NON CLASSIFICATO

Key recovery per certificati di classe B

Definizione del processo

V1.1, 05.12.2016

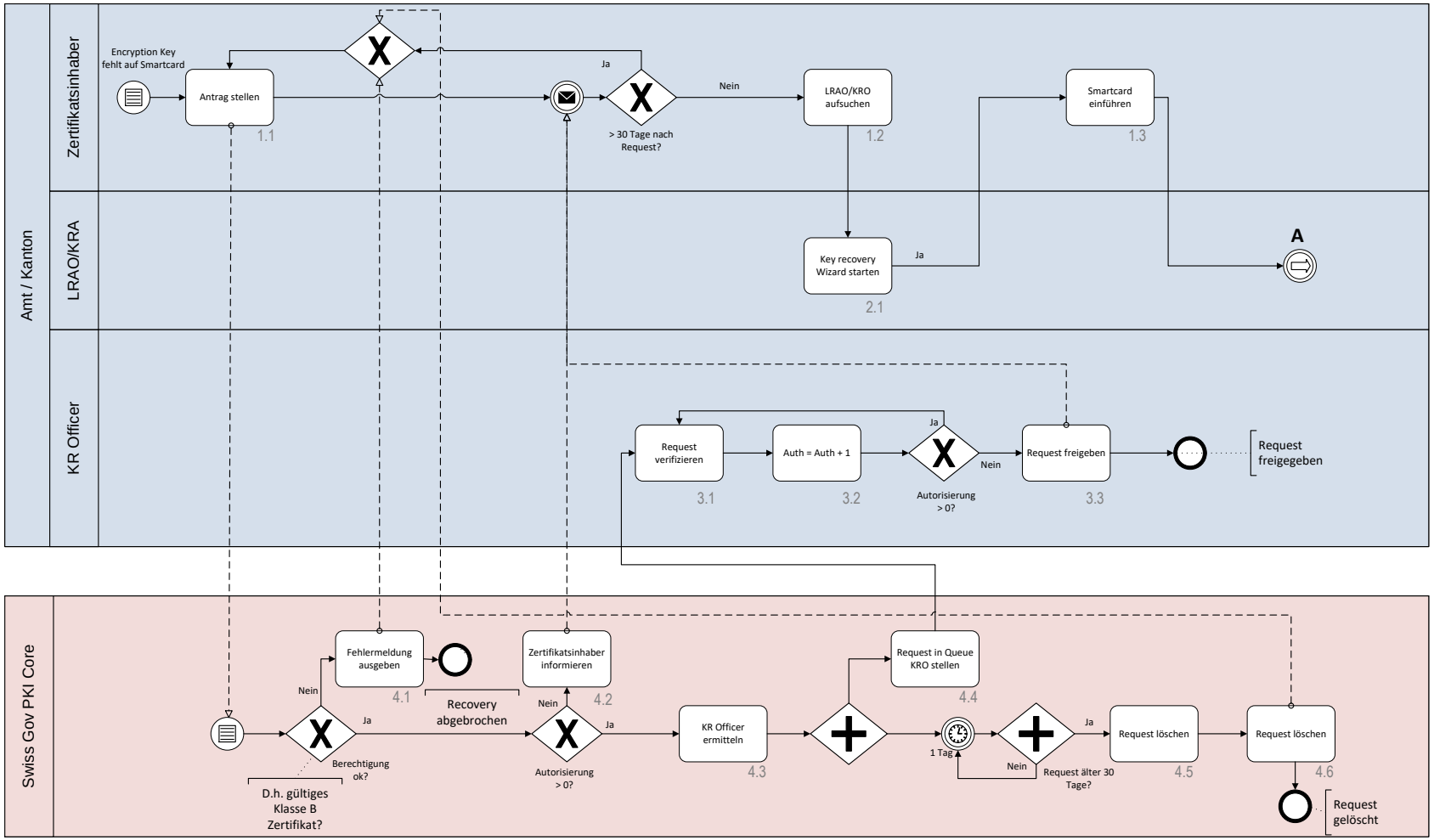
Processo	**Key recovery per certificati di classe B** Ripristino di una vecchia encrypion key sulla smart card attuale	**ID**	SGPKI-CLB-M13
Classificazione *	Non classificato		
Stato **	Approvato		
Autore	Daniel Stich		
Persona che rilascia l'autorizzazione (responsabile)	Swiss Government PKI Management Board		
Responsabilità operativa	BIT-BTR-BFS-BFO		
Doc_ID	0013-PD-SGPKI-CLB-M13.docx		
Luogo di archiviazione	Trustcenter PKI		
Descrizione	Il titolare dei certificati rileva di non essere più in grado di leggere una vecchia e-mail crittografata perché la relativa chiave privata non è più salvata sulla sua smart card attuale. Il titolare richiama l'applicazione di key recovery nel proprio browser, con la quale genera un ticket elettronico nel sistema PKI centrale. Se la sua unità amministrativa non richiede un'ulteriore autorizzazione per una key recovery request, riceve immediatamente il numero del ticket elettronico generato. In caso contrario, il ticket elettronico viene sottoposto al Key Recovery Officer (KRO) competente per l'autorizzazione. Se la richiesta viene autorizzata, il numero del ticket elettronico viene inviato al titolare dei certificati. Con il numero del