NON CLASSIFIÉ

Récupération de clés pour les certificats de classe B

Définition du processus

V1.1, 05.12.2016

Processus	**Récupération de clés pour les certificats de classe B** Rétablissement d'une ancienne clé de cryptage sur la carte à puce actuelle	**ID**	SGPKI-CLB-M13
Classification *	Non classifié		
Statut **	Validé		
Auteur	Daniel Stich		
Approbateur (propriétaire)	Comité de direction de la Swiss Government PKI		
Responsabilité opérationnelle	OFIT-BTR-BFS-BFO		
ID du document	0013-PD-SGPKI-CLB-M13.docx		
Classement	Trustcenter PKI		
Description	Le détenteur des certificats remarque qu'il ne peut plus lire un ancien courriel crypté car la clé privée correspondante n'est plus sauvegardée sur sa carte à puce actuelle. Il ouvre l'application de récupération de clé dans son navigateur et crée un ticket électronique dans le système PKI central. Il reçoit aussitôt le numéro du ticket électronique créé, à condition que son unité administrative ne requière pas d'autorisation supplémentaire pour une demande de récupération de clé. Sinon, le ticket électronique est soumis à un officier traitant la récupération de clé pour validation. Si la demande est acceptée, le numéro du ticket électronique est envoyé au détenteur des certificats. Muni du numéro du ticket électronique et de sa carte à puce, le détenteur des certificats se rend auprès de l'officier LRA responsable ou d'un agent habilité à la récupération des clés. Le rôle d'agent habilité à la récupération des clés est compris dans les autorisations dont dispose l'officier LRA. De plus, les RIO peuvent demander l'obtention de ce rôle au service Gestion des ordres de la PKI au moyen d'un formulaire ad hoc. Après que le détenteur des certificats a transmis son ticket à l'officier LRA ou à l'agent habilité à la récupération des clés, celui-ci démarre l'assistant de récupération des clés et saisit le numéro du ticket électronique. L'assistant affiche tous les certificats de cryptage qui ont déjà été délivrés au détenteur des certificats. Ce dernier indique à l'officier LRA ou à l'agent habilité à la récupération des clés quelles clés il souhaite récupérer. Après que le détenteur des certificats a saisi son code NIP personnel, l'assistant inscrit les clés de cryptage sur la carte à puce.		
Modèle de processus	Collaboration		
Participants	- Détenteur des certificats - Service Desk - Agent habilité à la récupération des clés - Officier traitant la récupération des clés - Officier LRA		
État initial	La clé correspondant à un certificat de cryptage (périmé) n'est plus sauvegardée sur la carte à puce.		
État final	La clé nécessaire est de nouveau utilisable sur la carte à puce.		
Remarques	Ce processus est destiné aux cartes à puce préparées et non préparées.		

