

Certificate Rekeying (Renewal) Klasse B

Prozessdefinition

V1.0, 25.05.2016

| | | | |
|--------------------------------|--|-----------|---------------|
| Prozess | Certificate Rekeying Klasse B Neue Zertifikate für eine bereits registrierte, mit gültigen Zertifikaten ausgerüstete Person ausstellen. | ID | SGPKI-CLB-M10 |
| Klassifizierung * | Nicht klassifiziert | | |
| Status ** | Freigegeben | | |
| Autor | Daniel Stich | | |
| Genehmigende (Eigner) | Swiss Government PKI Management Board | | |
| Operative Verantwortung | BIT-BTR-BFS-BFO | | |
| Doc_ID | 0010-PD-SGPKI-CLB-M10.docx | | |
| Ablageort | Trustcenter PKI | | |
| Beschreibung | Die Zertifikate der Klasse B haben eine Gültigkeit von drei Jahren. Nach den ersten 60 Tagen dieser Zeitspanne kann der Zertifikatsinhaber mit Hilfe des hier beschriebenen Wizards und seinem gültigen Klasse B Authentisierungszertifikat einen neuen Satz von Zertifikaten auf seiner Smartcard erstellen lassen. Der Benutzer wird vom System 90 und 30 Tage vor Ablauf der Gültigkeit der aktuellen Zertifikate per Mail auf den bevorstehenden Ablauf aufmerksam gemacht. Der Zertifikatsinhaber kann den Erneuerungsprozess selbstständig auf seiner Arbeitsstation durchführen und benötigt keine explizite Autorisierung dieses Vorgangs. | | |
| Prozessmodell | Kollaboration | | |
| Teilnehmer | - Zertifikatsinhaber | | |
| Input (Anfangszustand) | Die bestehenden Zertifikate des Zertifikatsinhabers laufen demnächst ab. | | |
| Output (Endzustand) | Auf der Smartcard des Zertifikatsinhaber stehen neue Zertifikate mit einer Laufzeit von drei Jahren zur Verfügung | | |
| Bemerkungen | | | |

1 Detailmodell (DM)

Prozessmodell (Ablaufdefinition)

