



TC TrustCenter

TC Enterprise ID

Leistungsbeschreibung

TC Enterprise ID
Version 1.8.1

Hamburg, Germany
Juli 2011

Geschäftsführung
Austin McCabe
Kristen Laubscher

HRB 96168 AG Hamburg
Ust.-ID-Nr. DE245979558

Bankverbindung
Bank of America
BLZ 50010900
Kto.-Nr. 9160016

IBAN DE14 5001 0900 0019 1600 16
BIC BOFADEFX

Sonninstraße 24-28
20097 Hamburg, Germany

Postfach 10 60 49
20041 Hamburg, Germany

Phone: +49 (0)40 / 80 80 26-0

Fax: +49 (0)40 / 80 80 26-1 26

<http://www.trustcenter.de>

Dieses Dokument ist urheberrechtlich geschützt. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung von TC TrustCenter unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Verbreitungen, Übersetzungen oder die Verwendung in elektronischen Systemen. Ausgenommen hiervon sind das Kopieren und der Ausdruck zum eigenen Gebrauch.

Alle Informationen in diesem Dokument wurden mit größter Sorgfalt erstellt. Weder TC TrustCenter noch der Autor können jedoch für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Dokumentes stehen.

„TC TrustCenter“, das TC TrustCenter-Logo, „Ident Point“, „TC PKI“ und „TC Info Line“ sind eingetragene Marken der TC TrustCenter GmbH.

Alle in diesem Dokument verwendeten, aber hier nicht genannten Marken- oder Produktnamen sind Marken oder Warenzeichen der entsprechenden Inhaber.

Copyright © 2011 TC TrustCenter GmbH

Alle Rechte vorbehalten.

All rights reserved. No information or images, fully or partially, in any form or by any means, may be reproduced, copied, duplicated, published or used in electronic systems or translations without the prior written consent of TC TrustCenter. This represents a crime, excluding printing and duplicating for one's own use.

All information in this document is compiled with great care. Neither TC TrustCenter nor the author are liable for any damages or disservice, that are in connection with the use of this document.

„TC TrustCenter“, the TC TrustCenter logo, „Ident Point“, „TC PKI“ and „TC Info Line“ are registered trademarks of the TC TrustCenter GmbH.

All brands, product names and trademarks used in this document, but not listed above, are trademarks or service marks of the respective owners.

Copyright © 2011 TC TrustCenter GmbH

Inhaltsverzeichnis

1	Web-basierte Registrierungsstelle (RA)	5
2	Verwalten von Benutzern	6
2.1	Benutzer hinzufügen	6
2.1.1	Benutzerrollen	7
2.1.2	Benutzergruppen verwalten	11
2.2	Benutzer suchen, ändern, löschen oder Benutzerkonten deaktivieren	12
3	Verwalten von Zertifikaten	14
3.1	Gültigkeitsdauer von Zertifikaten	14
3.2	Zertifikatsanzahl	14
3.3	PIN Verfahren	14
3.4	Schlüsselerzeugungrichtlinien	15
3.5	Schlüsselbereitsteller	16
3.6	Produktoptionen	16
3.7	Zertifikate anfordern	17
3.7.1	Ausstellung nicht wiederherstellbarer Benutzerzertifikate für „Basisbenutzer“	17
3.7.2	Ausstellung wiederherstellbarer Benutzerzertifikate für „Basisbenutzer“	19
3.7.3	Ausstellung nicht wiederherstellbarer Benutzerzertifikate für „Privilegierte Benutzer“	20
3.7.4	Ausstellung wiederherstellbarer Benutzerzertifikate für „Privilegierte Benutzer“	21
3.7.5	Anonyme Beantragung von Zertifikaten	23
3.8	Initiieren von Zertifikatsanträgen für andere Benutzer	23
3.8.1	Zertifikatseinladungen nicht wiederherstellbarer Zertifikate im Einzelverfahren	24
3.8.2	Zertifikatseinladungen wiederherstellbarer Zertifikate im Einzelverfahren	25
3.8.3	Zertifikatseinladungen nicht wiederherstellbarer Zertifikate im Batchverfahren	26
3.8.4	Zertifikatseinladungen wiederherstellbarer Zertifikate im Batchverfahren	27
3.9	Sperren, Suspendieren oder Desuspendieren von Zertifikaten sowie Initiieren von Key Recovery	27
3.9.1	Sperren und Suspendieren von Zertifikaten	28
3.9.2	Desuspendieren von Zertifikaten	30
3.9.3	Key Recovery	30
3.10	Key Escrow	31
3.11	Zertifikatsbesitzer wechseln	33
3.12	Überprüfen der SSL Server Installation	34
4	Berichte	35
4.1	SLA Reports	35
4.2	Aktivitätsberichte	35
4.3	Zertifikatsberichte	35
4.4	Auditberichte	36
5	Konfiguration	37
5.1	Einstellungen	37
5.2	„Affiliates“	38
5.3	Pre-Vetted Domains	40
5.4	„Verträge“	40



5.5	E-Mail-Vorlagen	41
6	Verzeichnisdienste	42
6.1	LDAP Service	42
6.2	LDAP Replikation	43
6.3	Validierungsdienst	43
7	Beantragung über SCEP	45
8	Beantragung über CMP	46
9	AutoEnrollment	48
9.1	Beantragen von Zertifikaten mittels Auto Enrollment	49
9.1.1	Schlüsselarchivierung (Key Archiving)	50
9.1.2	Certificate Templates for AutoEnrollment	50
10	Zertifikatsprofile	56
10.1	Zertifikatshierarchie	56
10.2	Zertifikatsprodukte	57
11	Service Levels	60
11.1	Verletzung von SLA-Werten	63
11.1.1	Unangekündigte Unterbrechungen	63
12	Glossar	64
13	Abbildungsverzeichnis	69

Leistungsbeschreibung TC Enterprise ID

In diesem Dokument sind die Eigenschaften von TC Enterprise ID beschrieben.

1 Web-basierte Registrierungsstelle (RA)

Das TC Enterprise ID Web-Portal stellt alle für die Administration benötigten Funktionen bereit. Die Benutzer und *Administratoren* können das Web-Portal zum Beantragen und Verwalten der Zertifikate über den gesamten Lebenszyklus hinweg nutzen.

Alle für die Ausführung der nachfolgend beschriebenen Prozesse benötigten technischen Infrastrukturkomponenten werden im Hochsicherheits-Rechenzentrum von TC TrustCenter betrieben. Die Installation von zusätzlicher Software durch *Administratoren* und Benutzer ist generell nicht notwendig. Sollen die mit TC Enterprise ID verwalteten Zertifikate auf Chipkarten oder USB-Tokens gespeichert werden, so müssen die dazu benötigten Treiber lokal installiert werden.

Abbildung 1 Architekturübersicht zeigt eine schematische Übersicht der Architektur und der involvierten Entitäten.

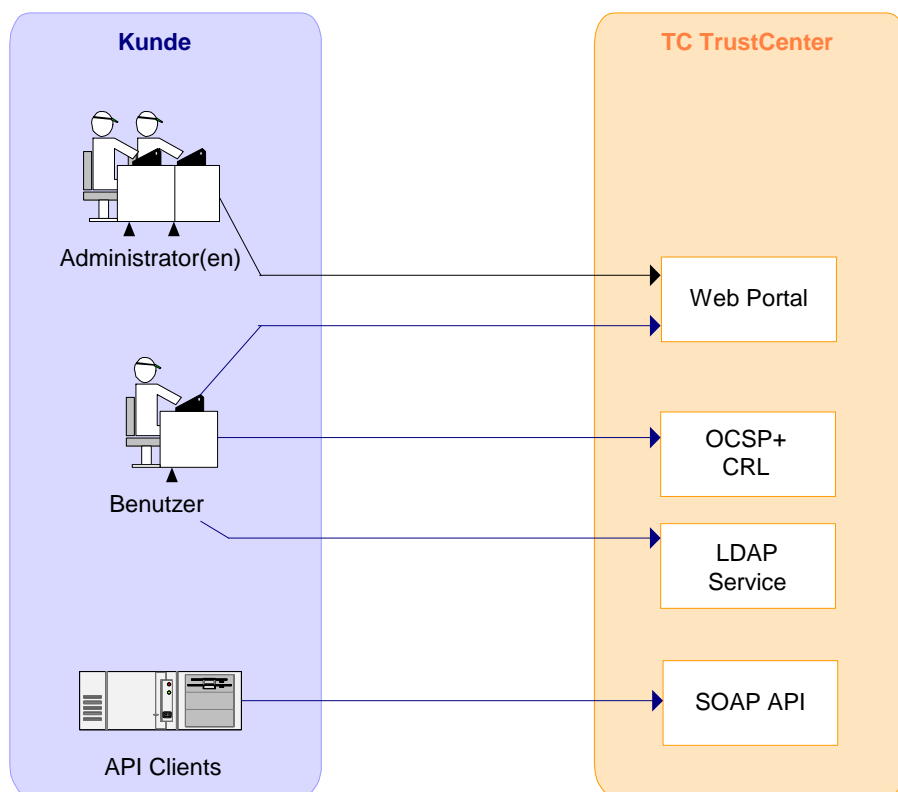


Abbildung 1 Architekturübersicht

2 Verwalten von Benutzern

Nachfolgend werden alle Personen, die ein Zertifikat aus TC Enterprise ID erhalten bzw. die das Web-Portal zum Beantragen von Zertifikaten bzw. zum Annehmen von Zertifikatseinladungen und zum Sperren, Suspendieren, Desuspendieren sowie zum Initiieren von Key-Recovery nutzen, als Benutzer bezeichnet – unabhängig von ihrer konkreten Rolle.


Das Web-Portal unterstützt die folgenden Funktionen zur Benutzerverwaltung:

1. Benutzer hinzufügen
2. Benutzer suchen, ändern oder löschen

Benutzer müssen im Web-Portal eingerichtet werden, bevor sie es nutzen können.

Benutzer können Gruppen zugewiesen werden. Dadurch wird ihre Verwaltung vereinfacht (siehe Abschnitt 2.1.2).

2.1 Benutzer hinzufügen

Benötigte Rolle	„PKI Superadministrator“, „PKI Administrator“ oder „Registration Officer“
Voraussetzungen	Keine
Formale Anforderungen	<ul style="list-style-type: none"> • Die Identität neuer Benutzer muss geprüft werden. • Vorname und Nachname müssen gemäß Personalausweis eingetragen werden. • Die Identifizierung der Benutzer muss gemäß der jeweiligen Zertifizierungsrichtlinien erfolgen..
Implizite Aktionen	Der neue Benutzer erhält eine automatisch generierte E-Mail mit den zum Anmelden am Web-Portal benötigten Daten (Benutzername und Passwort).
Benutzeroberfläche	

Jeder Benutzer ist einem Unternehmen bzw. „Affiliate“ zugeordnet. Die Daten für Organisation, Land, Bundesland sowie Stadt werden entsprechend dieser Zuordnung in Zertifikate übernommen.

Das Web Portal kann so konfiguriert werden, dass die Verwendung von Privatadressen der Benutzer unterstützt wird.

Vor ihrer Verwendung müssen Unternehmen bzw. „Affiliates“ registriert und dem System bekanntgegeben werden. Das dazu benötigte Formular steht auf den TC TrustCenter Webseiten zum Download bereit.

