

Réinitialisation du code NIP (certificats de classe B)

Définition du processus

V1.1, 10.01.2022

Processus	Réinitialisation du code NIP (certificats de classe B) Une carte à puce bloquée après 4 saisies erronées du code NIP est débloquée après contrôle. Un nouveau code NIP est ensuite défini.	ID	SGPKI-CLB-M12
Classification *	Non classifié		
Statut **	Validé		
Auteur	Daniel Stich / Gabrielle Lyoth		
Approbateur (propriétaire)	Comité de direction de la Swiss Government PKI		
Responsabilité opérationnelle	OFIT-BTR-BFS-BFO		
ID du document	0012-PD-SGPKI-CLB-M12_FR_2022-01-10.docx		
Classement	Certified PKI		
Description	<p>La carte à puce contenant des certificats de classe B est bloquée après quatre saisies erronées du code NIP. Dans un premier temps, le détenteur des certificats s'adresse au Service Desk. Son identité est vérifiée à l'aide des questions de sécurité enregistrées. Si la vérification est réussie, le collaborateur du Service Desk ouvre un ticket dans l'application Internet de la Swiss Government PKI et recherche la carte à puce bloquée au moyen du numéro de série ou du nom du détenteur des certificats.</p> <p>Après l'ouverture du ticket de réinitialisation du code NIP, le détenteur des certificats doit se rendre à un poste de travail disposant de deux lecteurs de carte. Un utilisateur pouvant réinitialiser des codes NIP (URN) doit être connecté à ce poste de travail. Il démarre l'assistant de réinitialisation du code NIP et se connecte au moyen de son certificat de classe B en cours de validité. Ensuite, le détenteur des certificats insère sa carte bloquée dans le lecteur libre. L'assistant de réinitialisation du code NIP lit le numéro de série de la carte et cherche un ticket correspondant à celui-ci dans le système central PKI.</p> <p>L'URN doit ensuite identifier clairement le détenteur des certificats: soit il connaît personnellement le détenteur des certificats, soit il l'identifie au moyen d'une pièce d'identité valable. L'URN doit confirmer l'identification dans l'assistant. Le système PKI envoie ensuite une version cryptée du PUK de la carte à l'assistant et le détenteur des certificats est invité à saisir son nouveau code NIP deux fois. L'assistant utilise ces informations, ainsi que le PUK, pour réinitialiser le code NIP de la carte. La carte à puce est maintenant débloquée et opérationnelle. Elle peut être retirée du lecteur.</p> <p>Les informations sur la carte débloquée dont le code NIP a été réinitialisé ainsi que le nom de l'URN sont consignés dans un rapport d'activité.</p>		
Modèle de processus	Collaboration		
Participants	<ul style="list-style-type: none"> - Détenteur des certificats - Service Desk - Utilisateur pouvant réinitialiser des codes NIP 		

État initial	La carte à puce du détenteur des certificats est bloquée après cinq saisies erronées du code NIP et doit donc être débloquée pour être utilisée de nouveau.
État final	La carte à puce est débloquée et un nouveau code NIP est défini. La carte peut de nouveau être utilisée et les certificats sont opérationnels.
Remarques	Ce processus est destiné aux cartes à puce préparées.

1 Modèle détaillé

Modèle de processus (description du déroulement)

Cette page n'a volontairement pas encore été réalisée.