Diese Seite ist mit Absicht leer gelassen

Erläuterungen

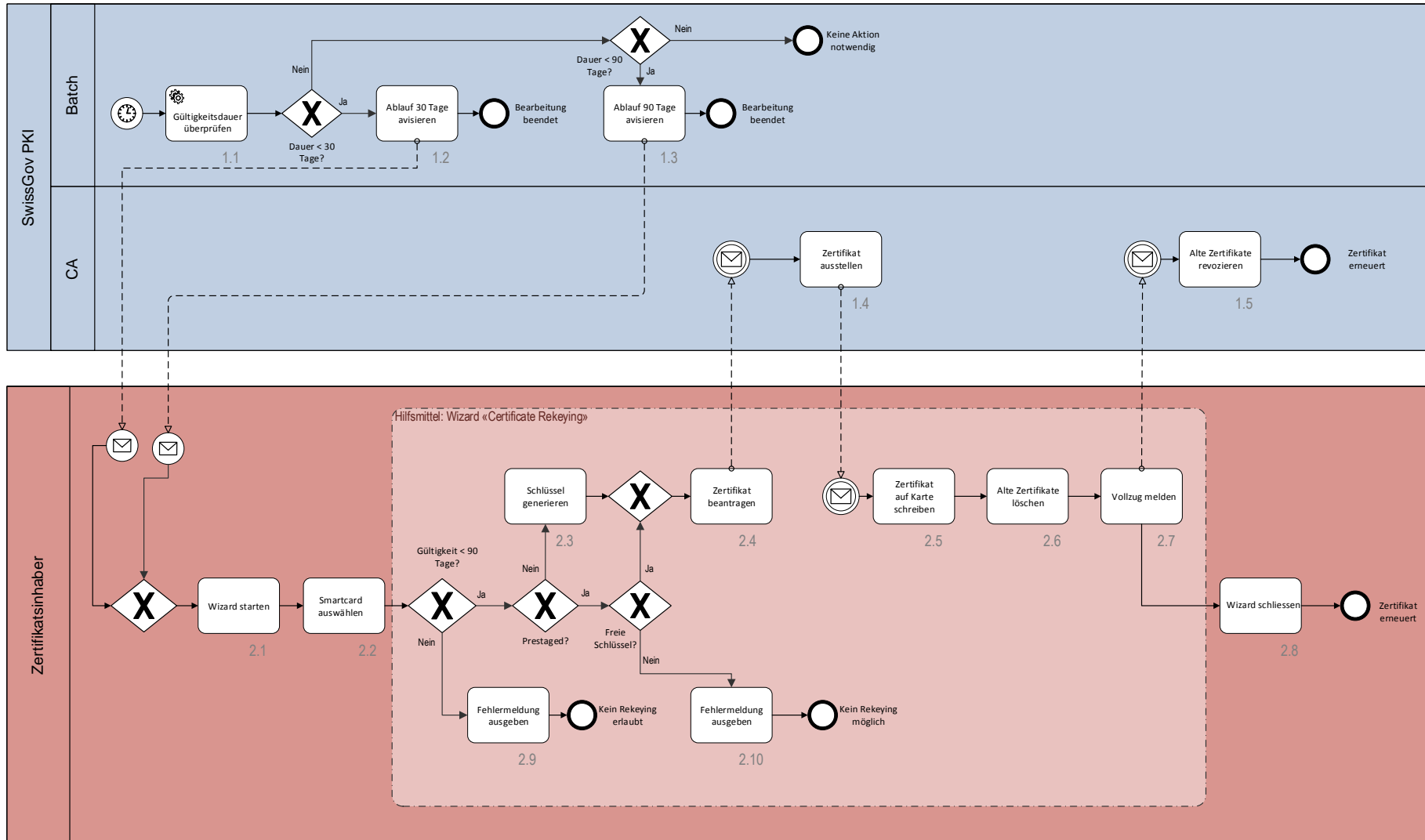
| Nr. | Element | Erläuterung | Verweis, Hilfsmittel |
|-----|---------|-------------|----------------------|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

2 Betriebsmodell (BM)

Prozessmodell (Ablaufdefinition)