Um die Zuordnung von Benutzern im TC Enterprise ID System und in den ggf. bereits bestehenden Benutzerkonten zu erleichtern, kann bei jedem Benutzer im Feld „Externe Referenznummer“ ein eindeutiges Zuordnungsmerkmal gespeichert werden, z.B. eine Mitarbeiternummer. Dieser Wert wird in die Benutzerzertifikate als „serialNumber“ im Antragstellernamen übernommen.

Benutzer können im Einzelverfahren oder im Batchverfahren hinzugefügt werden. Mittels Batchverfahren können die aus anderen IT-Systemen exportierten Benutzerlisten einfach übernommen werden. Die Qualität der Daten kann beim Batchverfahren deutlich besser sein als beim Einzelverfahren (weniger Schreibfehler).

Nach dem Hinzufügen eines Benutzers erhält dieser eine E-Mail mit den Zugangsdaten für das Web-Portal zugeschickt.

Hinweis: Für jedes Produkt kann getrennt das Verfahren der bei der Ausstellung und Wiederherstellung von Zertifikaten benötigten PINs ausgewählt werden. Ist das *ePIN*-Verfahren (siehe Abschnitt 3.3) gewählt, wird die PIN standardmäßig als E-Mail ausgeliefert. Soll die PIN als SMS ausgeliefert werden, kann dies beim Hinzufügen des Benutzers ausgewählt oder über „Benutzer ändern“ eingestellt werden.

Hinweis: Benutzer müssen gemäß der TC TrustCenter [Zertifizierungsrichtlinien](#) identifiziert werden. Typischerweise können Mitarbeiter gemäß Registrierungsklasse Class 2 und externe Partner gemäß Class 1 identifiziert werden. Die Registrierungsklasse muss beim Anlegen eines Benutzers korrekt angegeben werden.

2.1.1 Benutzerrollen

Jeder Benutzer hat mindestens eine, evtl. auch mehrere Rollen. Die Rollen sind in der nachfolgenden Tabelle aufgeführt und erklärt.

Um Zertifikate beantragen zu können, muss ein Benutzer mindestens eine der folgenden Rollen besitzen:

- „Basisbenutzer“
- „Privilegierter Benutzer“
- „PKI Administrator“

Die Officer-Rollen sollten üblicherweise in Kombination mit dem „Privilegierten Benutzer“ oder „Basisbenutzer“ vergeben werden, um das Beantragen von eigenen Zertifikaten zu ermöglichen.

Die Rolle „PKI Superadministrator“ wird immer in Kombination mit der Rolle „PKI Administrator“ vergeben.



Rollenname	Beschreibung
<p>„PKI Superadministrator“ Diese Rolle kann nur durch TC TrustCenter zugewiesen werden. Ein spezielles Training ist erforderlich.</p>	<ul style="list-style-type: none">• Zertifikatseinladung annehmen.• Benutzer hinzufügen, suchen, ändern oder löschen. Dabei kann er auch die Rollen „PKI Administrator“, „Registration Officer“, „Enrollment Officer“, „Revocation Officer“, „Unsuspendation Officer“, „Key Recovery Officer“, „Privilegierter Benutzer“, „Basisbenutzer“, „Externer Benutzer“ und „NoLogin Benutzer“ zuweisen.• Benutzerkonten deaktivieren.
<p>„PKI Administrator“ Diese Rolle kann nur durch den „PKI Superadministrator“ bzw. TC TrustCenter zugewiesen werden.</p>	<ul style="list-style-type: none">• Zertifikatseinladung annehmen.• Benutzer hinzufügen, suchen, ändern oder löschen (bis zu Registrierungsklasse Class 2). Der „PKI Administrator“ kann nur die Rollen „Revocation Officer“, „Unsuspendation Officer“ und „Key Recovery Officer“, „Privilegierter Benutzer“, „Basisbenutzer“, „Externer Benutzer“ und „NoLogin Benutzer“ vergeben bzw. entziehen.• Benutzerkonten deaktivieren.• Beantragen von Zertifikaten ohne benötigte Freischaltung durch einen „PKI Administrator“ oder einen „Enrollment Officer“.• Erzeugen von Zertifikatseinladungen für beliebige Benutzer sowie Freischalten von Anträgen von beliebigen Benutzern.• Sperren oder Suspendieren von beliebigen Zertifikaten• Desuspendieren von beliebigen Zertifikaten• Initiieren von Key Recovery für beliebige (wiederherstellbare) Zertifikate• Anträge suchen• Konfiguration des Web-Portals anpassen• E-Mail Vorlagen anpassen• Zertifikatsbericht erstellen• Aktivitätsbericht erstellen• Auditbericht einsehen• Benutzergruppen verwalten• <i>Zertifikatsbesitzer</i> wechseln• Ausführen des TC SSL Certificate Discovery Tools

Rollenname	Beschreibung
„Key Escrow Administrator (Request)“ Diese Rolle kann nur durch TC TrustCenter vergeben werden.	<ul style="list-style-type: none"> • Initiieren von <i>Key Escrow</i>
„Key Escrow Administrator (PSE)“ Diese Rolle kann nur durch TC TrustCenter vergeben werden.	<ul style="list-style-type: none"> • Hat das Recht im Rahmen von <i>Key Escrow</i> über die API auf die <i>PKCS#12 PSE</i> zuzugreifen.
„PIN Brief Administrator“ Diese Rolle kann nur durch TC TrustCenter vergeben werden.	<ul style="list-style-type: none"> • Drucken von PIN Briefen
„Registration Officer“ (Delegierte Rolle) Diese Rolle kann nur durch den „PKI Superadministrator“ bzw. TC TrustCenter zugewiesen werden.	<ul style="list-style-type: none"> • Zertifikatseinladung annehmen. • Benutzer hinzufügen, suchen, ändern oder löschen (nur „NoLogin Benutzer“, „Externe Benutzer“, „Basisbenutzer“ und „Privilegierte Benutzer“) • Benutzerkonten deaktivieren. • Anträge suchen • Zertifikatsbericht erstellen • Aktivitätsbericht erstellen • Benutzergruppen verwalten • <i>Zertifikatsbesitzer</i> wechseln • Konfiguration des Web-Portals anpassen (nur Einstellungen.)
„Enrollment Officer“ (Delegierte Rolle) Diese Rolle kann nur durch den „PKI Superadministrator“ bzw. TC TrustCenter zugewiesen werden.	<ul style="list-style-type: none"> • Zertifikatseinladung annehmen. • Benutzer suchen. • Erzeugen von Zertifikatseinladungen für beliebige Benutzer sowie Freischalten von Anträgen von beliebigen Benutzern. • Anträge suchen • Konfiguration des Web-Portals anpassen (nur Pre-Vetted Domains und Produktkonfiguration) • Benutzerkonten deaktivieren. • Aktivitätsbericht erstellen • Ausführen des TC SSL Certificate Discovery Tools
„Enrollment Agent“ (Delegierte Rolle) Diese Rolle kann nur durch den „PKI Superadministrator“ bzw. TC TrustCenter zugewiesen werden.	<ul style="list-style-type: none"> • Personalisierung von Chipkarten oder anderen kryptografischen Token für den Benutzer.
„Revocation Officer“ (Delegierte Rolle) Diese Rolle kann nur durch den „PKI Superadministrator“ oder den „PKI Administrator“ bzw. TC TrustCenter	<ul style="list-style-type: none"> • Zertifikatseinladung annehmen. • Benutzer suchen. • Sperren oder Suspendieren von



Rollenname	Beschreibung
zugewiesen werden.	<ul style="list-style-type: none">beliebigen Zertifikaten• Anträge suchen• Zertifikatsbericht erstellen• Aktivitätsbericht erstellen• Konfiguration des Web-Portals einsehen
„Unsuspendation Officer“ (Delegierte Rolle) Diese Rolle kann nur durch den „PKI Superadministrator“ bzw. TC TrustCenter zugewiesen werden.	<ul style="list-style-type: none">• Zertifikatseinladung annehmen.• Benutzer suchen.• Desuspendieren von beliebigen Zertifikaten• Anträge suchen• Zertifikatsbericht erstellen• Aktivitätsbericht erstellen• Konfiguration des Web-Portals einsehen• Entsperren von Token
„Key Recovery Officer“ (Delegierte Rolle) Diese Rolle kann nur durch den „PKI Superadministrator“ bzw. TC TrustCenter zugewiesen werden.	<ul style="list-style-type: none">• Zertifikatseinladung annehmen.• Benutzer suchen.• Initiieren von Key Recovery für beliebige (wiederherstellbare) Zertifikate• Anträge suchen• Zertifikatsbericht erstellen• Aktivitätsbericht erstellen• Konfiguration des Web-Portals einsehen
„Privilegierter Benutzer“	<ul style="list-style-type: none">• Zertifikatseinladung annehmen.• Beantragen von Zertifikaten ohne benötigte Freischaltung durch einen „PKI Administrator“ oder einen „Enrollment Officer“. Für EV Zertifikate ist weiterhin eine Freischaltung notwendig.• Sperren oder Suspendieren von eigenen Zertifikaten• Initiieren von Key Recovery für eigene (wiederherstellbare) Zertifikate• Zertifikate innerhalb der eigenen Gruppe suchen• Konfiguration des Web-Portals einsehen• Eigene Anträge suchen
„Basisbenutzer“	<ul style="list-style-type: none">• Zertifikatseinladung annehmen.• Beantragen von Zertifikaten mit benötigter Freischaltung durch einen „PKI

Rollenname	Beschreibung
	Administrator“ oder „Enrollment Officer“ <ul style="list-style-type: none"> • Sperren oder Suspendieren von eigenen Zertifikaten • Initiieren von Key Recovery für eigene (wiederherstellbare) Zertifikate • Zertifikate innerhalb der eigenen Gruppe suchen • Konfiguration des Web-Portals einsehen • Eigene Anträge suchen
„Externer Benutzer“	<ul style="list-style-type: none"> • Zertifikatseinladung annehmen. • Sperren oder Suspendieren von eigenen Zertifikaten • Initiieren von Key Recovery für eigene (wiederherstellbare) Zertifikaten • Eigene Zertifikate suchen • Eigene Anträge suchen
„NoLogin Benutzer“	<ul style="list-style-type: none"> • Zertifikatseinladung annehmen.
„SCEP Benutzer“	<ul style="list-style-type: none"> • Dieser Benutzer ist der Besitzer aller anonym über <i>SCEP</i> beantragten Zertifikate • Diese Rolle darf mit keinen weiteren Rollen kombiniert werden.

Tabelle 1 Beschreibung der Rollen

Hinweis: Die nachfolgend als *Administrator* bezeichnete Rolle kann entweder ein „PKI Superadministrator“, ein „PKI Administrator“ oder eine beliebige delegierte Rolle sein (siehe auch Glossar).

Beim Hinzufügen von Benutzern muss die initiale Rolle angegeben werden (Standardwert ist „Basisbenutzer“). Die Rollen eines Benutzers können jederzeit geändert werden.

Hinweis: Ein 4-Augen-Prinzip bei der Vergabe von Zertifikaten ist durch „Registration Officer“ (Benutzer anlegen) und „Enrollment Officer“ (Zertifikatsantrag freischalten) realisierbar.

Hinweis: Aufgrund der umfangreichen Befugnisse wird für die Vergabe der Rolle „PKI Superadministrator“ ein spezielles Training benötigt.

2.1.2 Benutzergruppen verwalten


Jeder Benutzer kann zu einer Gruppe gehören. Die Suche nach Benutzern kann anhand der Benutzergruppe erfolgen. Die Benutzergruppe ist daher eine weitere Möglichkeit zur Strukturierung der Daten.