Explications

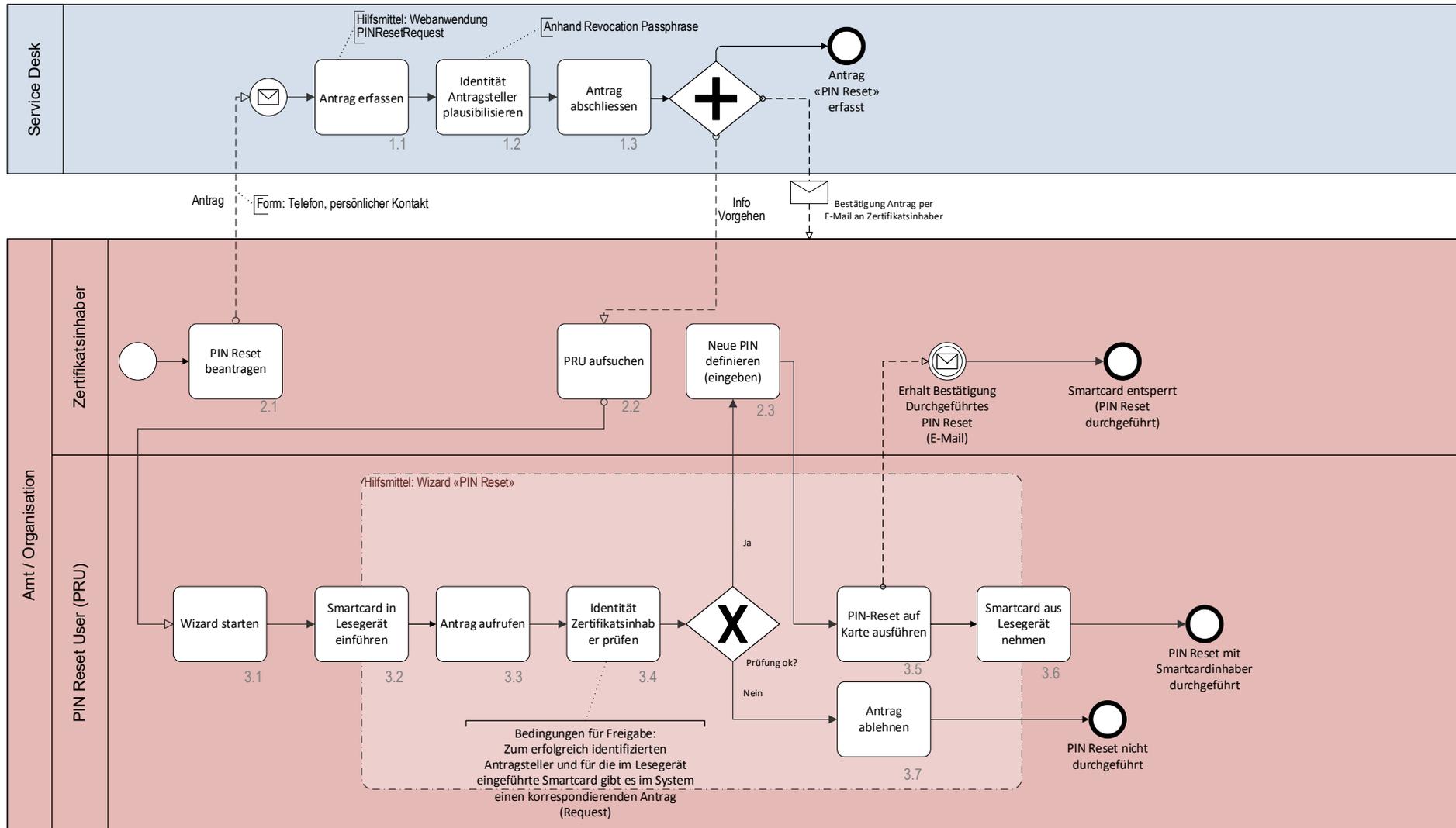
N°	Élément	Explication	Référence, aide

2 Modèle d'exploitation

Modèle de processus (description du déroulement)

