NON CLASSIFICATO

Unseal delle smart card per certificati di classe B

Definizione del processo

V1.2, 11.08.2016

Processo	**Unseal delle smart card per certificati di classe B** Wizard finalizzato a rendere operativa una smart card	**ID**	SGPKI-CLB_M00.02
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	0053-PD-SGPKI-CLB-M00.02		
Luogo di archiviazione	Trustcenter PKI		
Descrizione	Dopo aver ricevuto, nell'ambito del processo eseguito dal Registration Identification Officer (RIO) o del rilascio sincrono presso una CMC (Certificate Management Console), sia la propria prestaged smart card personale sia l'unseal document, il destinatario dei certificati può rimuovere il sealing della propria smart card. A questo scopo deve recarsi a una postazione di lavoro dotata di due lettori di schede nella quale un utente ha già effettuato il login. Dopo l'avvio dell'unseal wizard, che non necessita di una particolare autorizzazione, la smart card da cui deve essere rimosso il sealing viene inserita nel secondo lettore. Dopo l'immissione del numero del ticket elettronico riportato nell'unseal document, il wizard cerca i dati della scheda e dei certificati nel sistema centrale. Il destinatario dei certificati viene invitato a inserire il proprio PIN personale e la passphrase di revoca (domanda e risposta). A questo punto il wizard carica i certificati sulla scheda, la passphrase di revoca è salvata centralmente e la smart card è protetta dal PIN personale del destinatario dei certificati. La scheda è ora attiva e pienamente operativa.		
Modello di processo	Collaborazione		
Partecipanti	- Destinatario dei certificati - Postazione di lavoro di utente		
Input (situazione iniziale)	Il destinatario dei certificati è in possesso di una prestaged smart card. La scheda è ancora bloccata. I relativi certificati sono stati generati preliminarmente con il walk-in wizard o la CMC (Certificate Management Console). Il destinatario dei certificati è in possesso del relativo numero del ticket elettronico.		
Output (situazione finale)	La scheda è sbloccata, contiene i certificati di classe B validi ed è protetta dal PIN personale del destinatario dei certificati.		
Osservazioni	Questo processo è valido per tutte le smart card registrate centralmente (prestaged e non-prestaged) preparate con il register smart card wizard.		

Controllo delle modifiche, verifica, autorizzazione

Versione	Data	Descrizione, osservazione	Nome o ruolo
V0.1	19.05.2016	Versione in corso di verifica	Daniel Stich
V0.2	25.05.2016	Adeguamenti in base al feedback	Daniel Stich
V1.0	26.05.2016	1ª versione principale autorizzata	Daniel Stich
V1.1	11.08.2016	Adeguamento al handling delle non-prestaged smart card con propria gestione dei PUK nel processo RIO	Daniel Stich
V1.2	15.09.2016	Descrizione di dettaglio dello svolgimento	

Referenze

Segno di riconoscimento	Titolo, fonte
[1]	**Registrazione di non-prestaged smart card** **Definizione del processo** Versione 0.2 del 05.08.2016 Fonte: Swiss Government PKI
[2]	**Processo di rilascio dei certificati di classe B tramite RIO** **Definizione del processo** Versione 1.0 del 25.05.2016 Fonte: Swiss Government PKI

1 Modello di dettaglio (MD)

Modello di processo (definizione del processo)

Questa pagina non è ancora stata volutamente elaborata.