Benutzer mit der Rolle „Privilegierter Benutzer“ oder „Basisbenutzer“ können nur Zertifikate suchen und einsehen, die ihrer Gruppe zugeordnet sind. Ist der Benutzer keiner Gruppe zugeordnet, so kann er die Zertifikate aller Gruppen suchen und einsehen.

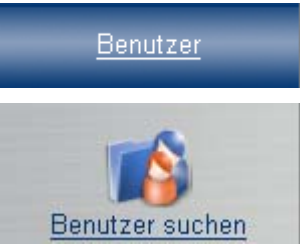
Delegierte Rollen („Registration Officer“, „Enrollment Officer“, „Revocation Officer“, „Unsuspendation Officer“ und „Key Recovery Officer“) können nur Benutzer anlagen bzw. bearbeiten, die auch zu ihrer Gruppe gehören. Wenn ein Benutzer mit einer delegierten Rolle keiner Gruppe angehört, so darf er für Benutzer *beliebiger Gruppen* tätig sein. Durch Zuweisung zu einer Gruppe kann die Befugnis von delegierten Rollen auf diese Gruppe eingeschränkt werden.

Die *Administratoren* (z.B. „PKI Superadministrator“ und „PKI Administrator“) können immer gruppenübergreifend tätig sein.

Benutzer können nur zu einer oder keiner Gruppe gehören, nicht zu mehreren.

Benötigte Rolle	„PKI Superadministrator“, „PKI Administrator“ oder „Registration Officer“
Voraussetzungen	Keine
Formale Anforderungen	Keine
Implizite Aktionen	Die Mitglieder einer zu löschenden Gruppe werden automatisch aus dieser Gruppe entfernt. Sie gehören nach dem Löschvorgang zu keiner Gruppe.
Benutzeroberfläche	

2.2 Benutzer suchen, ändern, löschen oder Benutzerkonten deaktivieren

Benötigte Rolle	„PKI Superadministrator“, „PKI Administrator“ oder „Registration Officer“
Voraussetzungen	Keine
Formale Anforderungen	Für das Ändern von Benutzern gelten dieselben formalen Anforderungen wie für das Hinzufügen von Benutzern.
Implizite Aktionen	Keine
Benutzeroberfläche	



Hinweis: Benutzerkonten können deaktiviert oder aktiviert werden. Eine Anmeldung ist nicht möglich, wenn das Benutzerkonto deaktiviert ist. Die Gültigkeit von Zertifikaten bleibt davon unberührt.

Hinweis: Vor dem Löschen eines Benutzers müssen alle *Team- und Applikationszertifikate* für die er als *Zertifikatsbesitzer* eingetragen ist einem anderen *Zertifikatsbesitzer* zugeordnet werden.

Hinweis: Beim Löschen eines Benutzers werden die ihm zugeordneten Benutzerzertifikate automatisch gesperrt.

Hinweis: Für jedes Produkt kann getrennt das Verfahren der bei der Ausstellung und Wiederherstellung von Zertifikaten benötigten PINs ausgewählt werden. Ist das *ePIN-Verfahren* (siehe Abschnitt 3.3) gewählt, wird die PIN standardmäßig als E-Mail ausgeliefert. Soll die PIN als SMS ausgeliefert werden, kann dies beim Hinzufügen des Benutzers ausgewählt oder über „Benutzer ändern“ eingestellt werden.

3 Verwalten von Zertifikaten

Das Web-Portal unterstützt die folgenden Verwaltungsaufgaben für Zertifikate:

1. Zertifikat anfordern
2. Zertifikatseinladungen erzeugen
3. Sperren, Suspendieren oder Desuspendieren sowie Key Recovery oder *Key Escrow* initiieren

Der Prozess „Zertifikat anfordern“ wird vom späteren *Zertifikatsbesitzer* ausgelöst.

Eine Zertifikatseinladung wird von einem *Administrator* angelegt. Die dabei benötigten Daten werden entweder (a) aus den hinterlegten Benutzerdaten des späteren *Zertifikatsinhabers* genommen oder (b) müssen durch den *Administrator* beim Anlegen der Zertifikatseinladung eingegeben werden.

Die Prozesse zum Sperren, Suspendieren von Zertifikaten sowie zum Initiieren von Key Recovery können von einem *Administrator* oder dem *Zertifikatsbesitzer* ausgelöst werden.

Alle Verwaltungstätigkeiten für Zertifikate müssen entsprechend der jeweiligen Zertifizierungsrichtlinie (CPD) und des jeweiligen Certificate Practice Statement (CPS) durchgeführt werden. Für alle unterhalb einer TC TrustCenter CA ausgestellten Zertifikate sind die TC TrustCenter **Zertifizierungsrichtlinien** und **CPS** maßgeblich.

3.1 Gültigkeitsdauer von Zertifikaten

Zertifikate sind üblicherweise zwischen 1-3 Jahren gültig. Die konkrete Dauer wird beim Auswählen des Zertifikatsproduktes (siehe Abschnitt 10.2) festgelegt.

Beim Verlängern von SSL Zertifikaten wird die Restlaufzeit (aber nicht mehr als 90 Tage) zur Laufzeit des neuen Zertifikates hinzuaddiert, wenn das aktuelle Zertifikat (mit gleichem CommonName) von TC TrustCenter oder einem der definierten Mitbewerber ausgestellt wurde.

3.2 Zertifikatsanzahl

Die mittlere Anzahl von Zertifikaten pro Benutzer kann 1, 2 oder 3 betragen. Sie ist im Vertrag festgelegt. Die vordefinierten Zertifikatsprodukte unterstützen eine sinnvolle Aufteilung der Zertifikatszwecke (siehe Abschnitt 10.2) für unterschiedliche Zertifikatszahlen pro Benutzer.

3.3 PIN Verfahren

Für jedes Produkt kann getrennt das Verfahren der bei der Ausstellung und Wiederherstellung von Zertifikaten benötigten PINs ausgewählt werden.

Standardmäßig werden die PINs von TC TrustCenter als E-Mail oder als SMS an den Benutzer ausgeliefert (*ePIN*-Verfahren).

Hinweis: Für die Auslieferung von PINs als SMS werden nicht alle weltweit verfügbaren Mobilfunknetze unterstützt. Insbesondere in den USA werden nur sehr wenige Mobilfunknetze unterstützt. Weitere Details über unterstützte Mobilfunknetze können Sie über unseren Support erfahren.



Alternativ kann durch den „PKI Administrator“ pro Zertifikatsprodukt das Verfahren *Externe PIN* oder *PIN Brief* gewählt werden. Im Fall der *Externen PIN* muss die PIN für jeden Antrag vom *Administrator* vorgegeben werden. Der *Administrator* ist ebenfalls für das Aushändigen der PIN an den Benutzer zuständig. Der „PIN Brief Administrator“ ist für das Drucken von PIN Briefen zuständig. Das PDF Dokument mit den PIN Brieftexten wird automatisch anhand der im Web Portal eingestellten Vorlage erzeugt.

Hinweis: Das System liefert keine *Externen PINs* aus. Die Länge von *Externen PINs* darf 125 Zeichen nicht überschreiten. Es sind nur druckbare ASCII Zeichen (mit den ASCII Codes 32 – 126) erlaubt.

Ist das *ePIN*-Verfahren gewählt, wird die PIN standardmäßig als E-Mail ausgeliefert. Soll die PIN als SMS ausgeliefert werden, kann dies beim Hinzufügen des Benutzers ausgewählt oder über „Benutzer ändern“ eingestellt werden (siehe auch Abschnitte 2.1. und 2.2).

Siehe auch Abschnitt 5.4 zur Einstellung von *Externe PIN* für ein Zertifikatsprodukt.

Hinweis: Bei Verwendung des Verfahrens *Externe PIN* ist Batch Key Recovery nicht möglich.

Hinweis: Das Verfahren *PIN Brief* kann nicht im Zusammenhang mit Zertifikatseinladungen (siehe Abschnitt 3.8) genutzt werden.

Hinweis: Beim Wiederherstellen von Zertifikaten (Key Recovery) wird immer dasjenige PIN-Verfahren genutzt welches auch bei der Beantragung für das jeweilige Produkt eingestellt war (entweder *ePIN* oder *Externe PIN*). Ein mittels *ePIN* beantragtes Zertifikat wird auch mittels *ePIN* wiederhergestellt – selbst wenn für Neubeantragungen des Produktes zwischenzeitlich auf *Externe PIN* umgestellt wurde.

Bei den nachfolgend beschriebenen Prozessen ist das *ePIN*-Verfahren zugrundegelegt.

3.4 Schlüsselerzeugungrichtlinien

Die Schlüsselerzeugungrichtlinien können selbst definiert werden. Die folgenden Parameter können vorgegeben werden:

1. Minimale Schlüssellänge
2. Privater Schlüssel exportierbar
3. Privaten Schlüssel schützen (d.h. der Benutzer wird vor jeder Verwendung des privaten Schlüssels informiert).
4. Zulässige CSPs. Hier kann eine Liste von Cryptographic Service Provider (CSP)-Namen für die Schlüsselerzeugung vorgegeben werden..
5. Nur MSIE. Wenn aktiviert wird nur der Microsoft Internet Explorer für die Schlüsselgenerierung zugelassen.

Hinweis: Nur der Microsoft Internet Explorer unterstützt eine detaillierte Vorgabe der Schlüsselerzeugungrichtlinie. Bei der Verwendung anderer Web Browser kann nur die minimale Schlüssellänge vorgegeben werden.

Hinweis: Für wiederherstellbare Zertifikate (wenn das Zertifikat mit dem privaten Schlüssel als *PKCS#12 PSE* ausgeliefert wird) ist nur die minimale Schlüssellänge relevant.


Hinweis: Abhängig vom Zertifikatsprodukt können einige der Parameter bereits durch TC TrustCenter vordefiniert sein. Diese Parameter können dann nicht geändert werden.

3.5 Schlüsselbereitsteller

Standardmäßig werden die öffentlichen Schlüssel durch den Antragsteller bereitgestellt (z.B. durch den Web Browser). Für einige Produkte kann der PKI Administrator den Schlüsselbereitsteller alternativ auch auf den „Enrollment Agent“ ändern.

In diesem Fall muss der „Enrollment Agent“ mittels des TC PersoClients die öffentlichen Schlüssel für Anträge bereitstellen. Der TC PersoClient ist ein Tool zum Personalisieren von Chipkarten oder USB Token. Der „Enrollment Agent“ muss sich mittels Zertifikat am Web Portal anmelden, um den TC PersoClient nutzen zu können (siehe Beschreibung der Anmelderichtlinie in Abschnitt 5.1).

Hinweis: Zur Nutzung des TC PersoClients muss für das betreffende Produkt das PIN Verfahren auf *PIN Brief* sowie die Schlüsselerzeugungsmethode auf „SMARTCARD“ gesetzt sein. Die Schlüsselerzeugungsmethode kann nicht vom „PKI Administrator“, sondern nur von TC TrustCenter geändert werden.

Hinweis: Falls mehrere Zertifikate auf eine Chipkarte personalisiert werden sollen, so muss dieses in einem Schritt erfolgen, d.h. die betreffenden Anträge müssen markiert und die Personalisierung muss mittels Klick auf den Button  gestartet werden.

Hinweis: Der TC PersoClient unterstützt keine Personalisierung von wiederherstellbaren Zertifikaten (solche Zertifikate enthalten „recoverable“ im Produktnamen).