ticket elettronico e la sua smart card il titolare dei certificati si reca dal suo Local Registration Authority Officer (LRAO) competente o dal Key Recovery Agent (KRA). Il ruolo del KRA è compreso nell'autorizzazione di LRAO. Inoltre, anche i RIO possono richiedere questo ruolo presso l'Order Management SG-PKI utilizzando un apposito modulo. Dopo che il titolare dei certificati ha consegnato il suo ticket al LRAO/KRA, quest'ultimo lancia il key recovery wizard e inserisce il numero del ticket elettronico. Il wizard visualizza quindi tutti gli encryption certificate rilasciati per questo titolare di certificati. Il titolare dei certificati fornisce al LRAO/KRA la chiave che desidera ripristinare. Dopo l'immissione del PIN personale il wizard scrive le encryption key desiderate sulla smart card del titolare dei certificati.		
Modello di processo	Collaborazione		
Partecipanti	- Titolare dei certificati - Service desk - Key Recovery Agent (KRA) - Key Recovery Officer (KRO) - Local Registration Authority Officer (LRAO)		
Input (situazione iniziale)	La chiave di un certificato di crittografia (scaduto) non è più salvata sulla smart card.		
Output (situazione finale)	La chiave necessaria è nuovamente utilizzabile sulla smart card.		
Osservazioni	Questo processo è valido per le prestaged e per le non-prestaged smart card.		