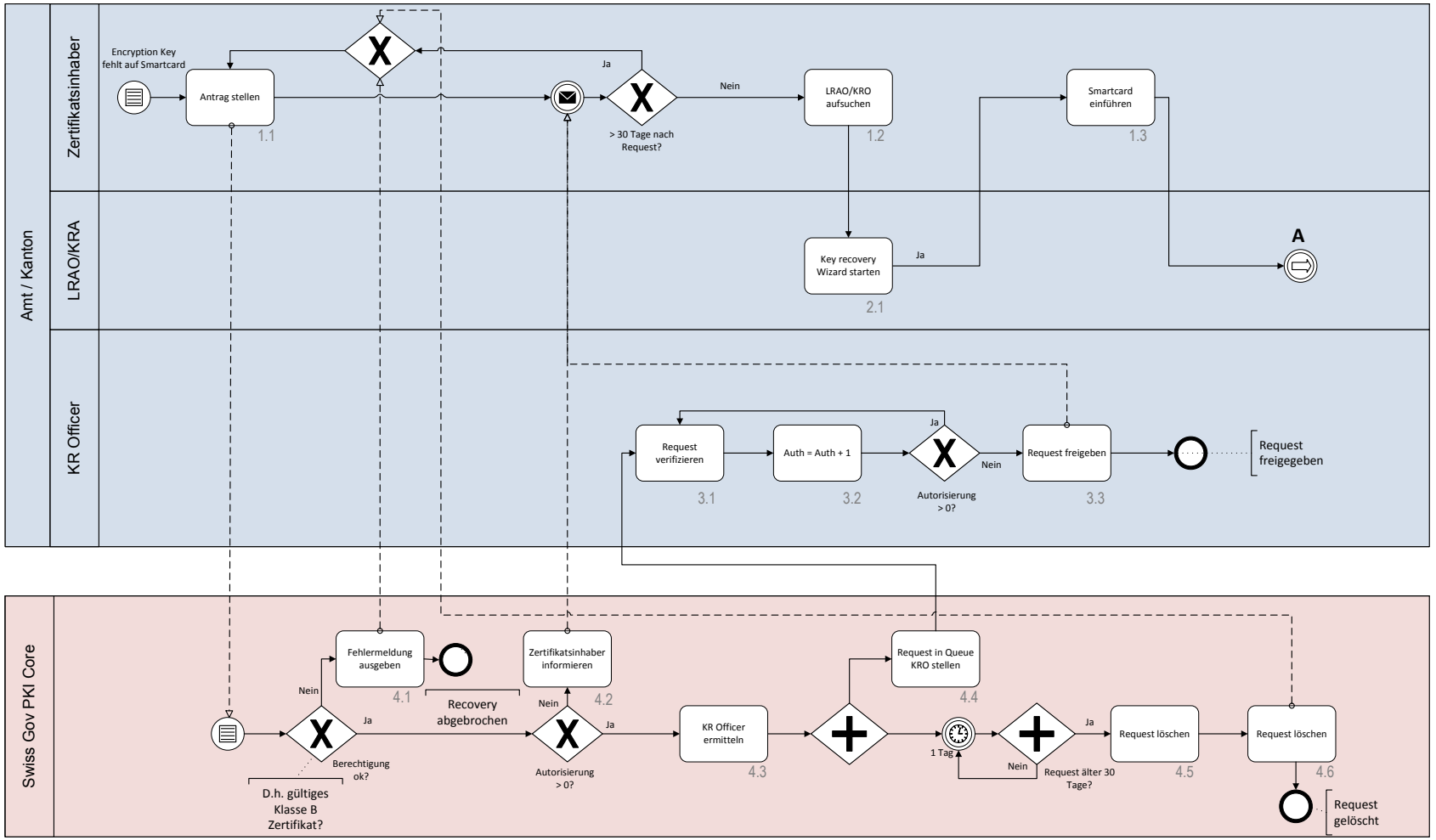
https://community.bit.admin.ch/team/Trustcenter-PKI-BIT/Private/Dokumentation SwissGov PKI/Certified PKI/Betriebs- und Supportdokumentation/03 Klasse B/0013-PD-SGPKI-CLB-M13_FR.docx

1 Modèle détaillé

Modèle de processus (description du déroulement)