Hinweis: Der TC PersoClient ist eine ClickOnce Applikation und unterstützt nur den Microsoft Internet Explorer unter Windows.

3.6 Produktoptionen

Für einige Produkte (z.B. SSL Zertifikate) können zusätzliche Produktoptionen (z.B. Anzahl der Serverlizenzen oder Anzahl von zusätzlichen Servernamen) angegeben werden.

Der Antragsteller muss diese Optionen beim Beantragen dieser Produkte auswählen.

Hinweis: Die Wahl der Produktoptionen kann sich auf den Preis auswirken.


3.7 Zertifikate anfordern

Ein Benutzer kann aktiv ein Zertifikat anfordern, er muss dabei nicht auf eine Zertifikatseinladung warten. Diese Funktion kann sowohl für das Anfordern von Benutzerzertifikaten als auch für das Anfordern von *Team- bzw. Applikationszertifikaten* genutzt werden. Der Ablauf für *Team- bzw. Applikationszertifikate* ist vergleichbar mit dem für Benutzerzertifikate. Der entscheidende Unterschied liegt in der Methode zur Schlüsselgenerierung. Für *Applikationszertifikate* muss ein *PKCS#10* Request hochgeladen werden. Im Falle von Benutzerzertifikaten wird das Schlüsselpaar durch den Web-Browser erzeugt.

Hinweis: Beim Anfordern von QuickSSL Premium Zertifikaten (siehe Abschnitt 7) muss eine zusätzliche E-Mail Adresse für eine Approval-E-Mail angegeben werden. Diese E-Mail Adresse kann nicht frei gewählt werden, sondern muss aus der Liste der Vorschläge ausgewählt werden.

Bei Benutzerzertifikaten sind *Zertifikatsinhaber* und *Zertifikatsbesitzer* identisch. Bei Applikationszertifikaten ist der *Zertifikatsinhaber* die Applikation selbst, der *Zertifikatsbesitzer* ist in der Regel der *Administrator* der Applikation.

Alle nachfolgend aufgeführten Abläufe beschreiben das Anfordern von Benutzerzertifikaten (siehe Abbildungen). Die unter 3.7.3 und 3.7.4 genannten Prozesse sind vergleichbar mit den entsprechenden Prozessen für Zertifikate für *Administratoren*.

Benötigte Rolle	„PKI Administrator“, „Privilegierter Benutzer“ oder „Basisbenutzer“
Voraussetzungen	Der Benutzer muss bereits im Web-Portal eingerichtet sein.
Formale Anforderungen	Keine
Implizite Aktionen	Im Falle der Rolle „Basisbenutzer“ muss der Antrag durch einen „PKI Administrator“ oder „Registration Officer“ freigegeben werden.
Benutzeroberfläche	

3.7.1 Ausstellung nicht wiederherstellbarer Benutzerzertifikate für „Basisbenutzer“

Schritt 1 und 2 sind vorbereitende Tätigkeiten, sie müssen für weitere Zertifikate nicht wiederholt werden.

1. Der „PKI Administrator“ oder „Registration Officer“ muss den Benutzer im Web-Portal anlegen. Dabei muss die Identität des Benutzers geprüft worden sein. Die Rolle wird auf „Basisbenutzer“ gesetzt.

- Der Benutzer wird eine Benachrichtigungs-E-Mail mit seinen Zugangsdaten (Benutzername und Passwort) für das Web-Portal erhalten.

Hinweis: Der „PKI Administrator“ oder „Registration Officer“ kann die Benutzerdaten jederzeit korrigieren.

- Der Benutzer kann sich am Web-Portal anmelden und ein Zertifikat anfordern. Abhängig vom Zertifikatsprodukt müssen dabei ggf. noch einige Daten durch den Benutzer angegeben werden. Die Erzeugung des Schlüsselpaares gehört zu diesem Prozess.
- Der „PKI Administrator“ oder „Registration Officer“ wird über den auf Freischaltung wartenden Antrag informiert.
- Ein beliebiger „PKI Administrator“ oder „Enrollment Officer“ kann den Antrag freischalten (oder ablehnen).
- TC TrustCenter erzeugt das Zertifikat und schickt eine URL zum Herunterladen an den Benutzer. Da Zertifikate keine geheimen Daten beinhalten, ist diese URL nicht durch eine PIN geschützt.
- Der Benutzer installiert durch Klick auf den Link das Zertifikat. Für diesen Vorgang ist keine Anmeldung am Web-Portal erforderlich.

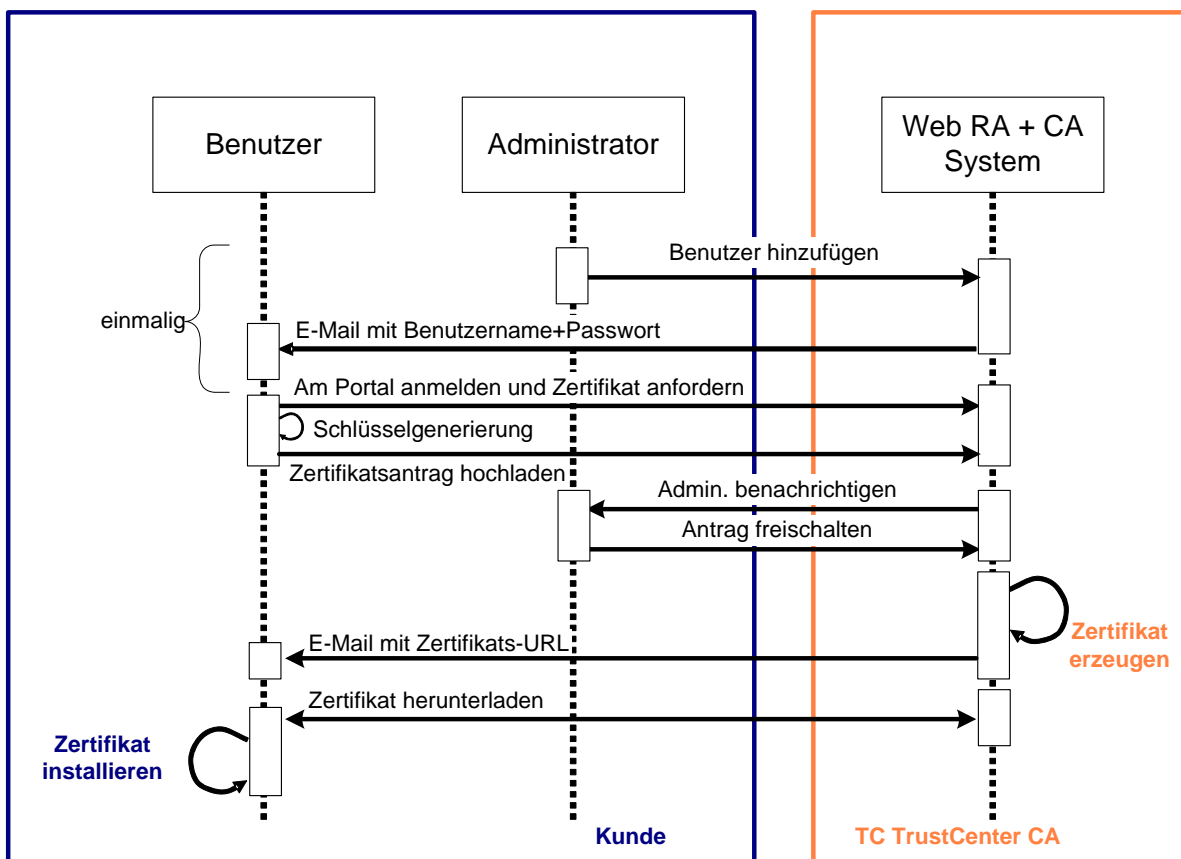


Abbildung 2 Antragsprozess nicht wiederherstellbarer Benutzerzertifikate für „Basisbenutzer“

Es können auch Chipkarten oder USB-Token zum Speichern der Zertifikate verwendet werden. In diesem Fall muss der zugehörige Cryptographic Service Provider (CSP) zur Schlüsselgenerierung ausgewählt bzw. die zugehörige *PKCS#11* Library im Web-Browser des Benutzers installiert werden. Die Liste der zulässigen CSPs kann durch eine Schlüsselerzeugungsrichtlinie vorgegeben werden, siehe Abschnitt 3.4).



3.7.2 Ausstellung wiederherstellbarer Benutzerzertifikate für „Basisbenutzer“

Schritt 1 und 2 sind vorbereitende Tätigkeiten, sie müssen für weitere Zertifikate nicht wiederholt werden.

1. Der „PKI Administrator“ oder „Registration Officer“ muss den Benutzer im Web-Portal anlegen. Dabei muss die Identität des Benutzers geprüft worden sein. Die Rolle wird auf „Basisbenutzer“ gesetzt.
2. Der Benutzer wird eine Benachrichtigungs-E-Mail mit seinen Zugangsdaten (Benutzername und Passwort) für das Web-Portal erhalten.

Hinweis: Der „PKI Administrator“ oder „Registration Officer“ kann die Benutzerdaten jederzeit korrigieren.

3. Der Benutzer kann sich am Web-Portal anmelden und ein Zertifikat anfordern. Abhängig vom Zertifikatsprodukt müssen dabei ggf. noch einige Daten durch den Benutzer angegeben werden.
4. Der „PKI Administrator“ oder „Registration Officer“ wird über den auf Freischaltung wartenden Antrag informiert.
5. Ein beliebiger „PKI Administrator“ oder „Enrollment Officer“ kann den Antrag freischalten (oder ablehnen).
6. TC TrustCenter erzeugt eine Einmal-PIN zum Schutz der *PKCS#12 PSE* gegen ungewünschten Zugriff und schickt sie an den Benutzer.
7. TC TrustCenter erzeugt das Schlüsselpaar und das Zertifikat (= Personal Security Environment (*PKCS#12 PSE*)).
8. TC TrustCenter schickt eine E-Mail mit der URL zum Herunterladen der *PKCS#12 PSE* an den Benutzer. Diese URL ist mit der Einmal-PIN geschützt.

Hinweis: Aus Sicherheitsgründen ist diese URL nur 30 Tage gültig und wird nach 3 Fehlversuchen bei der Einmal-PIN-Eingabe automatisch gesperrt. In diesem Fall kann durch Auslösen von Key Recovery ein neues Zeitfenster zur Installation der *PKCS#12 PSE* bereitgestellt werden.

9. Der Benutzer importiert die *PKCS#12 PSE* mit dem privaten Schlüssel und dem Zertifikat. Dabei muss die Einmal-PIN erneut eingegeben werden. Für diesen Vorgang ist keine Anmeldung am Web-Portal erforderlich.

