NON CLASSIFIÉ

Déblocage de cartes à puce avec des certificats de classe B

Définition du processus

V1.2, 11.08.2016

Processus	**Déblocage de cartes à puce avec des certificats de classe B** Utiliser l'assistant pour mettre une carte en service	**ID**	SGPKI-CLB_M00.02
Classification *	Non classifié		
État **	Validé		
Auteur	Daniel Stich		
Approbateur (propriétaire)	Comité de direction de la Swiss Government PKI		
Responsabilité opérationnelle	BIT-BTR-BFS-BFO		
ID du document	0053-PD-SGPKI-CLB-M00.02		
Classement	Trustcenter PKI		
Description	Une fois qu'il a obtenu sa carte personnelle préparée et le document de déblocage correspondant au terme d'un processus RIO ou d'un processus synchrone auprès d'une console de gestion des certificats (*Certificate Management Console*, CMC), le destinataire des certificats peut débloquer sa carte. Pour cela, il doit se rendre auprès d'un poste de travail disposant de deux lecteurs de carte et sur lequel un utilisateur est déjà connecté. Après le lancement de l'assistant de déblocage (ce qui ne nécessite pas d'autorisation particulière), il doit introduire sa carte à puce dans le second lecteur. Ensuite, il doit saisir le numéro du ticket électronique inscrit sur le document de déblocage. L'assistant recherche alors les données de la carte et des certificats dans le système central. Le destinataire des certificats doit ensuite saisir son code NIP ainsi qu'une question et une réponse servant à la révocation. L'assistant charge alors les certificats sur la carte, les question et réponse de révocation sont enregistrées de manière centralisée, tandis que la carte à puce est protégée par le code NIP du destinataire des certificats. La carte est activée et prête à l'emploi.		
Modèle de processus	Collaboration		
Participants	- Destinataire des certificats - Utilisateur du poste de travail		
État initial	Le destinataire des certificats est en possession d'une carte préparée. La carte est encore bloquée. Les certificats correspondants ont été préalablement émis au moyen de l'assistant d'enregistrement ou de la CMC. Le destinataire des certificats est également en possession du numéro du ticket électronique correspondant.		
État final	La carte est débloquée, contient les certificats de classe B valables et est protégée par le code NIP du destinataire des certificats.		
Remarques	Ce processus s'applique à toutes les cartes à puce enregistrées de façon centralisée (cartes préparées et cartes non préparées qui ont ensuite été configurées avec l'assistant d'enregistrement prévu à cet effet).		

Contrôle des modifications, vérification et approbation

Version	Date	Description, remarque	Nom ou rôle
V0.1	19.05.2016	Version en cours de vérification	Daniel Stich
V0.2	25.05.2016	Modifications en fonction du feed-back	Daniel Stich
V1.0	26.05.2016	1re version principale validée	Daniel Stich
V1.1	11.08.2016	Dans le cadre du processus RIO, adaptation au traitement des cartes à puce non préparées et dotées d'un système de gestion PUK qui leur est propre	Daniel Stich
V1.2	15.09.2016	Détails du processus	

Références

Identification	Titre, source
[1]	**Enregistrement de cartes à puce non préparées** **Définition du processus** Version 0.2 du 05.08.2016 Source: Swiss Government PKI
[2]	**Processus RIO pour les certificats de classe B** **Définition du processus** Version 1.0 du 25.05.2016 Source: Swiss Government PKI

1 Modèle détaillé (MD)

Modèle de processus (description du déroulement)

Cette page n'a intentionnellement pas encore été modifiée.