SGPKI-CLB-M13: Key Recovery

Kategorie: Detailmodell
Blatt: 1 / 2

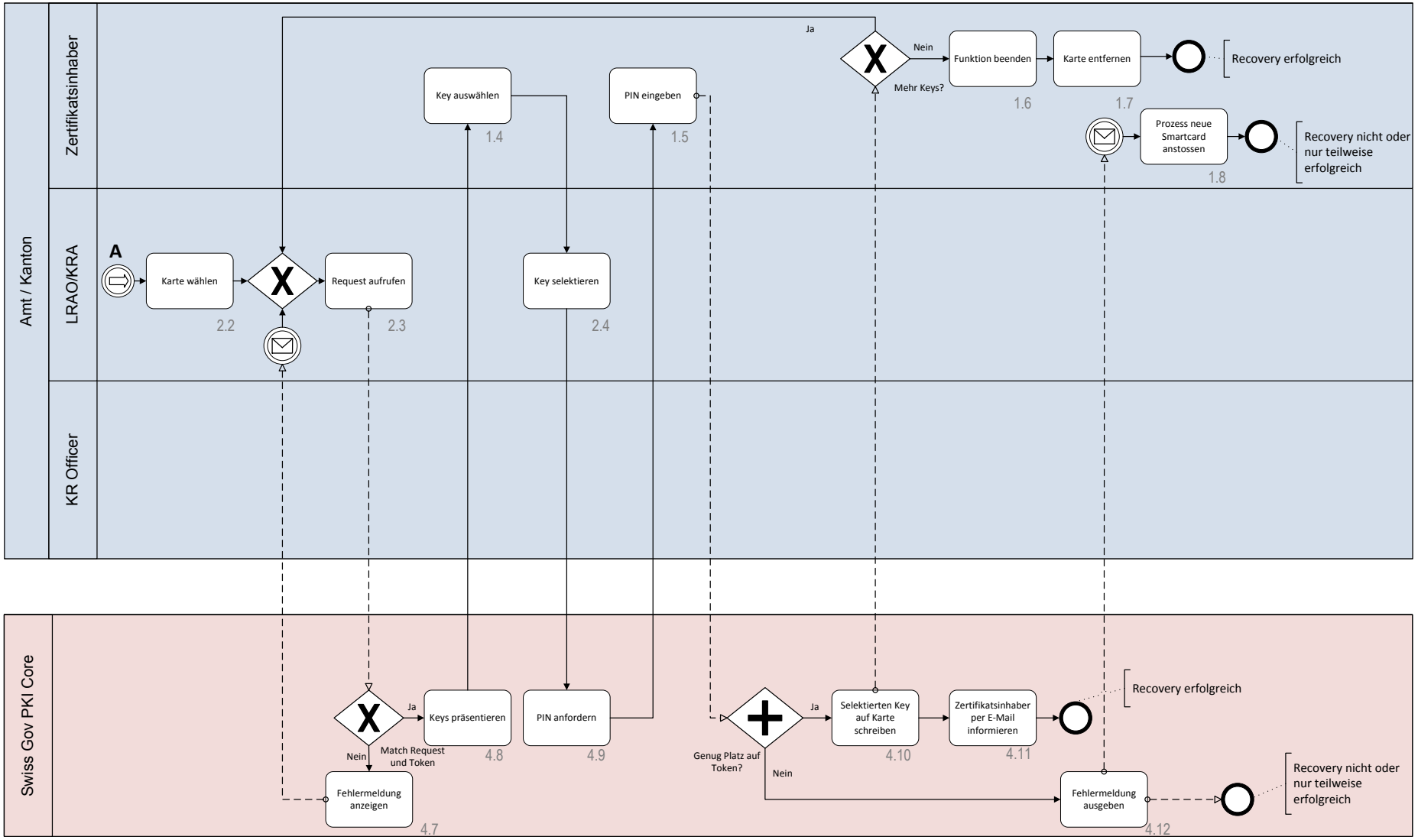


Explications

N°	Élément	Explication	Référence, aide
1	1.1	Chaque détenteur d'une carte à puce contenant un certificat de classe B valable peut faire une demande (par ticket électronique) de récupération de clé au moyen de l'outil web KeyRecoveryRequest.	
2	4.2	Après vérification de la validité des certificats de classe B, et dans la mesure où aucune autorisation supplémentaire n'est nécessaire, l'utilisateur reçoit le numéro du ticket électronique pour la récupération des clés.	
3	3.1., 3.2	Suivant la configuration, la demande doit être validée par un officier traitant la récupération des clés.	
4	3.3	Si toutes les procédures d'autorisation ont été effectuées avec succès, l'utilisateur reçoit le numéro du ticket électronique pour la récupération des clés.	
5	4.5, 4.6	Si une demande n'est pas traitée pendant une période de 30 jours, elle est supprimée automatiquement par le système.	
6	2.1	Une carte à puce comportant un certificat d'officier LRA est nécessaire au démarrage de l'assistant de récupération des clés. Il peut s'agir de la carte à puce d'un officier LRA ou d'un agent habilité, par autorisation spéciale, à la récupération des clés. Cette autorisation (et la carte à puce d'officier LRA correspondante) dont dispose l'agent habilité à la récupération des clés ne vaut que pour l'exécution de l'assistant de récupération des clés et doit être demandée au service Gestion des ordres de la PKI au moyen d'un formulaire signé par l'office.	