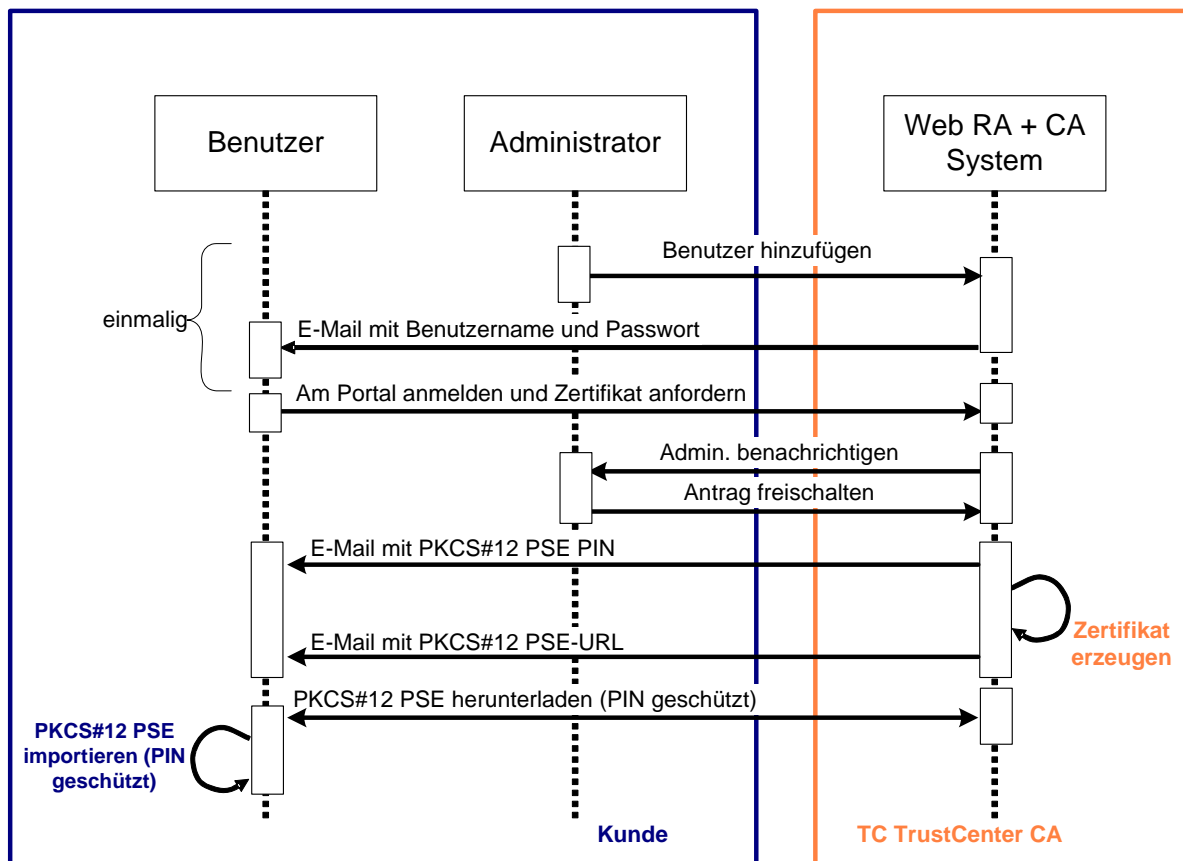


Abbildung 3 Antragsprozess wiederherstellbarer Benutzerzertifikate für „Basisbenutzer“

Es können auch Chipkarten oder USB-Token zum Speichern der Zertifikate verwendet werden. Bitte benutzen Sie in diesem Fall das zugehörige Programm zum Importieren der PKCS#12 PSE auf die Chipkarte.

3.7.3 Ausstellung nicht wiederherstellbarer Benutzerzertifikate für „Privilegierte Benutzer“

Schritt 1 und 2 sind vorbereitende Tätigkeiten, sie müssen für weitere Zertifikate nicht wiederholt werden.

1. Der „PKI Administrator“ oder „Registration Officer“ muss den Benutzer im Web-Portal anlegen. Dabei muss die Identität des Benutzers geprüft worden sein. Die Rolle wird auf „Basisbenutzer“ gesetzt.
2. Der Benutzer wird eine Benachrichtigungs-E-Mail mit seinen Zugangsdaten (Benutzernamen und Passwort) für das Web-Portal erhalten.

Hinweis: Der „PKI Administrator“ oder „Registration Officer“ kann die Benutzerdaten jederzeit korrigieren.

3. Der Benutzer kann sich am Web-Portal anmelden und ein Zertifikat anfordern. Abhängig vom Zertifikatsprodukt müssen dabei ggf. noch einige Daten durch den Benutzer angegeben werden. Die Erzeugung des Schlüsselpaares gehört zu diesem Prozess.
4. TC TrustCenter erzeugt das Zertifikat und schickt eine URL zum Herunterladen an den Benutzer. Da Zertifikate keine geheimen Daten beinhalten ist diese URL nicht durch eine PIN geschützt.
5. Der Benutzer installiert durch Klick auf den Link das Zertifikat. Für diesen Vorgang ist keine Anmeldung am Web-Portal erforderlich.

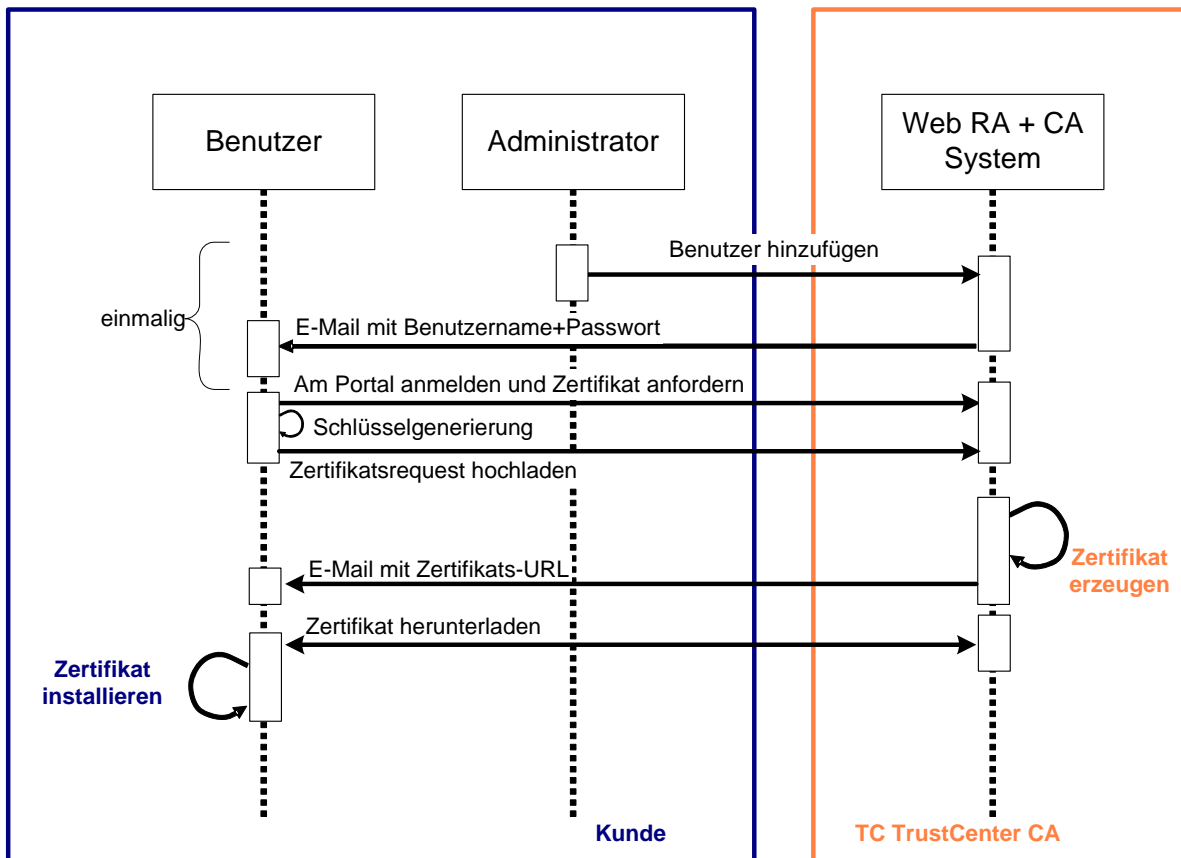


Abbildung 4 Antragsprozess nicht wiederherstellbarer Benutzerzertifikate für „Privilegierte Benutzer“

Es können auch Chipkarten oder USB-Token zum Speichern der Zertifikate verwendet werden. In diesem Fall muss der zugehörige Cryptographic Service Provider (CSP) zur Schlüsselgenerierung ausgewählt bzw. die zugehörige *PKCS#11* Library im Web-Browser des Benutzers installiert werden. Die Liste der zulässigen CSPs kann durch eine Schlüsselerzeugungsrichtlinie vorgegeben werden, siehe Abschnitt 3.4).

Dieser Prozess ist vergleichbar mit dem Antragsprozess nicht wiederherstellbarer Zertifikate für einen *Administrator* (siehe Abschnitt 3.4). In Tabelle 1 ist eine genaue Beschreibung der Rollen zu finden.

3.7.4 Ausstellung wiederherstellbarer Benutzerzertifikate für „Privilegierte Benutzer“

Schritt 1 und 2 sind vorbereitende Tätigkeiten, sie müssen für weitere Zertifikate nicht wiederholt werden.

1. Der „PKI Administrator“ oder „Registration Officer“ muss den Benutzer im Web-Portal anlegen. Dabei muss die Identität des Benutzers geprüft worden sein. Die Rolle wird auf „Basisbenutzer“ gesetzt.
2. Der Benutzer wird eine Benachrichtigungs-E-Mail mit seinen Zugangsdaten (Benutzername und Passwort) für das Web-Portal erhalten.

Hinweis: Der „PKI Administrator“ oder „Registration Officer“ kann die Benutzerdaten jederzeit korrigieren.

3. Der Benutzer kann sich am Web-Portal anmelden und ein Zertifikat anfordern. Abhängig vom Zertifikatsprodukt müssen dabei ggf. noch einige Daten durch den Benutzer angegeben werden.
4. TC TrustCenter erzeugt eine Einmal-PIN zum Schutz der *PKCS#12 PSE* gegen ungewünschten Zugriff und schickt sie an den Benutzer.
5. TC TrustCenter erzeugt das Schlüsselpaar und das Zertifikat (= Personal Security Environment (*PKCS#12 PSE*)).
6. TC TrustCenter schickt eine E-Mail mit der URL zum Herunterladen der *PKCS#12 PSE* an den Benutzer. Diese URL ist mit der Einmal-PIN geschützt.

Hinweis: Aus Sicherheitsgründen ist diese URL nur 30 Tage gültig und wird nach 3 Fehlversuchen bei der Einmal-PIN-Eingabe automatisch gesperrt. In diesem Fall kann durch Auslösen von Key Recovery ein neues Zeitfenster zur Installation der *PKCS#12 PSE* bereitgestellt werden.

7. Der Benutzer importiert die *PKCS#12 PSE* mit dem privaten Schlüssel und dem Zertifikat. Dabei muss die Einmal-PIN erneut eingegeben werden. Für diesen Vorgang ist keine Anmeldung am Web-Portal erforderlich.

