

# Génération de nouvelles clés pour les certificats de classe B

## Définition du processus

V1.0, 25.05.2016

|                                      |   |           |               |
|--------------------------------------|---|-----------|---------------|
| <b>Processus</b>                     | <b>Génération de nouvelles clés pour les certificats de classe B</b><br>Émission de nouveaux certificats pour une personne déjà enregistrée et détenant des certificats valables  | <b>ID</b> | SGPKI-CLB-M10 |
| <b>Classification *</b>              | Non classifié   |           |               |
| <b>État **</b>                       | Validé  |           |               |
| <b>Auteur</b>                        | Daniel Stich  |           |               |
| <b>Approbateur (propriétaire)</b>    | Comité de direction de la Swiss Government PKI  |           |               |
| <b>Responsabilité opérationnelle</b> | BIT-BTR-BFS-BFO   |           |               |
| <b>ID du document</b>                | 0010-PD-SGPKI-CLB-M10.docx  |           |               |
| <b>Classement</b>                    | Trustcenter PKI   |           |               |
| <b>Description</b>                   | Les certificats de classe B sont valables trois ans. Après ce délai, le détenteur des certificats dispose de 60 jours pour faire émettre une nouvelle série de certificats sur sa carte à puce à l'aide de l'assistant de génération de nouvelles clés et de son certificat d'authentification de classe B valable. Le système envoie un courriel à l'utilisateur 90 puis 30 jours avant l'expiration de ses certificats actuels pour l'avertir de l'invalidité prochaine de ces derniers. Le détenteur des certificats peut effectuer lui-même la procédure de renouvellement sur son poste de travail. Il n'a besoin pour ce faire d'aucune autorisation. |           |               |
| <b>Modèle de processus</b>           | Collaboration   |           |               |
| <b>Participants</b>                  | - Détenteur des certificats   |           |               |
| <b>État initial</b>                  | Les certificats actuels de l'utilisateur expireront prochainement.  |           |               |
| <b>État final</b>                    | La carte à puce est équipée de nouveaux certificats d'une durée de validité de trois ans.   |           |               |
| <b>Remarques</b>                     |   |           |               |