1 Modello di dettaglio (MD)

Modello di processo (definizione del processo)

SGPKI-CLB-M13: Key Recovery

Kategorie: Detailmodell
Blatt: 1 / 2

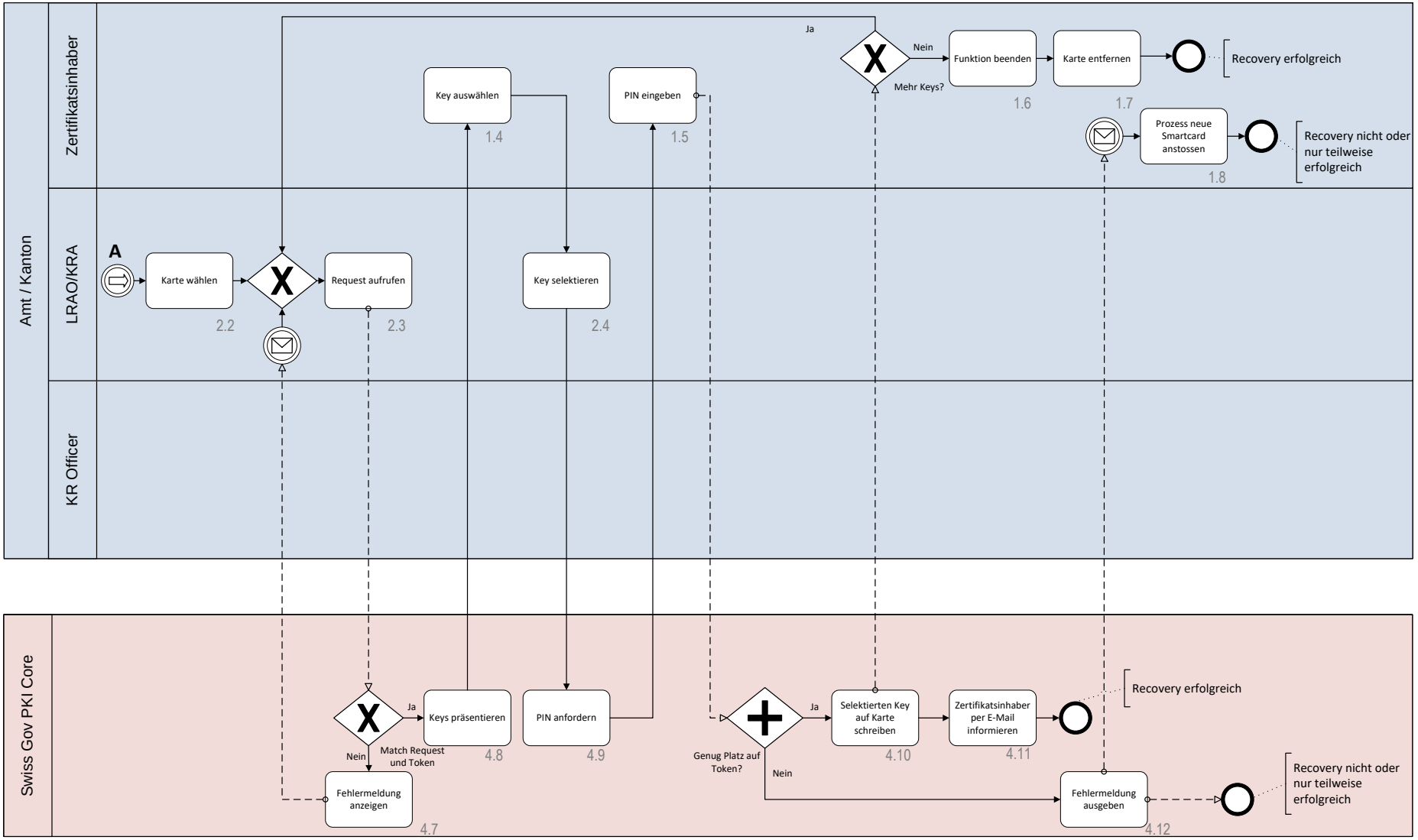


Descrizione

N.	Elemento	Descrizione	Rinvio, mezzi ausiliari
1	1.1	Ogni possessore di una smart card valida di classe B può aprire una richiesta (un ticket elettronico) di key recovery con il web tool KeyRecoveryRequest.	
2	4.2	Dopo la verifica della validità dei certificati di classe B e a condizione che non sia necessaria un'ulteriore autorizzazione, l'utente riceve il numero del ticket elettronico per la key recovery.	
3	3.1., 3.2	A seconda della configurazione dell'ufficio la richiesta deve essere autorizzata da 1-n KRO (Key Recovery Officer).	
4	3.3	Se tutti i livelli di autorizzazione sono stati superati con successo, l'utente riceve il numero del ticket elettronico per la key recovery	
5	4.5, 4.6	Se una richiesta già stilata non viene richiamata entro 30 giorni, il sistema la cancella automaticamente.	
6	2.1	Per avviare il key recovery wizard è necessaria la smart card di un LRAO con certificati LRAO. Può trattarsi della smart card di un LRAO pienamente autorizzato o di un KRA dotato di un'autorizzazione apposita. L'autorizzazione (e la relativa smart card LRAO) del KRA è limitata all'esecuzione del key recovery wizard e deve essere richiesta all'Order Management con un modulo firmato dall'ufficio.	