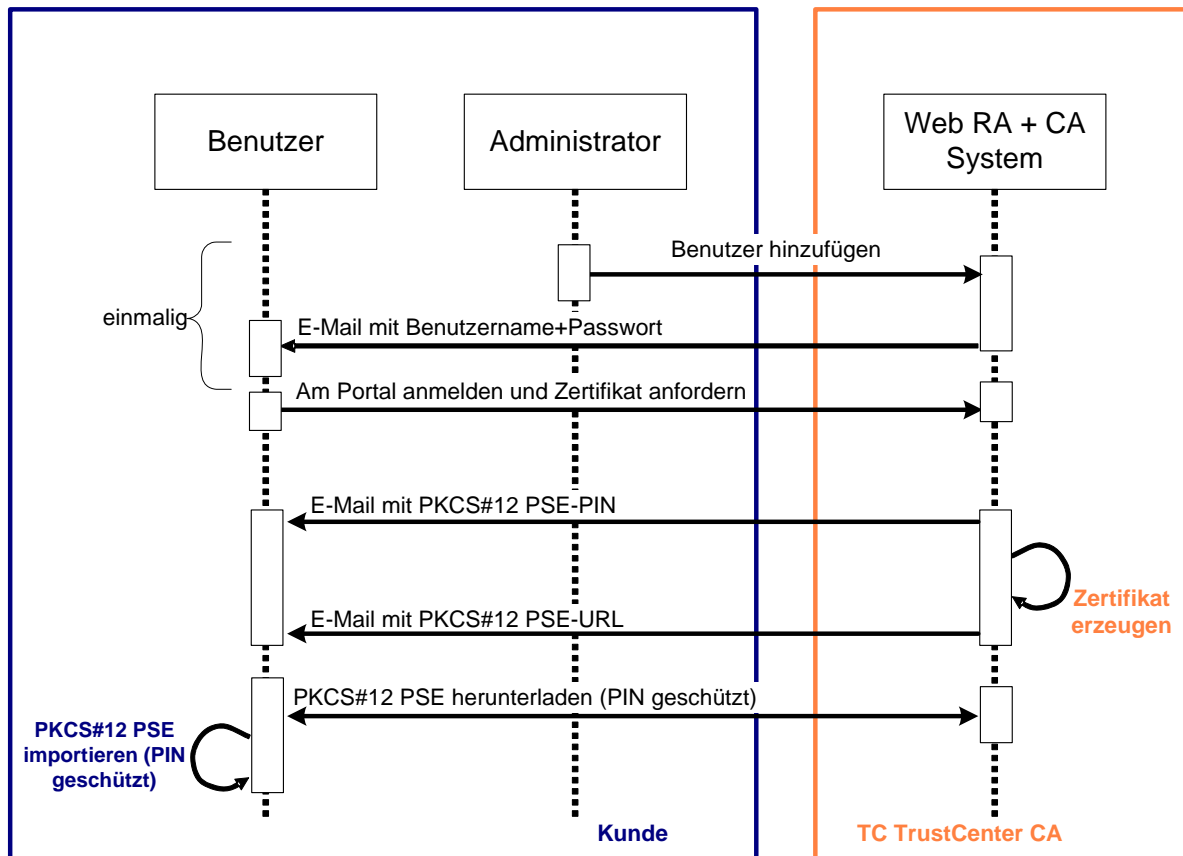


Abbildung 5 Antragsprozess wiederherstellbarer Benutzerzertifikate für „Privilegierte Benutzer“

Es können auch Chipkarten oder USB-Token zum Speichern der Zertifikate verwendet werden. Bitte benutzen Sie in diesem Fall das zugehörige Programm zum Importieren der *PKCS#12 PSE* auf die Chipkarte.

Dieser Prozess ist vergleichbar mit dem Antragsprozess wiederherstellbarer Zertifikate für einen *Administrator* (siehe Abschnitt 3.4). In Tabelle 1 ist eine genaue Beschreibung der Rollen zu finden.

3.7.5 Anonyme Beantragung von Zertifikaten

Zertifikate können auch ohne Authentisierung beantragt werden. Dieses „Anonymous Request“ Feature muss vor der Nutzung aktiviert werden.

URLs für anonyme Anträge müssen speziell generiert werden. Diese URLs müssen für die Antragsteller entsprechend veröffentlicht werden. Wir empfehlen, diese URLs nur im Intranet und nicht im Internet zu veröffentlichen.

Hinweis: Jeder, der diese URL kennt, kann anonyme Anträge stellen. Es ist die Aufgabe des „PKI Administrators“ oder „Enrollment Officers“ diese Anträge nach einer geeigneten Prüfung des Antragstellers abzulehnen oder freizuschalten.

Hinweis: Um Suchmaschinen von der Publizierung und Verfolgung derartiger anonymer Antrags-URLs abzuhalten, sollten entsprechende „robots.txt“ Dateien vorhanden sein.

Jede URL kann nur für ein Produkt für einen Affiliate verwendet werden.


Anonyme Anträge werden in der Benutzeroberfläche speziell markiert. Angaben des Antragstellers werden am Antrag gespeichert. Der Freischaltungsprozess ist vergleichbar zu dem bei Anträgen von „Basisbenutzern“.

Der *Zertifikatsbesitzer* für anonym beantragte Zertifikate wird wie folgt gesetzt:

1. auf den (neu als Benutzer angelegten) Antragsteller im Fall von Benutzerzertifikaten
2. auf den beim Erzeugen der Antrags-URL (SCEP) angegebenen Benutzer im Fall von SCEP Funktions- oder Serverzertifikaten.

3.8 Initiieren von Zertifikatsanträgen für andere Benutzer

Das Beantragen von Zertifikaten kann durch den *Administrator* initiiert werden. Dieser Prozess wird als „Zertifikatseinladung“ bezeichnet. Das Erzeugen von Zertifikatseinladungen kann sowohl im Einzelverfahren als auch im Batchverfahren erfolgen. Mittels Batchverfahren können für die aus anderen IT-Systemen exportierten Benutzer einfach Zertifikatseinladungen erzeugt werden. Die Qualität der Daten kann beim Batchverfahren deutlich besser sein als beim Einzelverfahren (weniger Schreibfehler).

Benötigte Rolle	„PKI Administrator“ oder „Enrollment Officer“
Voraussetzungen	Der Benutzer muss bereits im Web-Portal eingerichtet sein.
Formale Anforderungen	Keine
Implizite Aktionen	Benachrichtigungs-E-Mail wird an den Benutzer verschickt.
Benutzeroberfläche	



Zertifikatseinladungen sind für einen „Externen Benutzer“, „Basisbenutzer“ oder „Privilegierten Benutzer“ identisch.

3.8.1 Zertifikatseinladungen nicht wiederherstellbarer Zertifikate im Einzelverfahren

Schritt 1 und 2 sind vorbereitende Tätigkeiten, sie müssen für weitere Zertifikate nicht wiederholt werden.

1. Der „PKI Administrator“ oder „Registration Officer“ muss den Benutzer im Web-Portal anlegen. Dabei muss die Identität des Benutzers geprüft worden sein. Die Rolle wird auf „Basisbenutzer“ gesetzt.
2. Der Benutzer wird eine Benachrichtigungs-E-Mail mit seinen Zugangsdaten (Benutzername und Passwort) für das Web-Portal erhalten.

Hinweis: Der „PKI Administrator“ oder „Registration Officer“ kann die Benutzerdaten jederzeit korrigieren.

3. „PKI Administrator“ oder „Registration Officer“ erzeugen eine Zertifikatseinladung um den Ausstellungsprozess für ein Zertifikat zu initiieren.
4. TC TrustCenter erzeugt eine Einmal-PIN um den Benutzer für den Schlüsselerzeugungsprozess zu authentifizieren und schickt diese mit der zugehörigen URL zur Schlüsselerzeugung an den Benutzer.
5. Der Benutzer klickt auf den Link, gibt die PIN ein und initiiert so die Schlüsselerzeugung durch den Web-Browser. Der öffentliche Schlüssel wird zu TC TrustCenter hochgeladen.
6. TC TrustCenter erzeugt das Zertifikat und schickt eine URL zum Herunterladen an den Benutzer. Da Zertifikate keine geheimen Daten beinhalten ist diese URL nicht durch eine PIN geschützt.
7. Der Benutzer installiert durch Klick auf den Link das Zertifikat. Für diesen Vorgang ist keine Anmeldung am Web-Portal erforderlich.

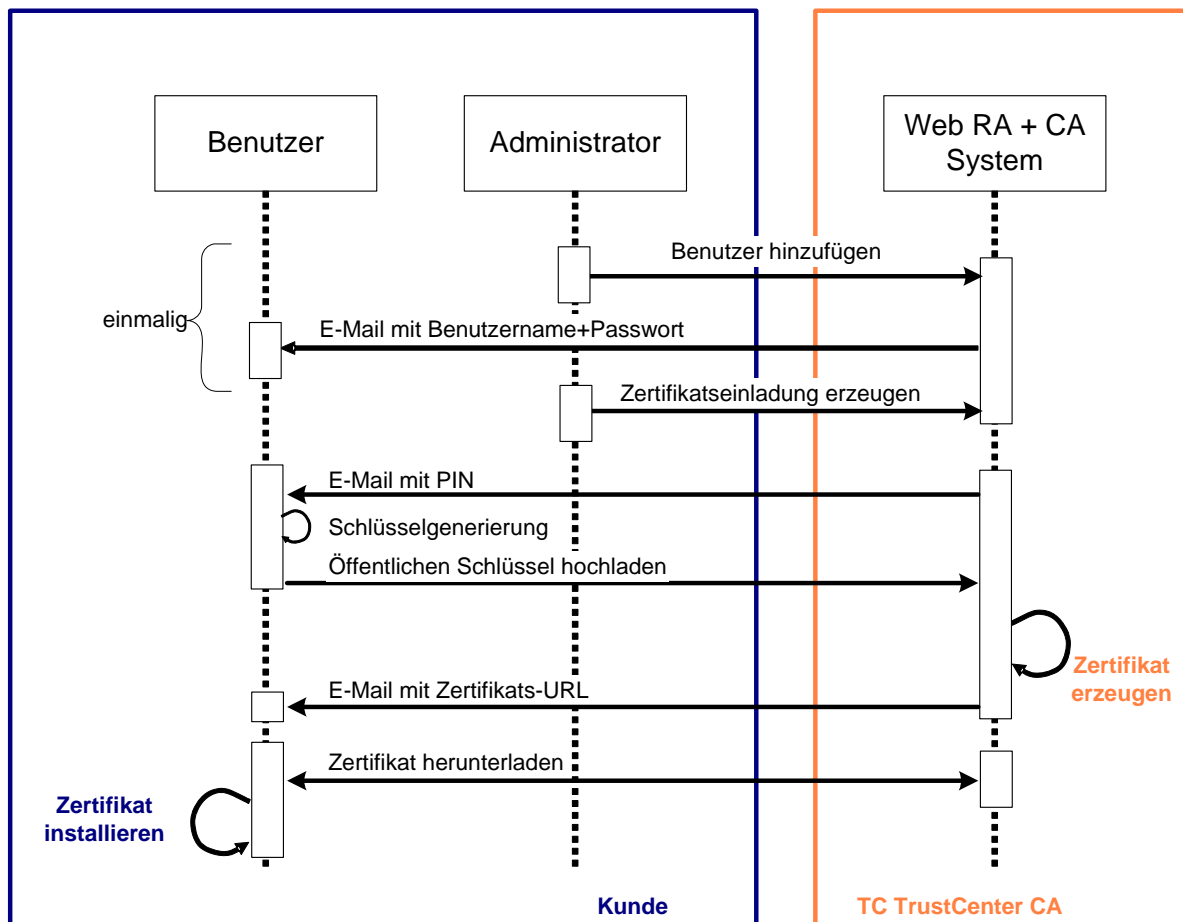


Abbildung 6 Zertifikatseinladung für nicht wiederherstellbare Zertifikate im Einzelverfahren

Es können auch Chipkarten oder USB-Token zum Speichern der Zertifikate verwendet werden. In diesem Fall muss der zugehörige Cryptographic Service Provider (CSP) zur Schlüsselgenerierung ausgewählt bzw. die zugehörige *PKCS#11* Library im Web-Browser des Benutzers installiert werden. Die Liste der zulässigen CSPs kann durch eine Schlüsselerzeugungsrichtlinie vorgegeben werden, siehe Abschnitt 3.4).