Descrizione

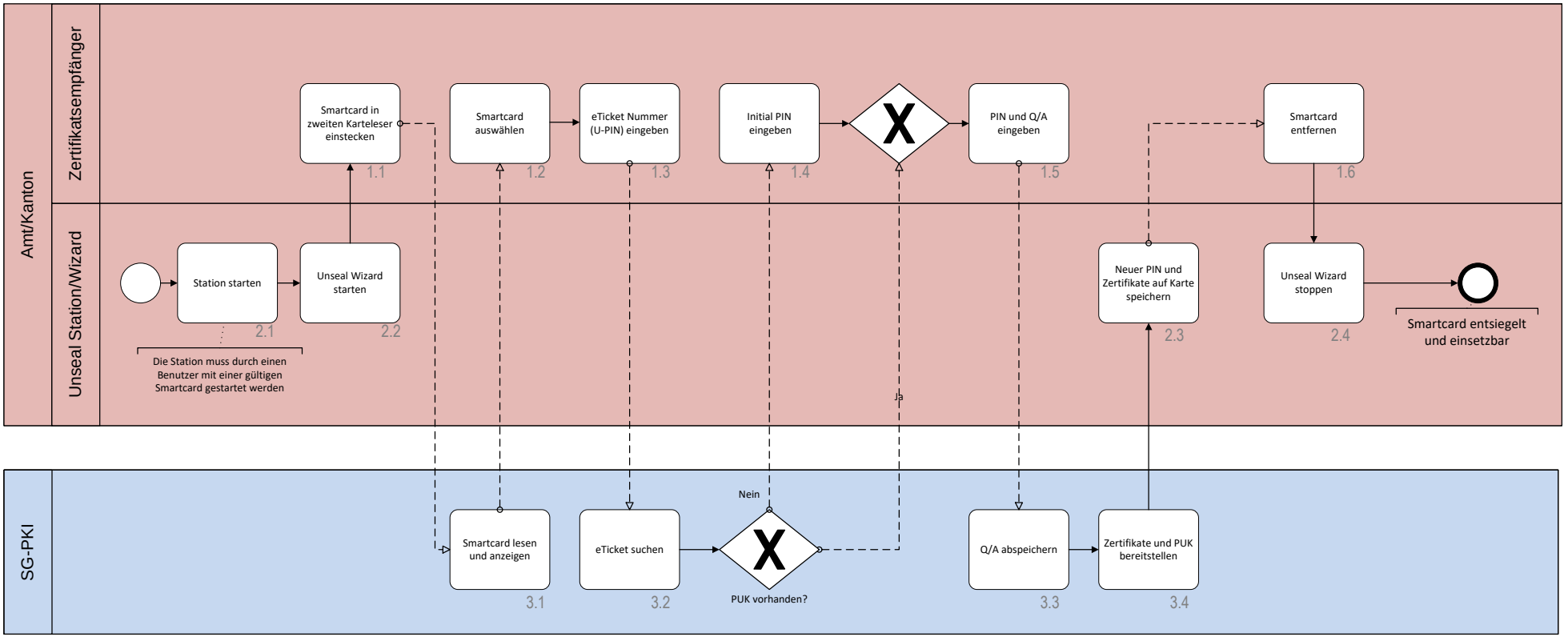
N.	Elemento	Descrizione	Rinvio, mezzi ausiliari

2 Modello operativo (MO)

Modello di processo (definizione del processo)