SGPKI-CLB-M13: Key Recovery

Kategorie: Detailmodell
Blatt: 2 / 2



Descrizione

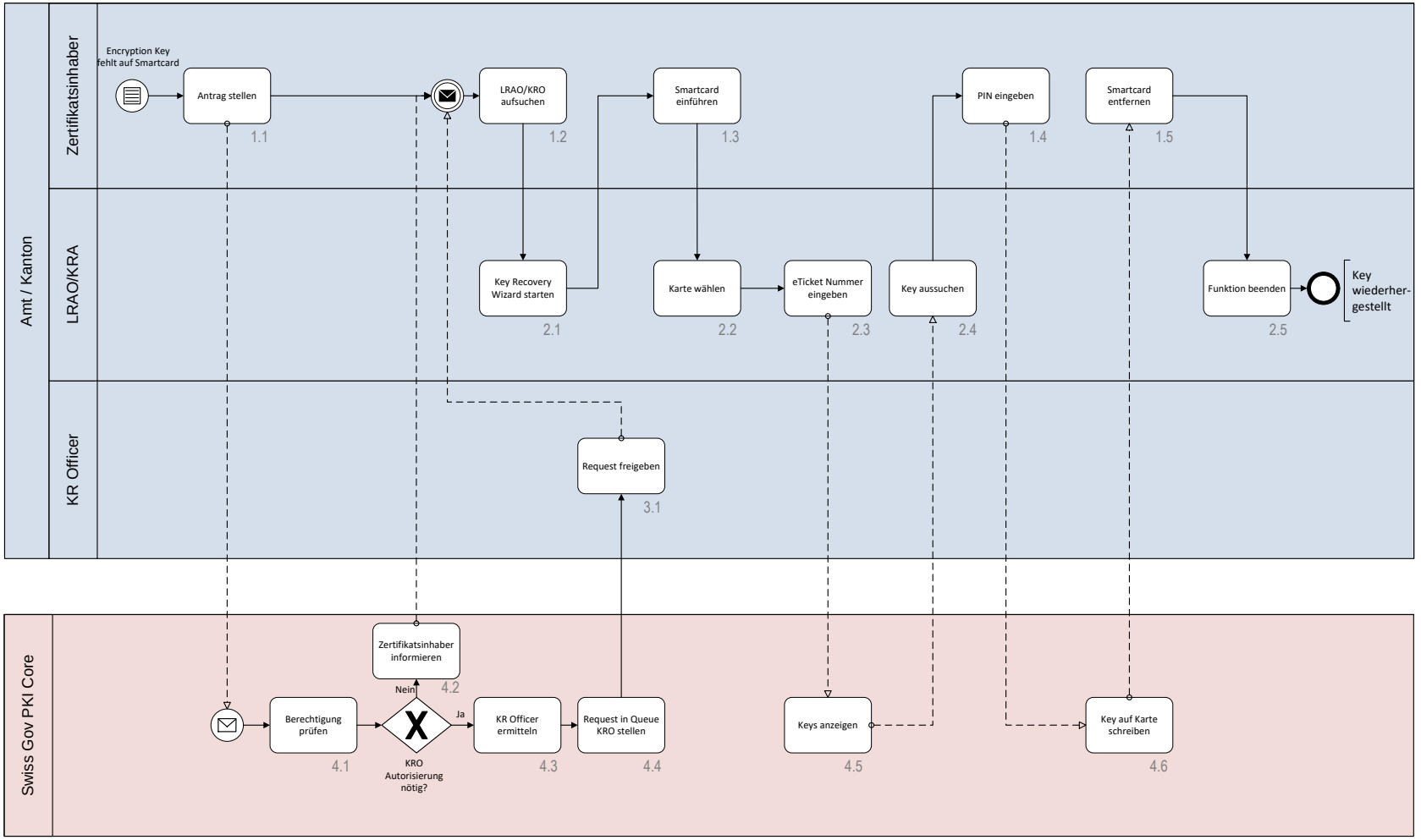
N.	Elemento	Descrizione	Rinvio, mezzi ausiliari
1	2.2	Occorre dapprima selezionare la scheda inserita.	
2	2.3	La richiesta viene richiamata in background con il numero del ticket elettronico.	
3	4.8	Il background verifica il numero di serie della scheda, cerca il ticket elettronico indicato e confronta i dati del ticket con quelli della scheda inserita. Se la scheda coincide con i dati contenuti nel ticket, vengono visualizzate tutte le encryption key memorizzate per questo utente in KAS:	
4	1.4, 2.4	L'utente sceglie la chiave desiderata in collaborazione con il LRAO/KRA.	
5	1.5	Affinché la smart card risulti scrivibile, l'utente deve inserire il proprio PIN.	
6	4.10	Se sulla scheda è disponibile spazio di memoria sufficiente, la private key specificata viene registrata sulla scheda.	
7	1.6	Qualora occorra riscrivere ulteriori chiavi, il wizard torna all'inizio del processo di elaborazione della richiesta. In caso contrario il wizard viene concluso.	