SGPKI-CLB-M13: Key Recovery

Kategorie: Detailmodell
Blatt: 2 / 2



Explications

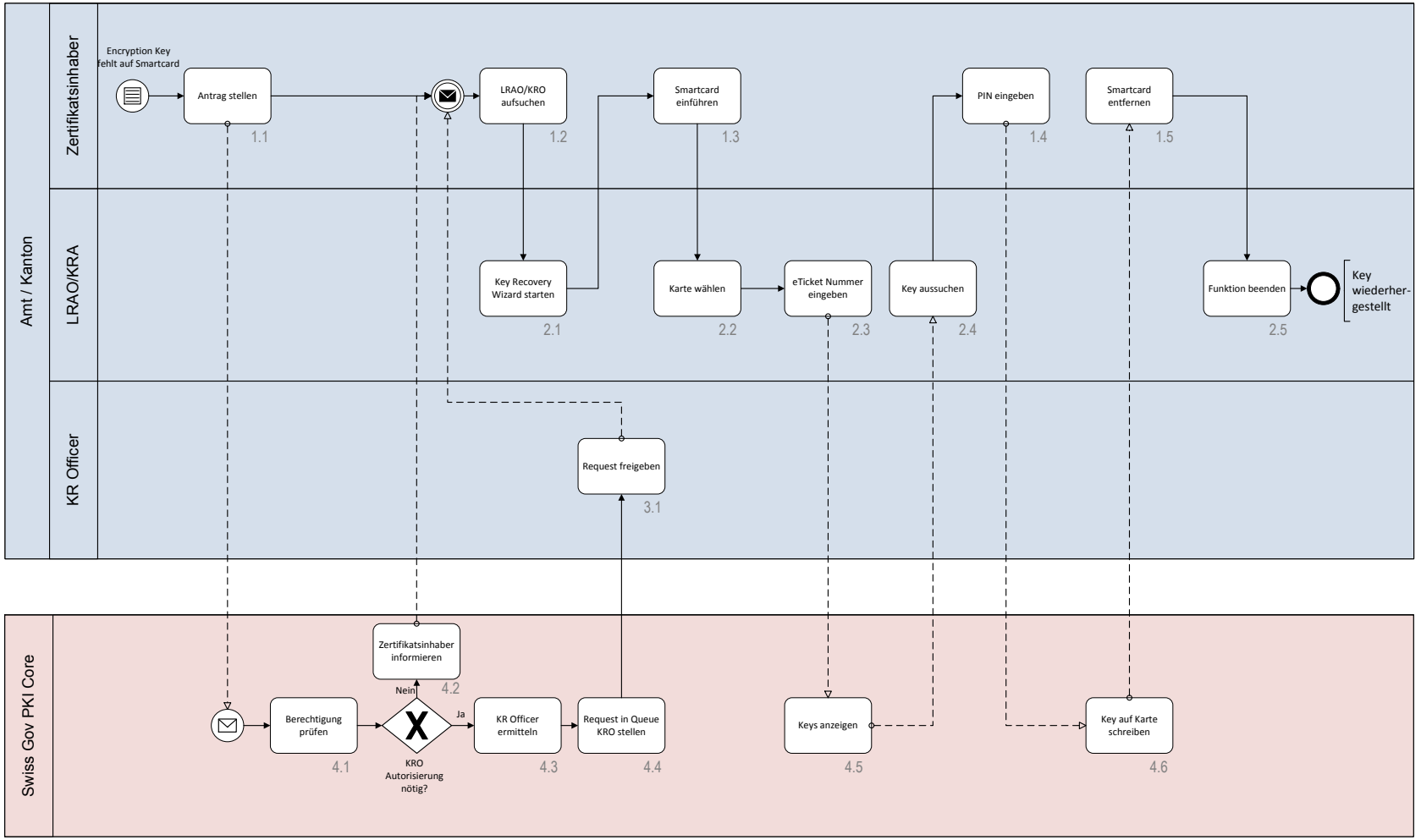
N°	Élément	Explication	Référence, aide
1	2.2	La carte insérée doit tout d'abord être sélectionnée.	
2	2.3	La demande est ouverte dans le service d'arrière-plan au moyen du numéro du ticket électronique.	
3	4.8	Le service d'arrière-plan vérifie le numéro de série de la carte, recherche le ticket électronique et compare les données du ticket avec celles de la carte insérée. Si les données de la carte et du ticket correspondent, toutes les clés de cryptage sauvegardées dans le système pour cet utilisateur s'affichent.	
4	1.4, 2.4	L'utilisateur sélectionne la clé souhaitée, avec l'aide de l'officier LRA ou de l'agent habilité à la récupération des clés.	
5	1.5	L'utilisateur doit saisir son code NIP pour que la clé puisse être inscrite sur la carte à puce.	
6	4.10	Si la carte dispose de suffisamment de mémoire, la clé est inscrite sur la carte.	
7	1.6	Si d'autres clés doivent être inscrites, l'assistant revient au début du traitement de la demande. Sinon, l'assistant se ferme.	