3.8.2 Zertifikatseinladungen wiederherstellbarer Zertifikate im Einzelverfahren

Schritt 1 und 2 sind vorbereitende Tätigkeiten, sie müssen für weitere Zertifikate nicht wiederholt werden.

1. Der „PKI Administrator“ oder „Registration Officer“ muss den Benutzer im Web-Portal anlegen. Dabei muss die Identität des Benutzers geprüft worden sein. Die Rolle wird auf „Basisbenutzer“ gesetzt.
2. Der Benutzer wird eine Benachrichtigungs-E-Mail mit seinen Zugangsdaten (Benutzername und Passwort) für das Web-Portal erhalten.

Hinweis: Der „PKI Administrator“ oder „Registration Officer“ kann die Benutzerdaten jederzeit korrigieren.

3. „PKI Administrator“ oder „Registration Officer“ erzeugen eine Zertifikatseinladung um den Ausstellungsprozess für ein Zertifikat zu initiieren.
4. TC TrustCenter erzeugt eine Einmal-PIN zum Schutz der *PKCS#12 PSE* gegen ungewünschten Zugriff und schickt sie an den Benutzer.

5. TC TrustCenter erzeugt das Schlüsselpaar und das Zertifikat (= Personal Security Environment (*PKCS#12 PSE*)).
6. TC TrustCenter schickt eine E-Mail mit der URL zum Herunterladen der *PKCS#12 PSE* an den Benutzer. Diese URL ist PIN geschützt.

Hinweis: Aus Sicherheitsgründen ist diese URL nur 30 Tage gültig und wird nach 3 Fehlversuchen bei der Einmal-PIN-Eingabe automatisch gesperrt. In diesem Fall kann durch Auslösen von Key Recovery ein neues Zeitfenster zur Installation der *PKCS#12 PSE* bereitgestellt werden.

7. Der Benutzer importiert die *PKCS#12 PSE* mit dem privaten Schlüssel und dem Zertifikat. Dabei muss die Einmal-PIN erneut eingegeben werden. Für diesen Vorgang ist keine Anmeldung am Web-Portal erforderlich.

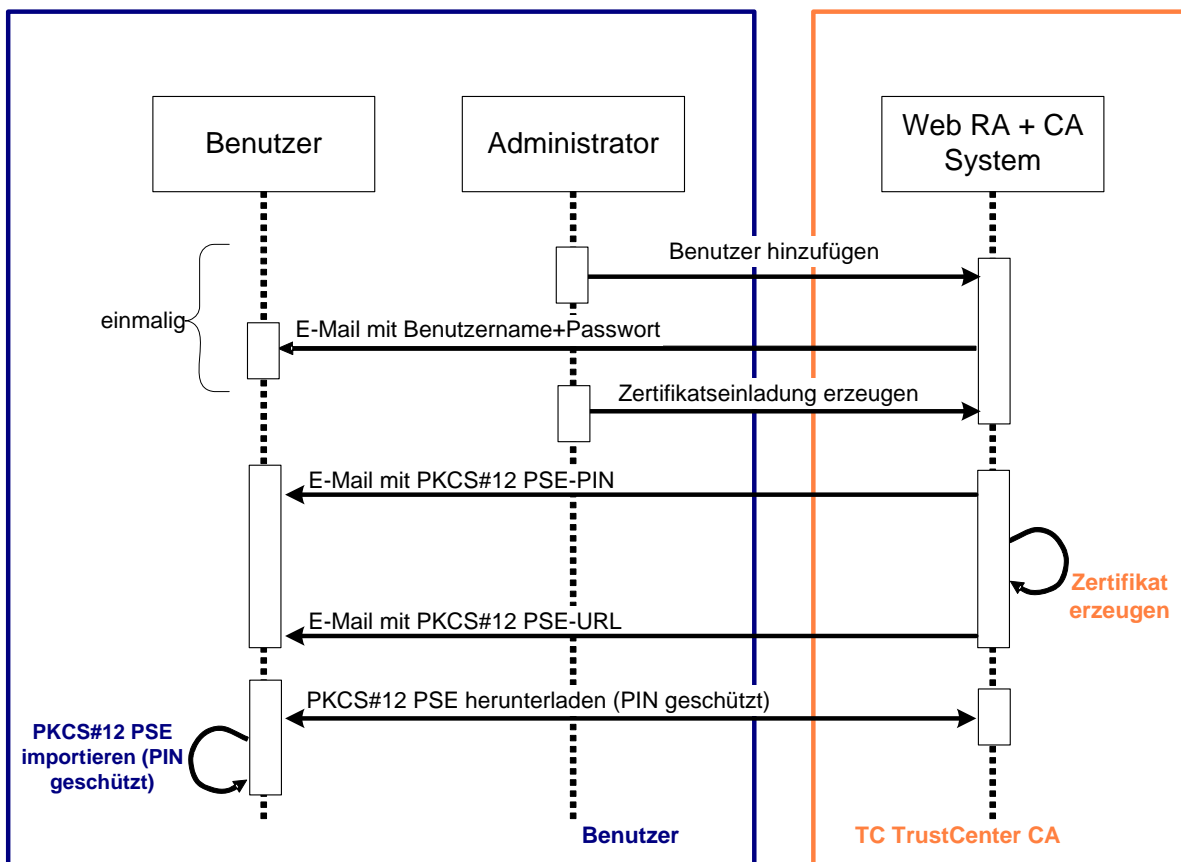


Abbildung 7 Zertifikatseinladung für wiederherstellbare Zertifikate im Einzelverfahren

Es können auch Chipkarten oder USB-Token zum Speichern der Zertifikate verwendet werden. Bitte benutzen Sie in diesem Fall das zugehörige Programm zum Importieren der *PKCS#12 PSE* auf die Chipkarte.

3.8.3 Zertifikatseinladungen nicht wiederherstellbarer Zertifikate im Batchverfahren

1. Der „PKI Administrator“ oder „Registration Officer“ kann entweder Zertifikatseinladungen im Batchverfahren für bestehende Benutzer erzeugen oder die Benutzer hinzufügen und dann automatisch Zertifikatseinladungen für sie erzeugen lassen.
2. Der „PKI Administrator“ oder „Registration Officer“ lädt eine CSV-Datei mit den Benutzernamen oder E-Mail-Adressen der gewünschten Benutzer oder aber er lädt die vollständigen Benutzerdaten hoch.

3. TC TrustCenter erzeugt Einmal-PINs um die Benutzer für den Schlüsselerzeugungsprozess zu authentifizieren und schickt diese mit den zugehörigen URLs zur Schlüsselerzeugung an die Benutzer.
4. Der Benutzer klickt auf den Link, gibt die PIN ein und initiiert so die Schlüsselerzeugung durch den Web-Browser. Der öffentliche Schlüssel wird zu TC TrustCenter hochgeladen.
5. TC TrustCenter erzeugt das Zertifikat und schickt eine URL zum Herunterladen an den Benutzer. Da Zertifikate keine geheimen Daten beinhalten ist diese URL nicht durch eine PIN geschützt.
6. Der Benutzer installiert durch Klick auf den Link das Zertifikat. Für diesen Vorgang ist keine Anmeldung am Web-Portal erforderlich.

Es können auch Chipkarten oder USB-Token zum Speichern der Zertifikate verwendet werden. In diesem Fall muss der zugehörige Cryptographic Service Provider (CSP) zur Schlüsselgenerierung ausgewählt bzw. die zugehörige PKCS#11 Library im Web-Browser des Benutzers installiert werden. Die Liste der zulässigen CSPs kann durch eine Schlüsselerzeugungsrichtlinie vorgegeben werden, siehe Abschnitt 3.4).

3.8.4 Zertifikatseinladungen wiederherstellbarer Zertifikate im Batchverfahren







1. Der „PKI Administrator“ oder „Registration Officer“ kann entweder Zertifikatseinladungen im Batchverfahren für bestehende Benutzer erzeugen oder die Benutzer hinzufügen und dann automatisch Zertifikatseinladungen für sie erzeugen lassen.
2. Der „PKI Administrator“ oder „Registration Officer“ lädt eine CSV-Darei mit den Benutzernamen oder E-Mail-Adressen der gewünschten Benutzer oder aber er lädt die vollständigen Benutzerdaten hoch.
3. TC TrustCenter erzeugt Einmal-PINs zum Schutz der *PKCS#12 PSEs* gegen ungewünschten Zugriff und schickt sie an die Benutzer.
4. TC TrustCenter erzeugt die Schlüsselpaare und Zertifikate (= Personal Security Environments (*PKCS#12 PSEs*)).
5. TC TrustCenter schickt eine E-Mail mit der URL zum Herunterladen der *PKCS#12 PSE* an jeden Benutzer. Diese URLs sind PIN geschützt.

<p>Hinweis: Aus Sicherheitsgründen ist diese URL nur 30 Tage gültig und wird nach 3 Fehlversuchen bei der Einmal-PIN-Eingabe automatisch gesperrt. In diesem Fall kann durch Auslösen von Key Recovery ein neues Zeitfenster zur Installation der <i>PKCS#12 PSE</i> bereitgestellt werden.</p>
--

6. Der Benutzer importiert die *PKCS#12 PSE* mit dem privaten Schlüssel und dem Zertifikat. Dabei muss die Einmal-PIN erneut eingegeben werden. Für diesen Vorgang ist keine Anmeldung am Web-Portal erforderlich.

Es können auch Chipkarten oder USB-Token zum Speichern der Zertifikate verwendet werden. Bitte benutzen Sie in diesem Fall das zugehörige Programm zum Importieren der *PKCS#12 PSE* auf die Chipkarte.



3.9 Sperren, Suspendieren oder Desuspendieren von Zertifikaten sowie Initiieren von Key Recovery

Benötigte Rolle	„PKI Administrator“ (alle Vorgänge), Delegierte Rollen (siehe Tabelle 1 für eine genaue Beschreibung), <i>Zertifikatsbesitzer</i> mit Rolle „Privilegierter Benutzer“ (bis auf Desuspendieren), oder „Basisbenutzer“ (bis auf Desuspendieren),
Voraussetzungen	Der Benutzer muss mindestens ein Zertifikat besitzen.
Formale Anforderungen	<ul style="list-style-type: none"> Desuspendieren: Es muss geprüft werden, ob der Benutzer weiterhin den privaten Schlüssel unter seiner Kontrolle hat und ein derartiges Zertifikat auch weiterhin besitzen darf.
Implizite Aktionen	<ul style="list-style-type: none"> Key Recovery: Der Benutzer (= <i>Zertifikatsinhaber</i>) erhält eine E-Mail mit dem Link zum Herunterladen der <i>PKCS#12 PSE</i> sowie eine zweite E-Mail mit der PIN um (a) die <i>PKCS#12 PSE</i> herunterzuladen und sie (b) zu importieren.
Benutzeroberfläche	  <p>Klicken Sie auf das zugehörige Symbol in der Ergebnistabelle: , ,  oder </p>

3.9.1 Sperren und Suspendieren von Zertifikaten

Die Vorgänge Sperren und Suspendieren von Zertifikaten können durch den „PKI Administrator“, den „Revocation Officer“ oder den *Zertifikatsbesitzer* ausgelöst werden.