2 Modello operativo (MO)

Modello di processo (definizione del processo)

SGPKI-CLB-M13: Key Recovery

Kategorie: Betriebsmodell
Blatt: 1 / 1

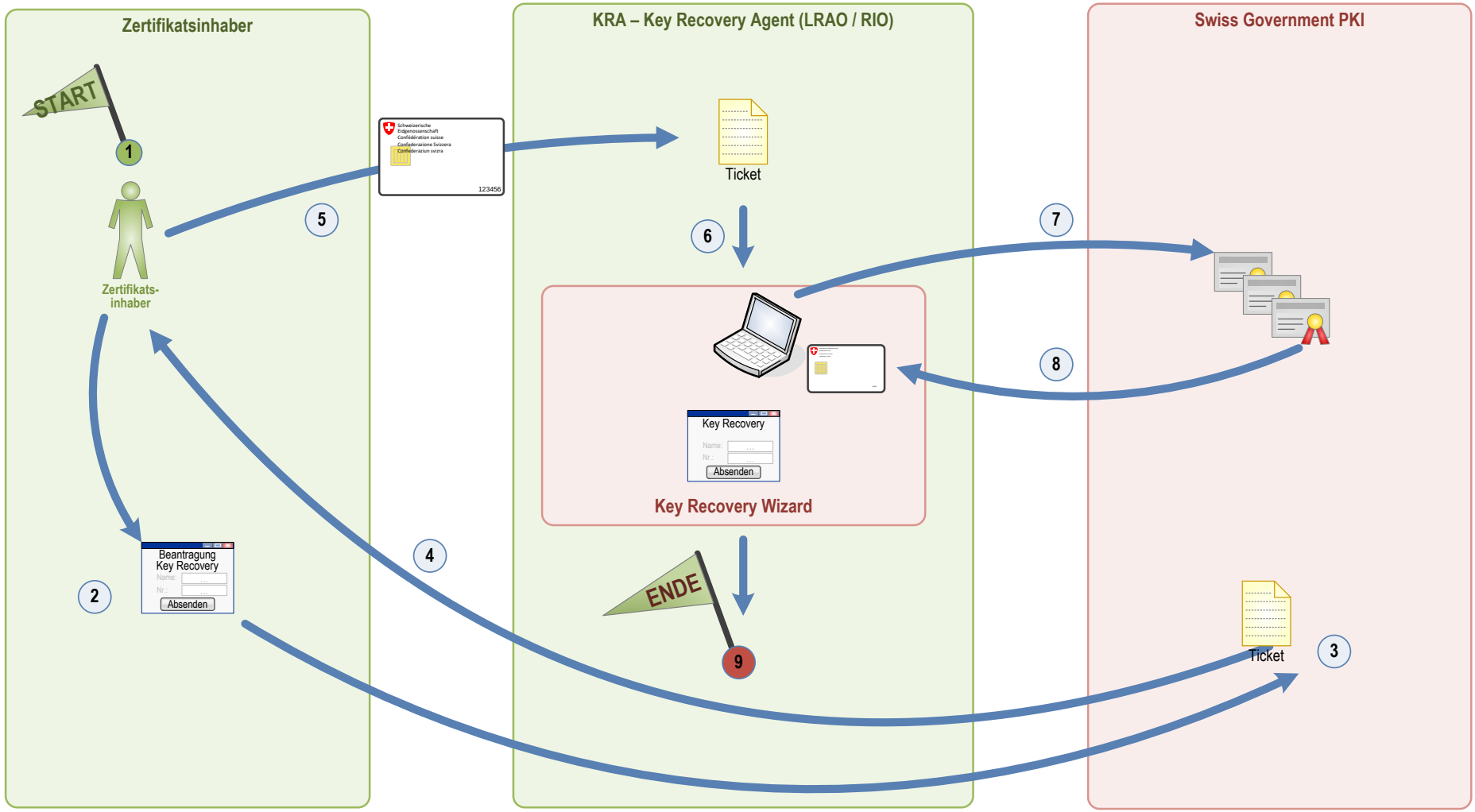


Descrizione

N.	Elemento	Descrizione	Rinvio, mezzi ausiliari
1	1.1	Ogni possessore di una smart card valida di classe B può aprire una richiesta (un ticket elettronico) per la key recovery utilizzando il web tool KeyRecoveryRequest.	
2	4.1	A seconda della configurazione dell'ufficio l'ulteriore autorizzazione della richiesta deve essere disposta da un KRO.	
3	2.1	Per poter avviare il key recovery wizard è necessaria un'autorizzazione di un LRAO o di un KRA.	
4	2.3	Il numero del ticket elettronico generato dal titolare dei certificati durante la stesura della richiesta.	
5	1.4	Per l'operazione di recovery è necessario il PIN valido della scheda sulla quale viene scritta la chiave.	