SGPKI-CLB-M12: PIN Reset

Kategorie: Betriebsmodell
Blatt: 1/1



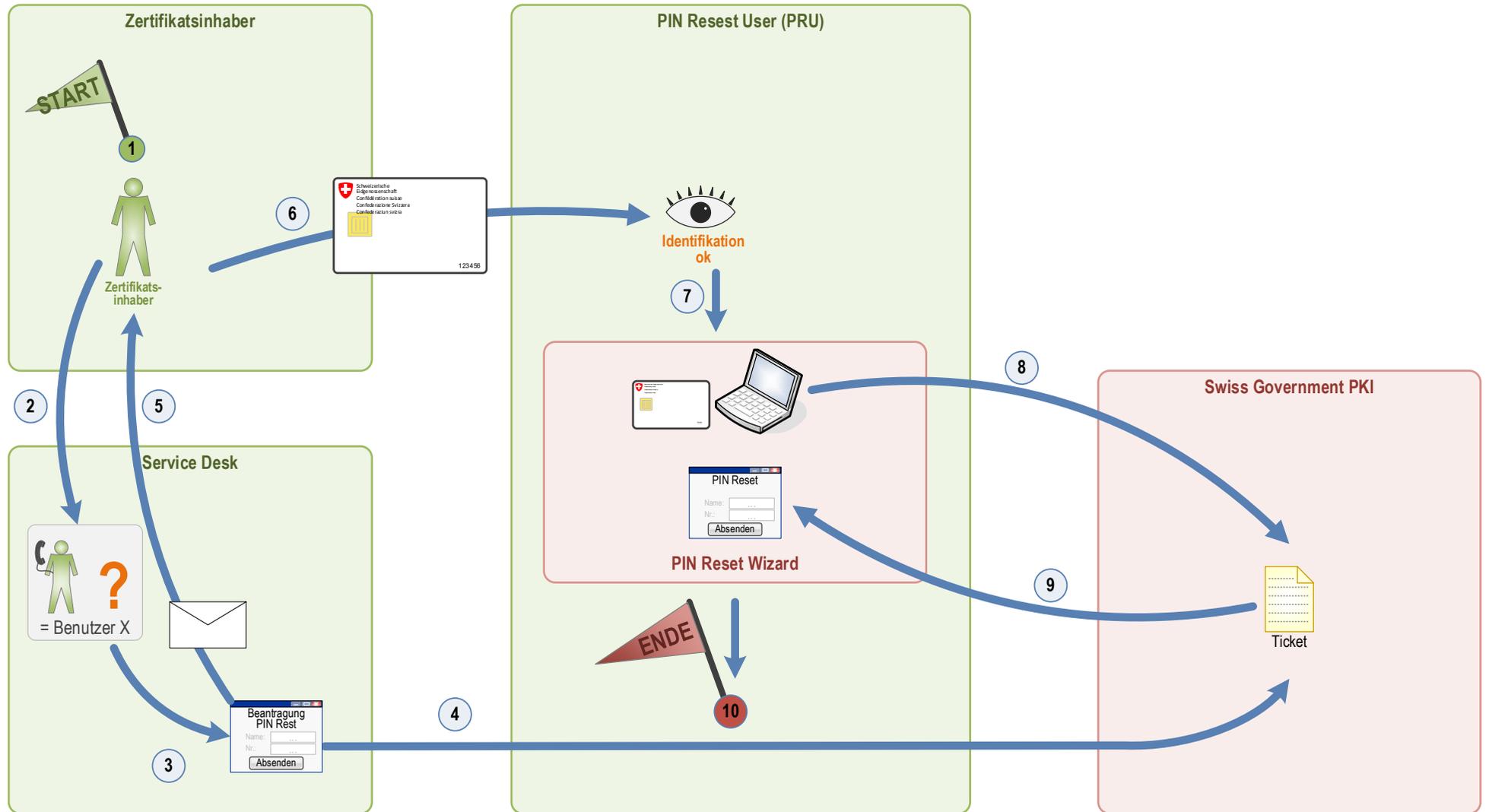
Explications

N°	Élément	Explication	Référence, aide
1	1.1	Le numéro de série ou le nom du détenteur des certificats peuvent être utilisés pour rechercher la carte bloquée.	
2	1.2	Le Service Desk vérifie l'identité de l'auteur de la demande en lui posant la question de sécurité servant aussi à la révocation.	
3	2.2	L'URN doit être détenteur d'un certificat de classe B valable et disposer d'un deuxième lecteur de carte à son poste de travail.	
4	3.1	L'URN se connecte au moyen de son certificat de classe B.	
5	3.3	L'assistant cherche automatiquement la demande au moyen du numéro de série de la carte à puce insérée.	
6	3.4	L'identification doit être confirmée explicitement par l'URN et est consignée dans le rapport de réinitialisation avec les informations relatives aux personnes concernées.	

3 Schéma explicatif

PIN Reset

ID: Zeichenblatt-1



Explications

N°	Élément	Explication	Référence, aide
1	1	La carte à puce du détenteur des certificats est bloquée.	
2	2	Le détenteur des certificats prend contact avec le Service Desk par téléphone.	
3	3	Le Service Desk contrôle l'identité du détenteur des certificats à l'aide des questions de sécurité personnelles enregistrées.	
4	4	Le Service Desk ouvre le ticket de réinitialisation du code NIP avec l'application Internet de la PKI et doit pour ce faire entrer le numéro de série de la carte à puce bloquée.	
5	5	Le Service Desk charge le détenteur des certificats de se rendre auprès d'un URN. Dans le même temps, le détenteur des certificats reçoit les détails de la demande dans un courriel du système PKI. En règle générale, le détenteur des certificats ne peut lire ce courriel que lorsque le processus est terminé. Toutefois, si une demande de réinitialisation du code NIP a été effectuée pour lui par erreur, il peut intervenir aussitôt auprès du Service Desk.	
6	6	Le détenteur des certificats se rend auprès de l'URN avec sa carte à puce bloquée.	Tout utilisateur en possession d'un certificat de classe B valable peut agir en tant qu'URN. L'accès à un poste de travail comprenant un deuxième lecteur de carte est par ailleurs requis.
7	7	L'URN identifie le détenteur des certificats, soit parce qu'il le connaît personnellement, soit parce qu'il a contrôlé sa pièce d'identité.	
8	8	Une fois la carte à puce bloquée introduite dans le lecteur, l'assistant cherche le ticket correspondant dans le système PKI.	
9	9	Le PUK requis est transmis sous forme codée depuis le système PKI vers l'assistant. Le détenteur des certificats entre le nouveau code NIP. L'assistant débloque la carte avec le PUK et définit simultanément le nouveau code NIP.	
10	10	La carte est débloquée et de nouveau opérationnelle.	