Explications

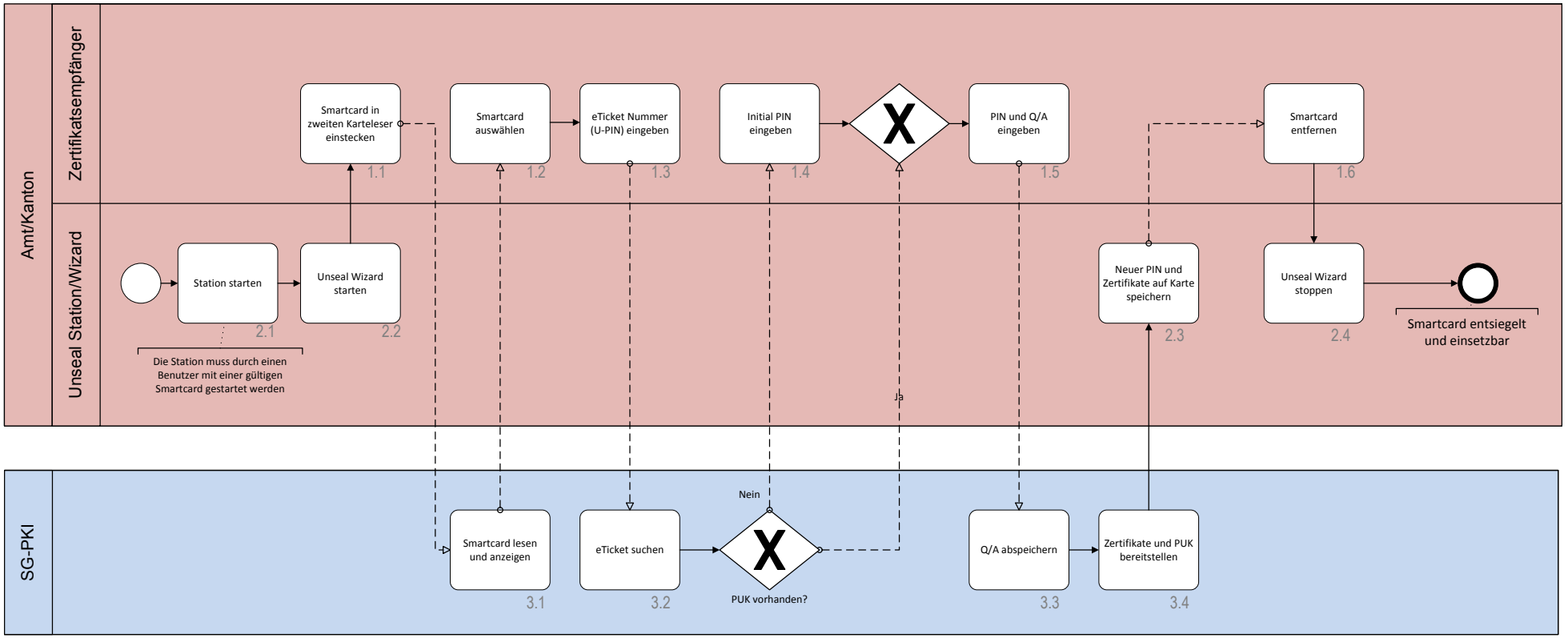
N°	Élément	Explication	Référence, aide

2 Modèle d'exploitation

Modèle de processus (description du processus)