3 Schema illustrativo

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

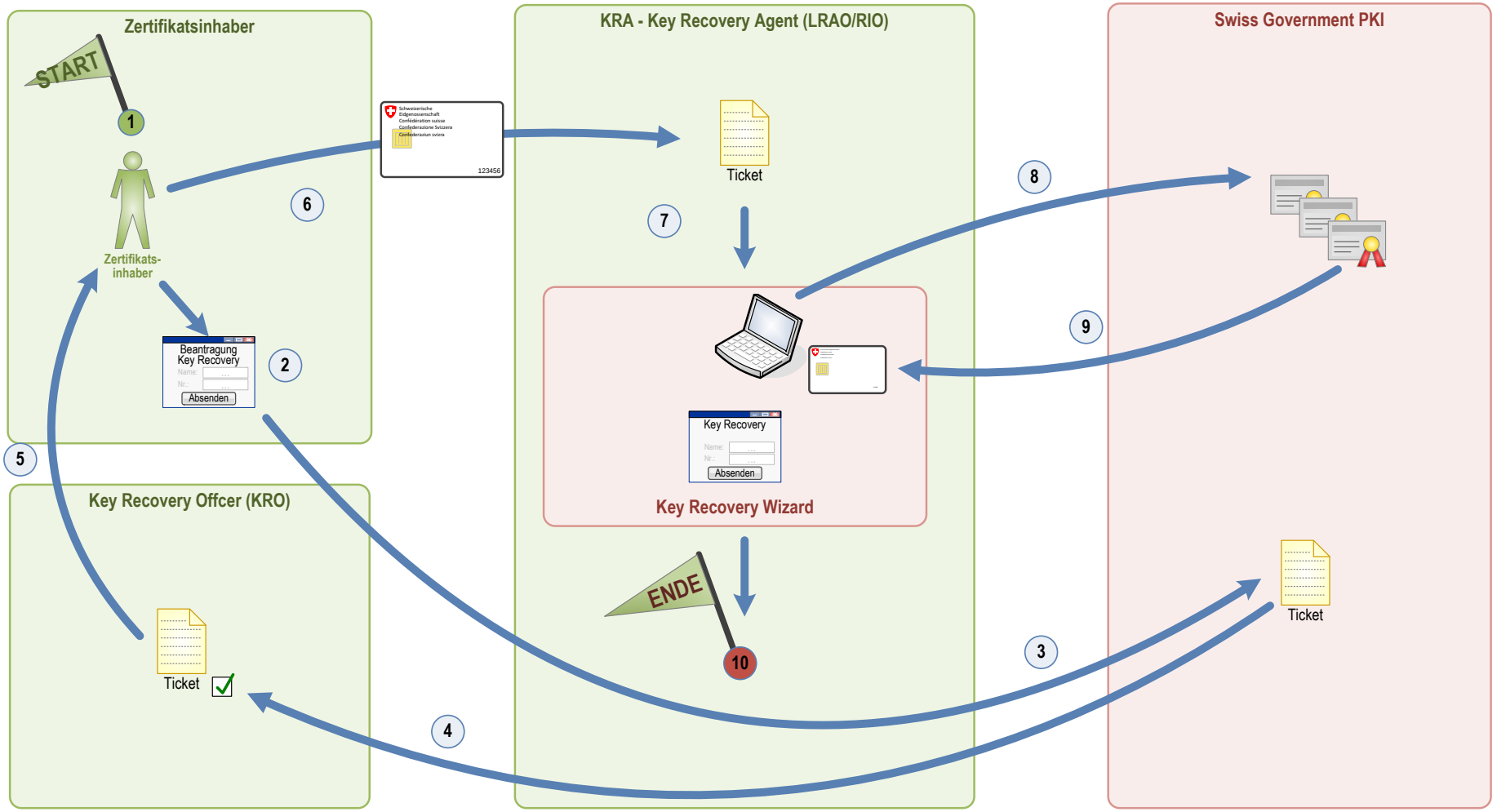


Descrizione

N.	Elemento	Descrizione	Rinvio, mezzi ausiliari
1	1	Il titolare dei certificati rileva di non essere in grado di decodificare un'e-mail perché non dispone della relativa encryption key o perché gli è stata rilasciata una nuova smart card.	
2	2,3	Con il web tool KeyRecoveryRequest il titolare dei certificati apre un ticket elettronico per la key recovery.	
3	4	Al titolare dei certificati viene comunicato il numero del ticket elettronico.	
4	5	Con il numero del ticket elettronico il titolare dei certificati si rivolge al suo LRAO o al suo KRA competente.	
5	6	Il LRO/KRA lancia il recovery wizard e seleziona con il titolare dei certificati le chiavi da ripristinare. Queste vengono scritte sulla smart card dal wizard.	

Key Recovery mit KRO (Key Recovery Officer) Funktion

ID: Zeichenblatt-1



Descrizione

N.	Elemento	Descrizione	Rinvio, mezzi ausiliari
1	1	Il titolare dei certificati rileva di non essere in grado di decodificare un'e-mail perché non dispone della relativa encryption key o perché gli è stata rilasciata una nuova smart card.	
2	2,3	Con il web tool KeyRecoveryRequest il titolare dei certificati apre un ticket elettronico per la key recovery.	
3	4	Il KRO riceve dal sistema l'invito ad autorizzare la key recovery request.	
4	5	Dopo l'autorizzazione della richiesta da parte del KRO al titolare dei certificati viene comunicato il numero del ticket elettronico.	
5	6	Con il numero del ticket elettronico il titolare dei certificati si rivolge al suo LRAO o al suo KRA competente.	
6	7, 8, 9	Il LRAO/KRA lancia il recovery wizard e seleziona con il titolare dei certificati le chiavi da ripristinare. Queste vengono scritte sulla smart card dal wizard.	