2 Modèle d'exploitation

Modèle de processus (description du déroulement)

SGPKI-CLB-M13: Key Recovery

Kategorie: Betriebsmodell
Blatt: 1 / 1

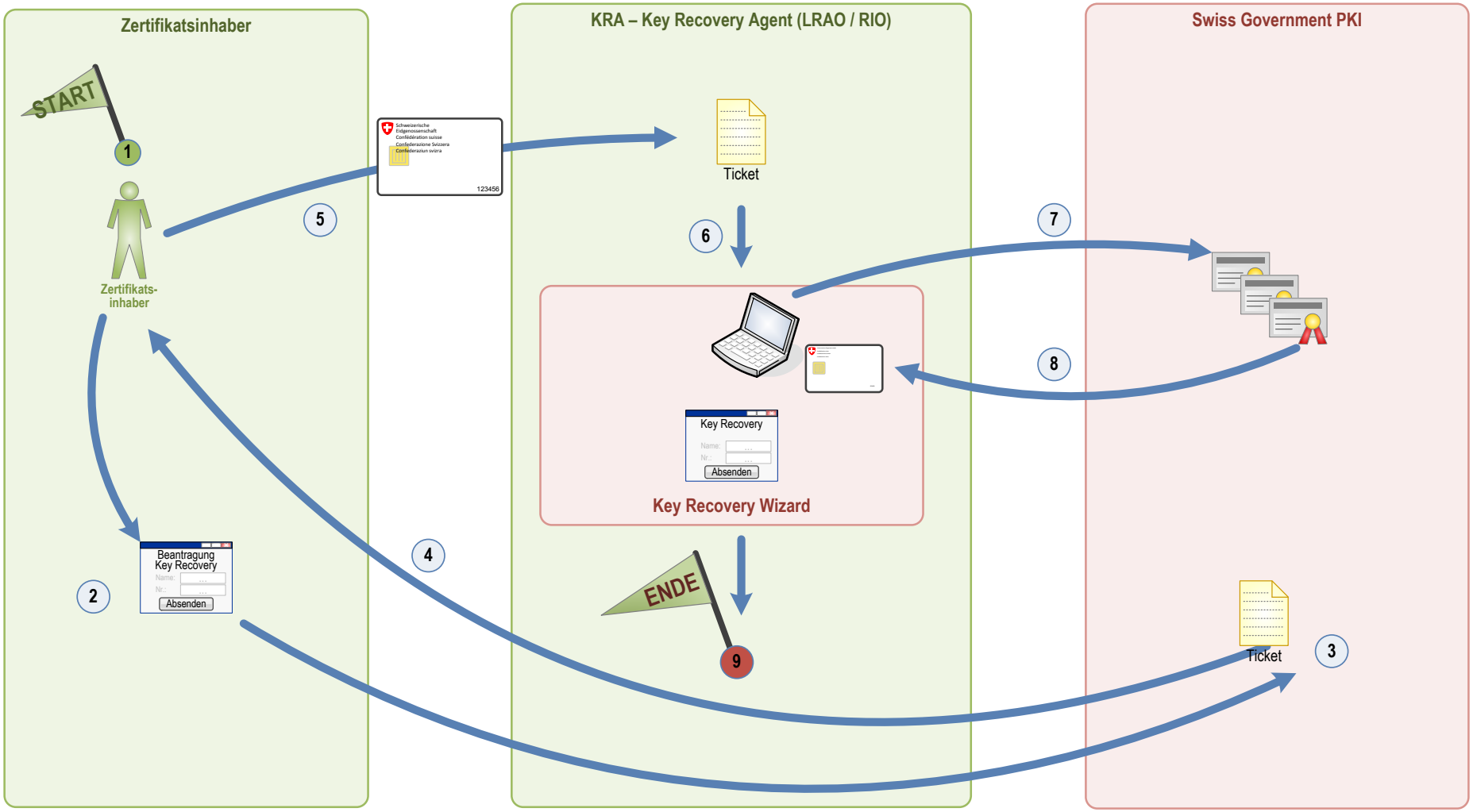


Explications

N°	Élément	Explication	Référence, aide
1	1.1	Chaque détenteur d'une carte à puce contenant un certificat de classe B valable peut faire une demande (par ticket électronique) de récupération de clé au moyen de l'outil web KeyRecoveryRequest.	
2	4.1	Selon les paramètres de l'office, une autorisation supplémentaire d'un officier traitant la récupération de clés peut être nécessaire pour la demande.	
3	2.1	L'assistant de récupération des clés peut uniquement être démarré par un officier LRA ou un agent habilité à la récupération des clés.	
4	2.3	Il convient d'indiquer le numéro du ticket électronique généré par le détenteur des certificats lorsqu'il a établi sa demande.	
5	1.4	Pour pouvoir récupérer la clé, le code NIP de la carte sur laquelle la clé sera inscrite est requis.	