SGPKI-CLB-M00.02: Smartcard entsiegeln

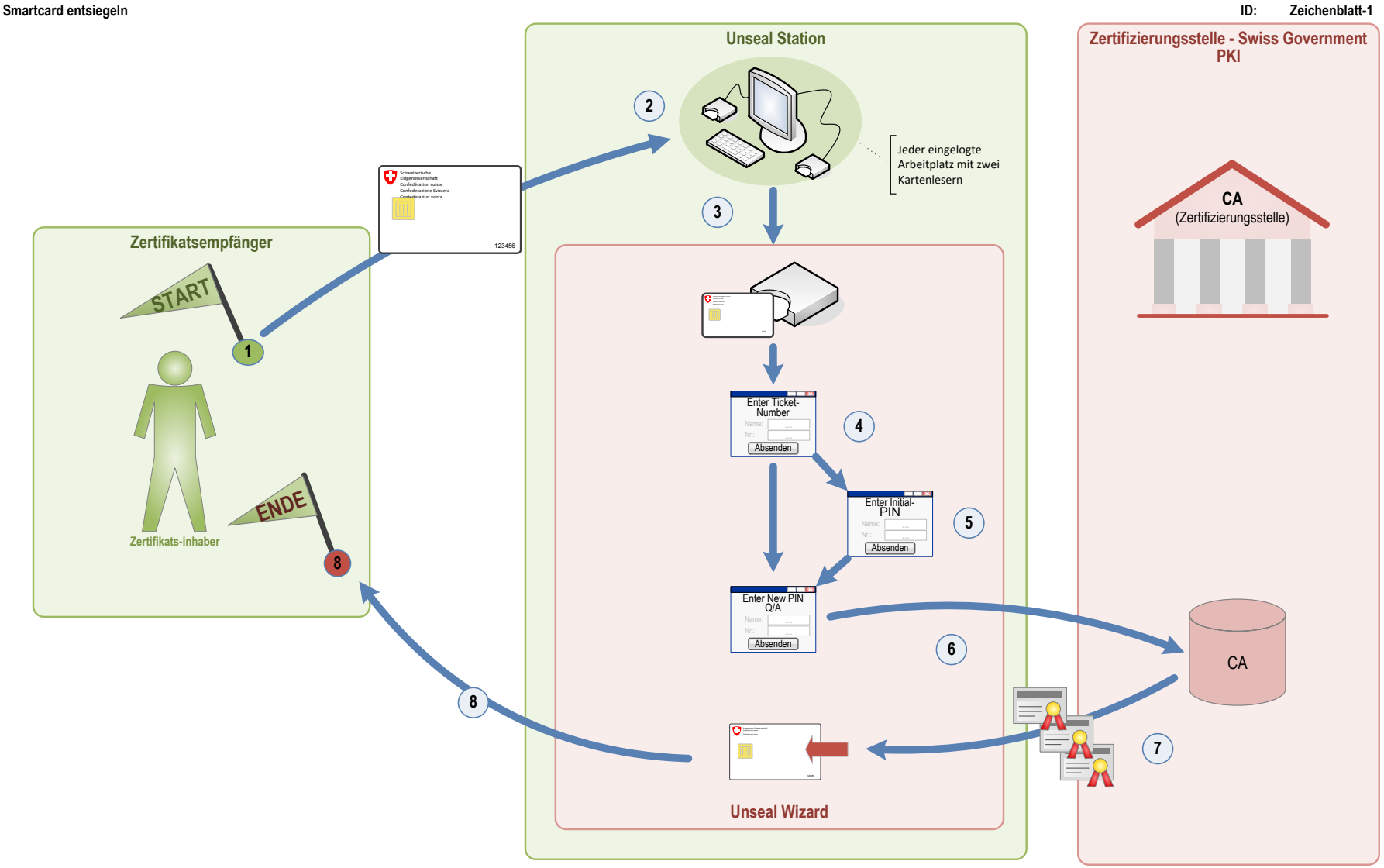
Kategorie: Betriebsmodell
Blatt: 1 / 1



Explications

N°	Élément	Explication	Référence, aide
1	2.1	L'assistant de déblocage peut être lancé sans autorisation particulière.	
2	1.1	La carte à débloquer doit être insérée dans le second lecteur de carte seulement après que l'assistant a été lancé.	
3	1.3	Le numéro du ticket électronique est inscrit sur le document de déblocage que le destinataire des certificats a reçu de l'officier LRA ou du RIO.	
4	1.4	Les services d'arrière-plan ne reconnaissent pas le PUK des cartes à puce disposant de leur propre système de gestion PUK. Pour cette raison, il faut saisir le code NIP initial de la carte dans l'assistant.	
5	1.5	Le destinataire des certificats définit son code NIP ainsi que ses question et réponse de révocation.	
6	2.3	L'assistant inscrit les certificats sur la carte et la sécurise avec le code NIP du destinataire des certificats.	

3 Schéma explicatif



Explications

N°	Éléments	Explication	Référence et aide
1	1	Le destinataire des certificats doit être en possession d'une carte à puce préparée et du document de déblocage correspondant.	
2	2	Un autre utilisateur doit être connecté au poste de travail et ce dernier doit disposer d'un second lecteur de carte.	
3	4	Il convient de saisir le numéro du ticket électronique mentionné sur le document de déblocage.	
4	5	Les services d'arrière-plan ne reconnaissent pas le PUK des cartes à puce disposant de leur propre système de gestion PUK. Pour cette raison, il faut saisir le code NIP initial de la carte dans l'assistant.	
5	6	Le destinataire des certificats définit son code NIP ainsi que ses question et réponse servant à la révocation.	
6	7	L'assistant transmet les question réponse de révocation à la banque de données centrale pour obtenir les certificats. Ceux-ci sont importés sur la carte à l'aide du PUK ou du code NIP initial. Le nouveau code NIP de la carte est alors enregistré.	
7	8	La carte à puce est activée et protégée par le code NIP du détenteur des certificats.	