SGPKI-CLB-M00.02: Smartcard entsiegeln

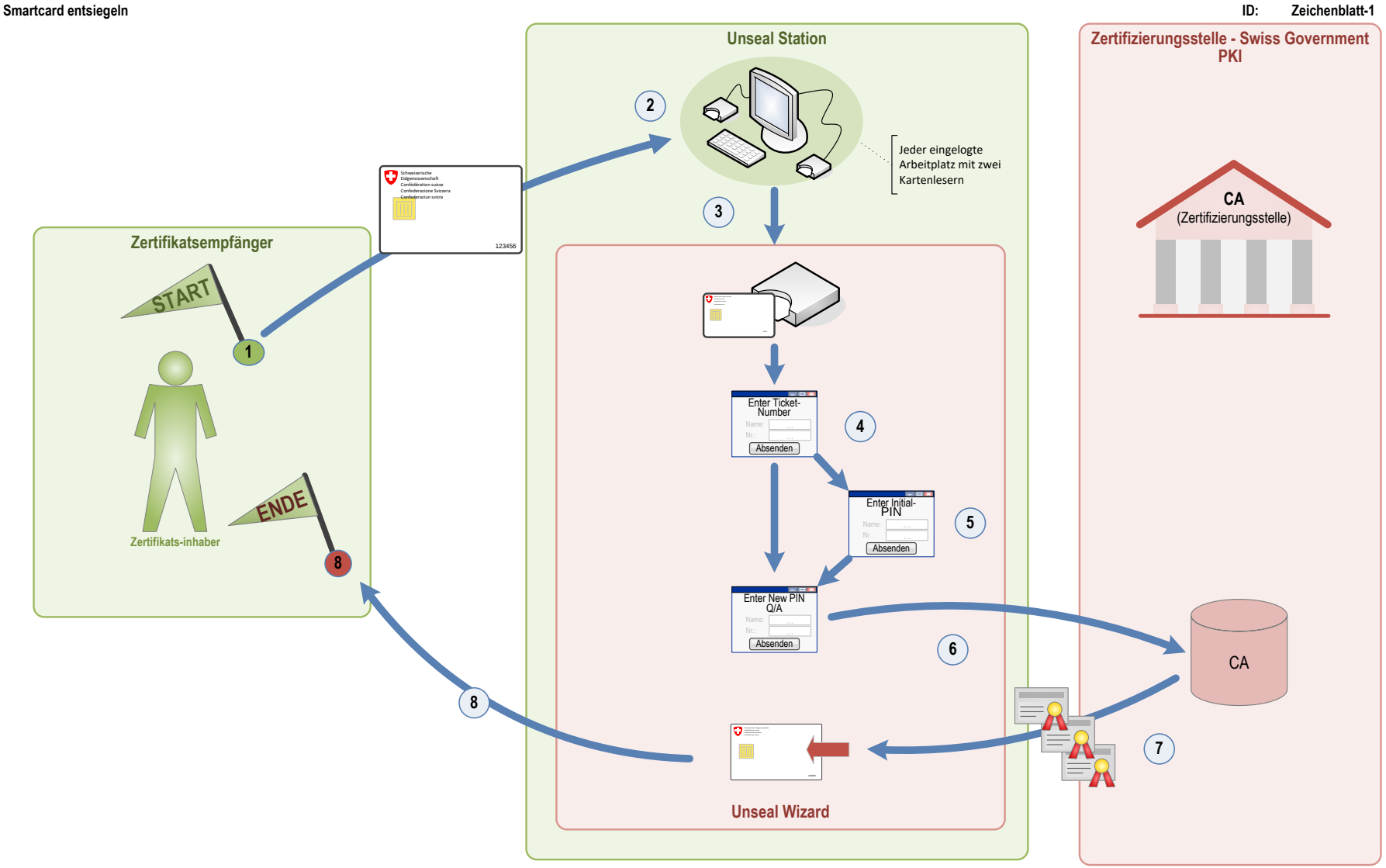
Kategorie: Betriebsmodell
Blatt: 1 / 1



Descrizione

N.	Elemento	Descrizione	Rinvio, mezzi ausiliari
1	2.1	L'unseal wizard può essere avviato senza un'apposita autorizzazione.	
2	1.1	La smart card da cui deve essere rimosso il sealing può essere introdotta nel secondo lettore di schede solo quando il wizard è stato avviato.	
3	1.3	Il numero del ticket elettronico è contenuto nell'unseal document che il destinatario dei certificati ha ricevuto dall'ufficiale LRA o dal RO.	
4	1.4	In caso di smart card con un proprio sistema di gestione dei PUK, il PUK non è noto al backend. Per questo motivo la scheda deve essere aperta con il PIN iniziale per il wizard.	
5	1.5	Il destinatario dei certificati specifica il suo PIN personale e la sua passphrase di revoca (domanda e risposta).	
6	2.3	Il wizard scrive i certificati sulla smart card e li protegge con il PIN personale del destinatario dei certificati.	

3 Schema illustrativo



Descrizione

N.	Elemento	Descrizione	Rinvio, mezzi ausiliari
1	1	Il presupposto è che il destinatario dei certificati possieda una prestaged smart card a lui assegnata e l'unseal document corrispondente.	
2	2	Occorre aver effettuato il login nella postazione di lavoro, che deve essere inoltre provvista di un secondo lettore di schede.	
3	4	È necessario specificare il numero del ticket elettronico dell'unseal document.	
4	5	In caso di smart card con un proprio sistema di gestione dei PUK, il PUK non è noto al backend. Per questo motivo la scheda deve essere aperta con il PIN iniziale per il wizard.	
5	6	Il destinatario dei certificati specifica il suo PIN personale e la sua passphrase di revoca.	
6	7	Il wizard trasmette la passphrase di revoca alla banca dati centrale e ritira i certificati messi a disposizione. I certificati vengono importati sulla scheda con l'aiuto del PUK o del PIN iniziale e viene impostato il PIN personale della scheda.	
7	8	La smart card è attiva e protetta dal PIN personale del titolare dei certificati.	