## 1 Modèle détaillé

### Modèle de processus (description du déroulement)

*Cette page est volontairement vide.*

**Explications**

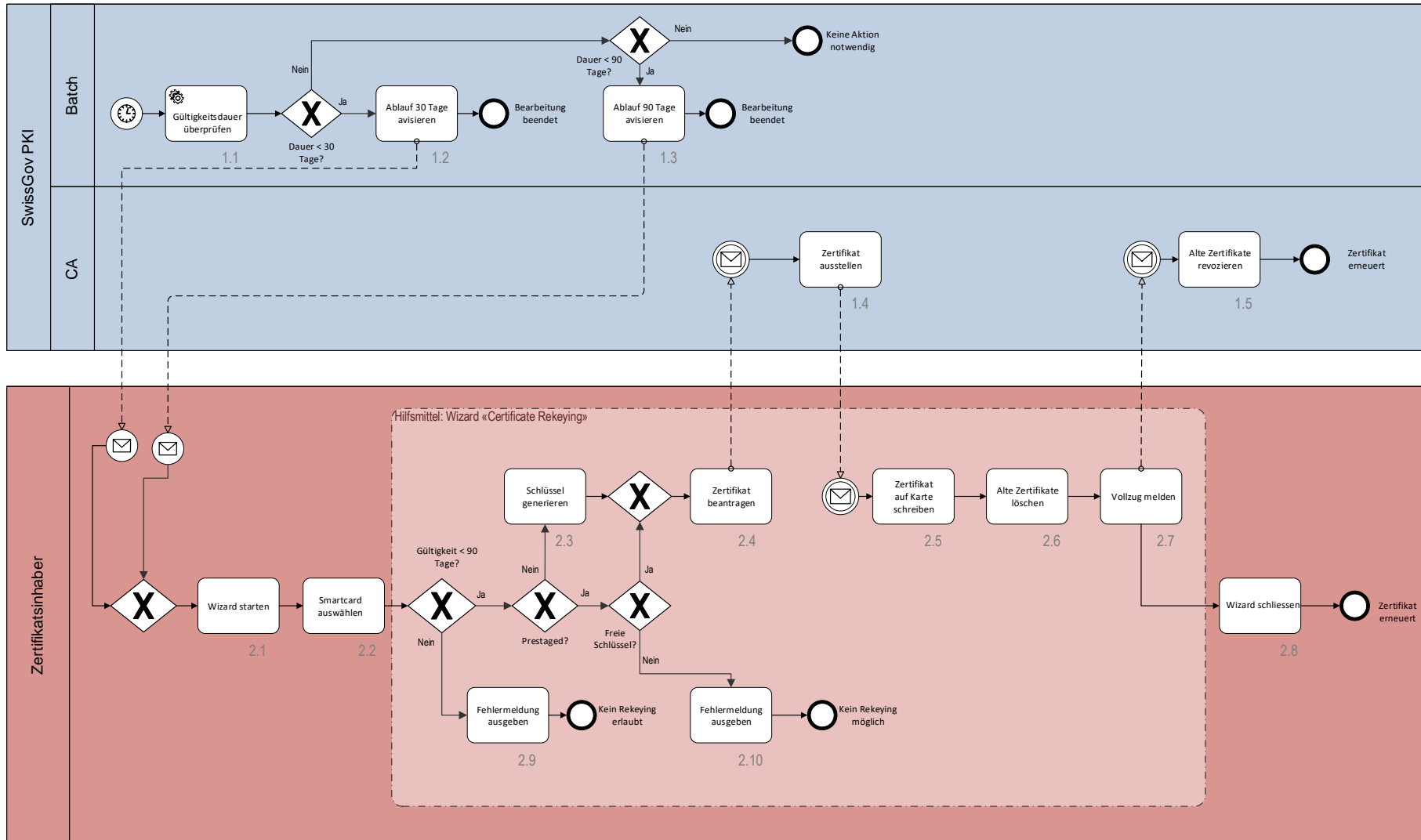
| N° | Élément | Explication | Référence, aide |
|----|---------|-------------|-----------------|
|    |         |             |                 |
|    |         |             |                 |
|    |         |             |                 |
|    |         |             |                 |
|    |         |             |                 |