3 Schéma explicatif

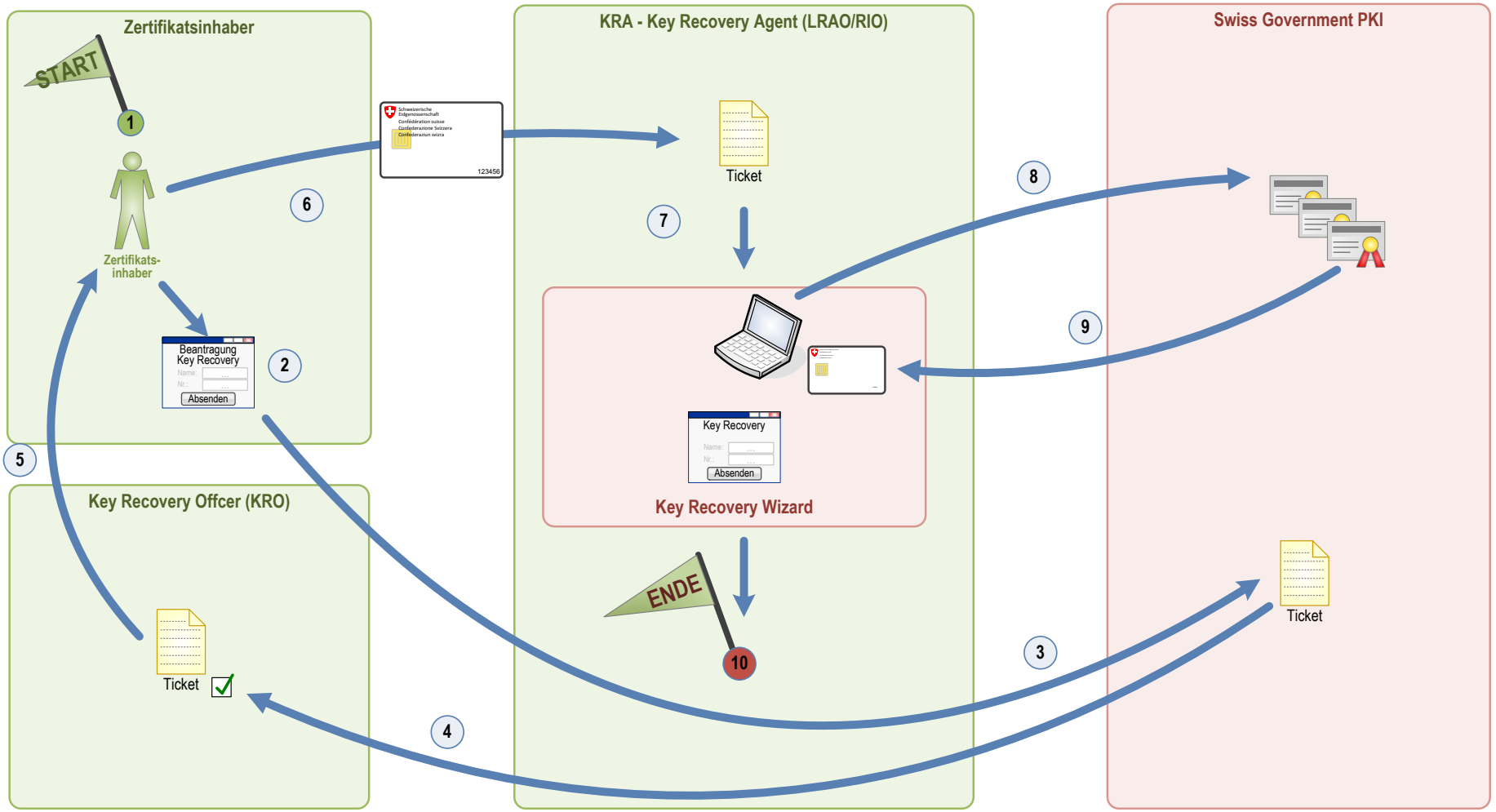
Key Recovery ohne KRO (Key Recovery Officer) Funktion **ID: Zeichenblatt-1**



Explications

N°	Élément	Explication	Référence, aide
1	1	Le détenteur des certificats constate qu'il ne peut plus ouvrir un courriel crypté parce qu'il ne dispose pas de la clé privée de cryptage correspondante ou parce qu'une nouvelle carte à puce lui a été délivrée.	
2	2,3	Au moyen de l'outil web KeyRecoveryRequest, le détenteur des certificats ouvre un ticket électronique pour la récupération des clés.	
3	4	Le numéro du ticket électronique est transmis au détenteur des certificats.	
4	5	Le détenteur des certificats se rend auprès de l'officier LRA ou de l'agent habilité à la récupération des clés avec le numéro du ticket électronique.	
5	6	L'officier LRA ou l'agent habilité à la récupération des clés démarre l'assistant de récupération et, accompagné du détenteur des certificats, sélectionne les clés à récupérer. Ensuite, l'assistant inscrit celles-ci sur la carte à puce.	

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



Explications

N°	Élément	Explication	Référence, aide
1	1	Le détenteur des certificats constate qu'il ne peut plus ouvrir un courriel crypté parce qu'il ne dispose pas de la clé privée de cryptage correspondante ou parce qu'une nouvelle carte à puce lui a été délivrée.	
2	2, 3	Au moyen de l'outil web KeyRecoveryRequest, le détenteur des certificats ouvre un ticket électronique pour la récupération des clés.	
3	4	L'officier traitant la récupération des clés doit valider la demande de récupération.	
4	5	Après que l'officier traitant la récupération des clés a validé la demande, le numéro du ticket électronique est transmis au détenteur des certificats.	
5	6	Le détenteur des certificats se rend auprès de l'officier LRA ou de l'agent habilité à la récupération des clés avec le numéro du ticket électronique.	
6	7, 8, 9	L'officier LRA ou l'agent habilité à la récupération des clés démarre l'assistant de récupération et, accompagné du détenteur des certificats, sélectionne les clés à récupérer. Ensuite, l'assistant inscrit celles-ci sur la carte à puce.	