SGPKI-CLB-M10: Certificate Rekeying

Kategorie: Betriebsmodell
Blatt: 1/1



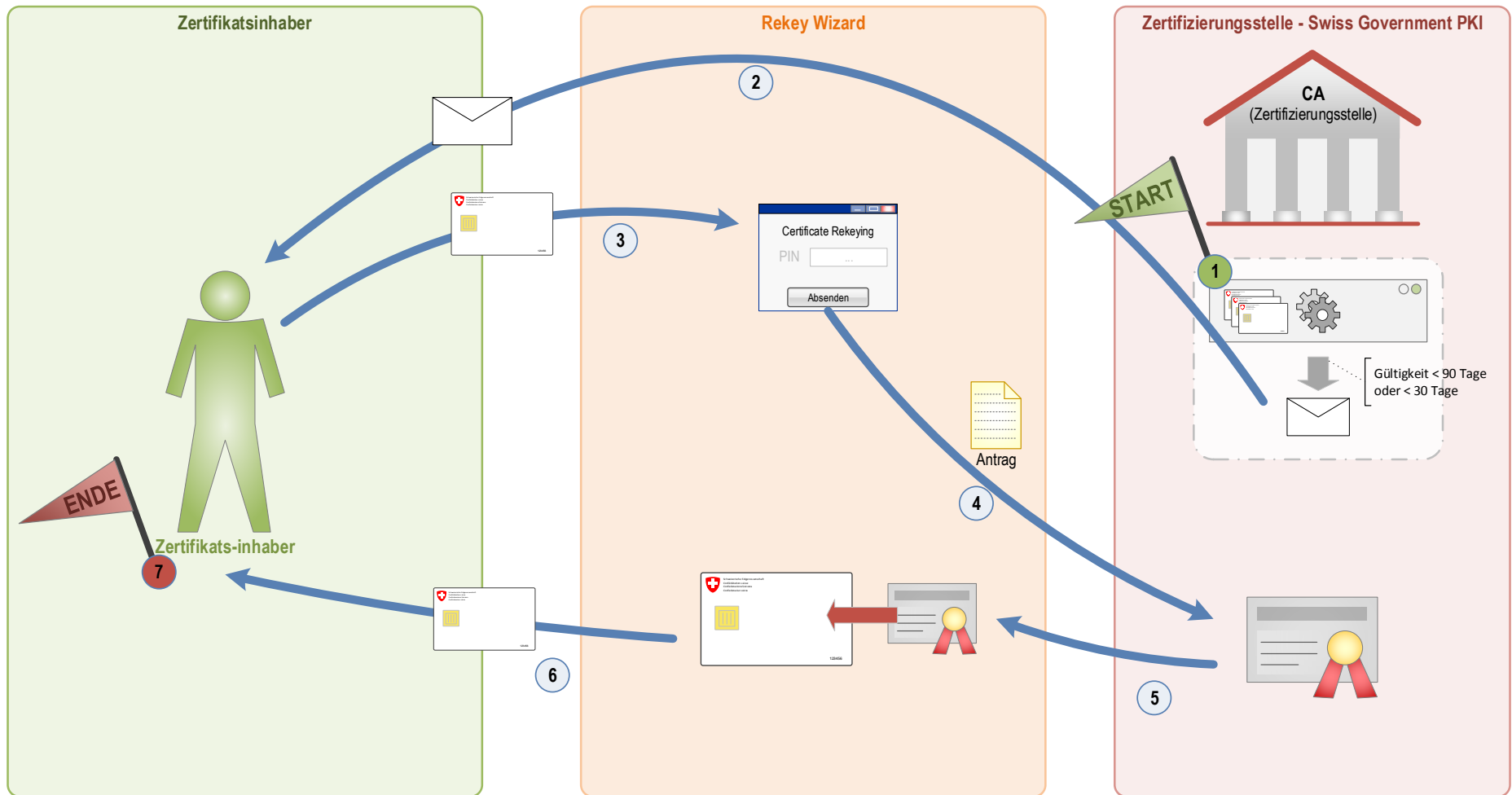
Erläuterungen

| Nr. | Element | Erläuterung | Verweis, Hilfsmittel |
|-----|----------|--|----------------------|
| 1 | 1.2, 1.3 | Der Zertifikatsinhaber wird vom zentralen System 90 und 30 Tage vor Ablauf des Zertifikats per Mail auf diesen Umstand hingewiesen | |
| 2 | 2.1 | Der Wizard wird als Schale 1 Produkt verteilt und ist somit auf jeder Arbeitsstation des Bundes installiert. | |
| 3 | 2.9 | Eine Erneuerung ist erst 90 Tage vor Ablauf der Zertifikate möglich | |
| 4 | 2.10 | Prestaged Smartcards besitzen 3 vollständige Sätze von 3 Schlüsselpaaren. Somit kann auf einer solchen Karte zwei Mal ein Renewal durchgeführt werden. Danach muss die Karte ersetzt werden. | |
| 5 | 2.6 | Die alten Zertifikate werden automatisch revoziert und von der Karte gelöscht. Lediglich die Verschlüsselungszertifikate bleiben weiterhin gespeichert. | |

3 Schaubild

Certificate Rekeying

ID: Zeichenblatt-1



Erläuterungen

| Nr. | Element | Erläuterung | Verweis, Hilfsmittel |
|-----|---------|---|----------------------|
| 1 | 1 | Das zentrale System informiert den Zertifikatinhaber jeweils 90 und 30 Tage vorher über den bevorstehenden Ablauf des gültigen Zertifikats und fordert ihn auf, das Zertifikat zu erneuern. | |
| 2 | 3 | Der Wizard steht auf jedem Bundesclient als Schale 1 Software zur Verfügung. | |