## 2 Modèle d'exploitation

### Modèle de processus (description du déroulement)

SGPKI-CLB-M10: Certificate Rekeying

Kategorie: Betriebsmodell  
Blatt: 1/1



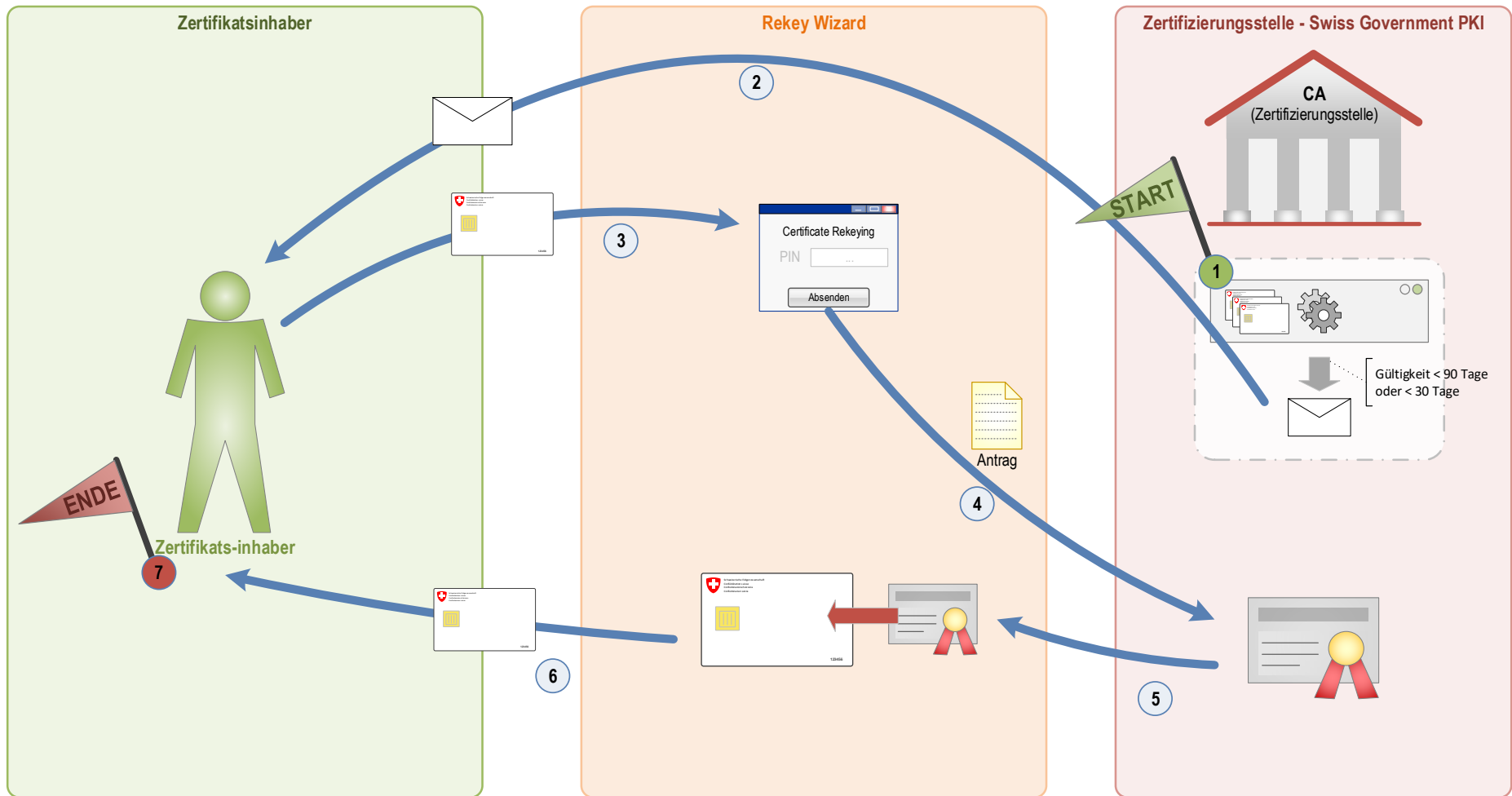
**Explications**

| N° | Élément  | Explication  | Référence, aide |
|----|----------|--|-----------------|
| 1  | 1.2, 1.3 | Le système central envoie un courriel à l'utilisateur 90 puis 30 jours avant l'expiration de ses certificats pour l'avertir de leur invalidité prochaine.  |                 |
| 2  | 2.1      | L'assistant est installé sur tous les postes de travail de la Confédération à titre de produit de couche 1.  |                 |
| 3  | 2.9      | Les certificats ne peuvent être renouvelés que 90 jours avant leur expiration.   |                 |
| 4  | 2.10     | Les cartes à puce préparées possèdent trois jeux complets de trois paires de clés. Ainsi, les certificats peuvent être renouvelés deux fois sur ce type de carte avant que celle-ci ne soit remplacée. |                 |
| 5  | 2.6      | Les anciens certificats sont automatiquement révoqués et supprimés de la carte. Seuls les certificats de chiffrement restent enregistrés sur la carte.   |                 |

### 3 Schéma explicatif

Certificate Rekeying

ID: Zeichenblatt-1



**Explications**

| N° | Élément | Explication  | Référence, aide |
|----|---------|--|-----------------|
| 1  | 1       | Le système central informe l'utilisateur 90 puis 30 jours avant l'expiration de ses certificats de leur invalidité prochaine et l'invite à les renouveler. |                 |
| 2  | 3       | L'assistant est disponible sur chaque ordinateur de l'administration fédérale à titre de logiciel de couche 1.   |                 |