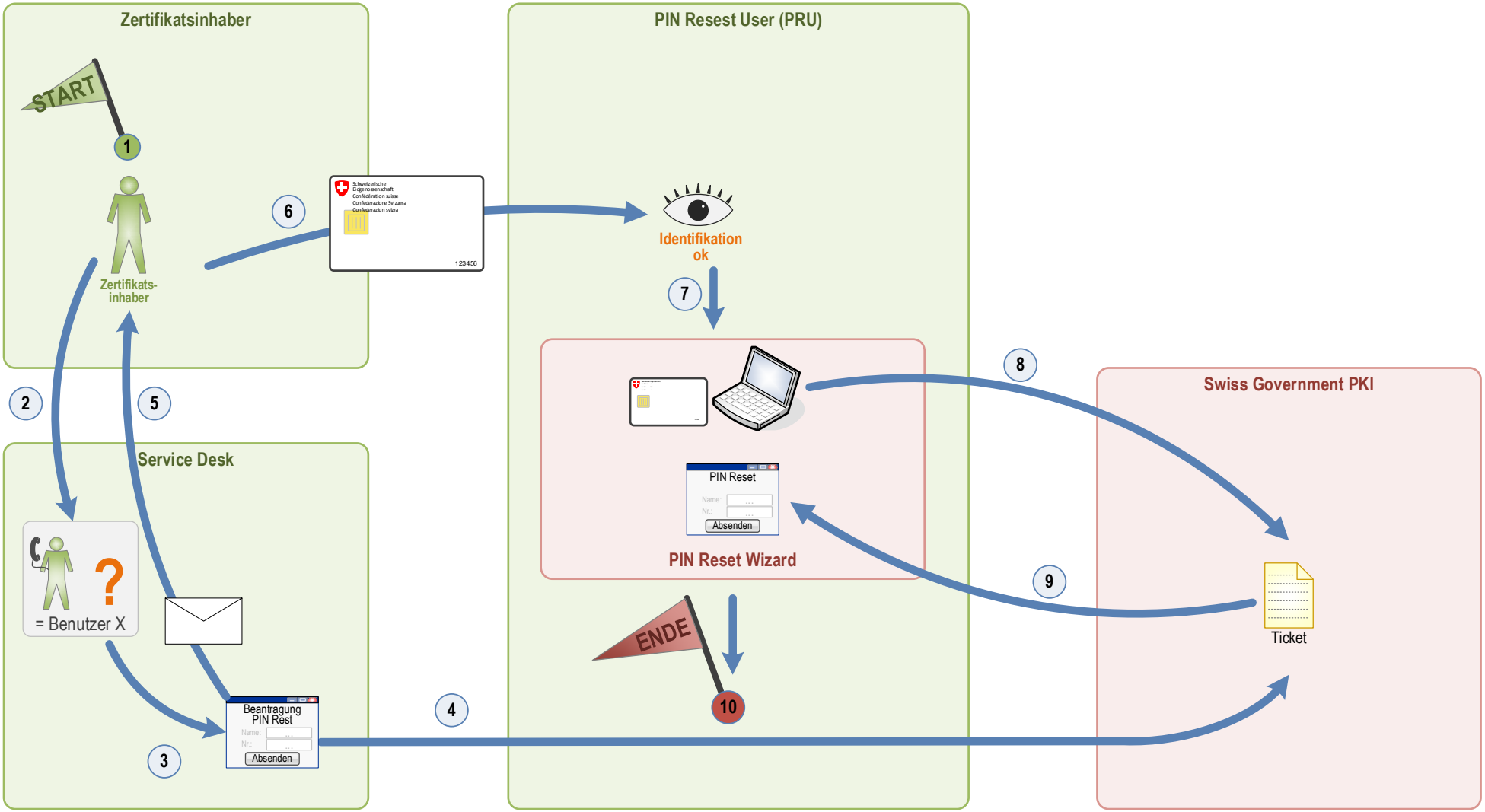


Erläuterungen

Nr.	Element	Erläuterung	Verweis, Hilfsmittel
1	1.1	Für den Antrag kann die gesperrte Karte entweder über die Seriennummer oder den Namen des Zertifikatsinhabers gesucht werden	
2	1.2	Die Plausibilisierung des Antragstellers durch das Service Desk geschieht durch die Abfrage der Revocation Passphrase	
3	2.2	Der PRU muss im Besitz eines gültigen Klasse B Zertifikats sein und an seiner Arbeitsstation einen zweiten Kartenleser zur Verfügung haben	
4	3.1	Anmeldung PRU mit seinem Klasse B Zertifikat	
5	3.3	Der Wizard sucht den Antrag selbstständig mit der Seriennummer der eingeführten Smartcard	
6	3.4	Die Identifizierung muss durch den PRU explizit bestätigt werden und wird mit den Informationen über die beteiligten Personen in das Reset-Log geschrieben	

3 Schaubild

PIN Reset **ID: Zeichenblatt-1**



Erläuterungen

Nr.	Element	Erläuterung	Verweis, Hilfsmittel
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 Zertifikatsinhabers anhand der hinterlegten persönlichen ‚Revocation Passphrase'	
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. Gleichzeitig erhält der Zertifikatsinhaber vom PKI-System eine E-Mail mit den Details des Antrags. Im Regelfall kann der Zertifikatsinhaber diese E-Mail erst lesen, nachdem der Prozess abgeschlossen wurde. Falls jedoch für ihn irrtümlicherweise ein PIN-Reset-Antrag gestellt wurde, kann der Zertifikatsinhaber sofort beim Service Desk intervenieren.	
6	6	Der Zertifikatsinhaber begibt sich mit der gesperrten Smartcard zum PIN Reset User	Jeder Benutzer mit einem gültigen Klasse B Zertifikat kann als PRU agieren. Weitere Voraussetzung ist der Zugang zu einer Arbeitsplatzstation mit einem zweiten Kartenleser.
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 entsperrt die Karte mit dem PUK und setzt gleichzeitig den neuen PIN.	
10	10	Die Karte ist entsperrt und wieder einsatzbereit.	