Der Administrationsprozess im Einzelverfahren läuft wie folgt ab:

1. Wählen Sie den Menüeintrag „Zertifikate“ im Web-Portal.
2. Der „PKI Administrator“, der „Revocation Officer“ oder der *Zertifikatsbesitzer* kann das zu sperrende bzw. zu suspendierende Zertifikat mittels verschiedener Kriterien, z.B. Seriennummer oder Benutzername suchen. Die Sperrung / Suspendierung wird durch einen Klick auf das zugehörige Aktionssymbol „Sperren“ () / „Suspendieren“ () ausgeführt. Es können auch mehrere Zeilen ausgewählt werden. In dem Fall muss eine der zugehörigen Schaltflächen am Ende der Ergebnistabelle gedrückt werden.
3. Falls ein Benutzer mehr als ein Zertifikat besitzt muss jedes Zertifikat einzeln gesperrt bzw. suspendiert werden.
4. Die Seriennummern der gesperrten bzw. suspendierten Zertifikate werden in die nächste Sperrliste (CRL) aufgenommen.
5. TC TrustCenter schickt nach erfolgter Sperrung / Suspendierung eine Bestätigungs-E-Mail an den *Zertifikatsbesitzer*.

Der Administrationsprozess im Batchverfahren läuft wie folgt ab:

1. Wählen Sie den Menüeintrag „Zertifikate“ im Web-Portal.
2. Der „PKI Administrator“, der „Revocation Officer“ oder der *Zertifikatsbesitzer* kann eine Batch-Suche durch Hochladen einer CSV-Datei mit den Benutzernamen oder E-Mail-Adressen durchführen. Die Sperrung / Suspendierung wird durch einen Klick auf das zugehörige Aktionssymbol „Sperrern“ (🛑) / „Suspendieren“ (🌐) ausgeführt. Es können auch mehrere Zeilen ausgewählt werden. In dem Fall muss eine der zugehörigen Schaltflächen am Ende der Ergebnistabelle gedrückt werden.
3. Die Seriennummern der gesperrten bzw. suspendierten Zertifikate werden in die nächste Sperrliste (CRL) aufgenommen.
4. TC TrustCenter schickt nach erfolgter Sperrung / Suspendierung eine Bestätigungs-E-Mail an den *Zertifikatsbesitzer*.

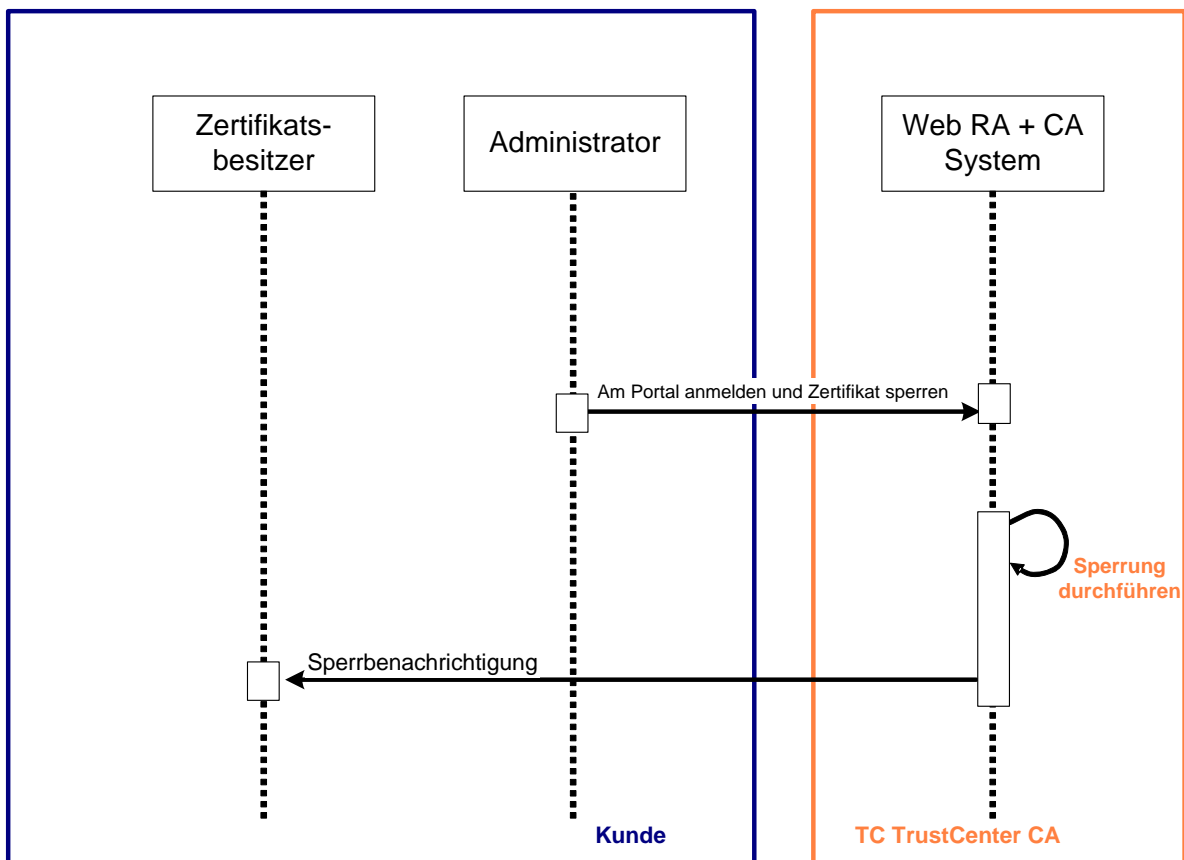


Abbildung 8 Ablauf des Sperrens bzw. Suspendierens durch „PKI Administrator“ / „Revocation Officer“

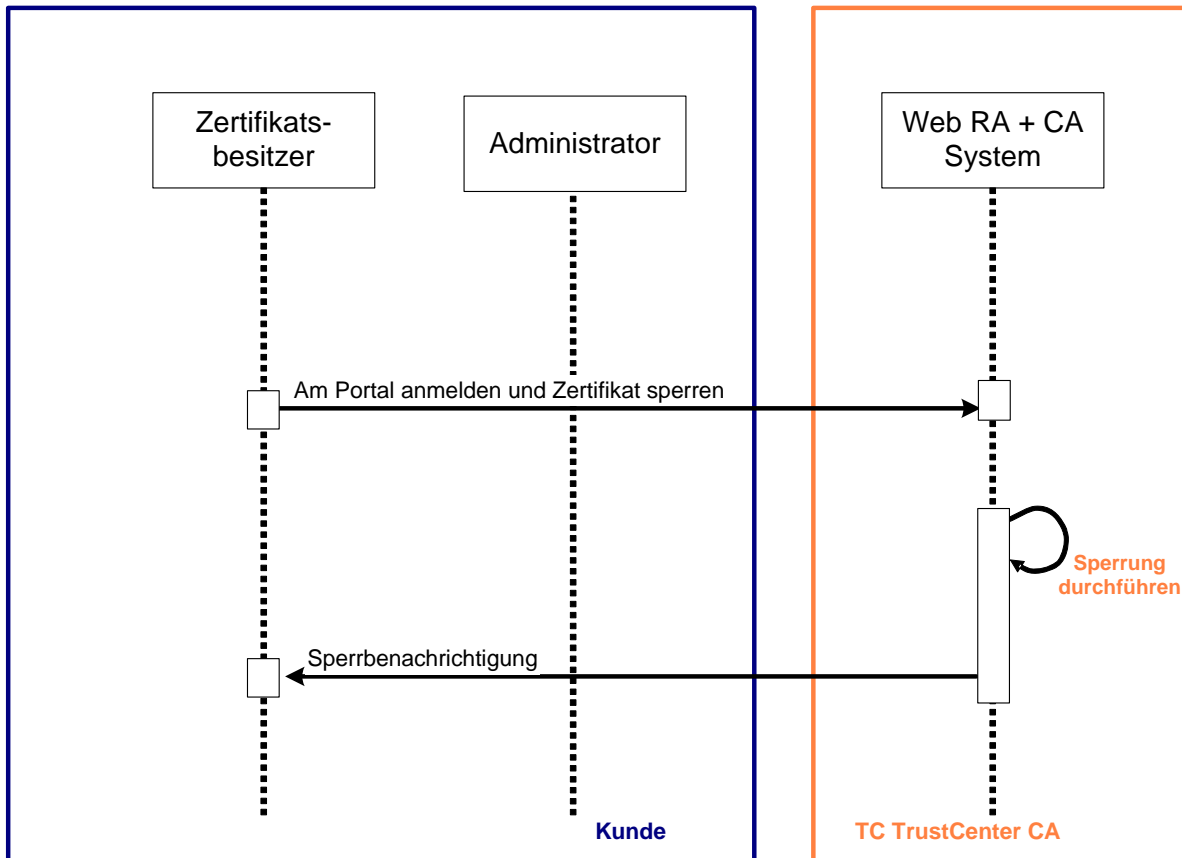



Abbildung 9 Ablauf des Sperrens bzw. Suspendierens durch den Zertifikatsbesitzer

3.9.2 Desuspendieren von Zertifikaten

Durch das Desuspendieren wird eine Suspendierung aufgehoben. Das Zertifikat gilt danach uneingeschränkt als gültig. Die Desuspendierung kann nur durch den „PKI Administrator“ oder den „Unsuspendation Officer“ durchgeführt werden.


Hinweis: Nach dem Desuspendieren gilt ein Zertifikat als ununterbrochen gültig.

Der Ablauf der Desuspendierung ist identisch mit dem des Sperrens bzw. Suspendierens. Nur die benötigten Rollen unterscheiden sich. Das Symbol für Desuspendieren ist .

3.9.3 Key Recovery

Key Recovery, also das Wiederherstellen von privatem Schlüssel und Zertifikat, wird durch den „PKI Administrator“, den „Key Recovery Officer“ oder den *Zertifikatsbesitzer* initiiert.

Der Wiederherstellungsprozess im Einzelverfahren läuft wie folgt ab:

1. Die wiederherzustellenden Schlüssel/Zertifikate können mittels verschiedener Kriterien, z.B. Seriennummer oder Benutzername gesucht werden. Die Wiederherstellung wird durch den Klick auf das Symbol für „Wiederherstellen“ () initiiert.
2. Falls ein Benutzer mehr als ein Zertifikat besitzt muss jedes Zertifikat einzeln wiederhergestellt werden.
3. TC TrustCenter erzeugt eine Einmal-PIN zum Schutz der *PKCS#12 PSE* gegen ungewünschten Zugriff und schickt sie an den Benutzer.

4. TC TrustCenter schickt eine E-Mail mit der URL zum Herunterladen der *PKCS#12 PSE* an den Benutzer. Diese URL ist mit der Einmal-PIN geschützt.
5. Der Benutzer importiert die *PKCS#12 PSE* mit dem privaten Schlüssel und dem Zertifikat. Dabei muss die Einmal-PIN erneut eingegeben werden. Für diesen Vorgang ist keine Anmeldung am Web-Portal erforderlich.

Der Wiederherstellungsprozess im Batchverfahren läuft wie folgt ab:

1. Wählen Sie den Menüeintrag „Zertifikate“ im Web-Portal.
2. Der „PKI Administrator“, der „Revocation Officer“ oder der *Zertifikatsbesitzer* kann eine Batch-Suche durch Hochladen einer CSV-Datei mit den Benutzernamen oder E-Mail-Adressen durchführen. Die Wiederherstellung wird durch einen Klick auf das zugehörige Aktionssymbol „Wiederherstellen“ (🌐) mit *ePIN* initiiert. Es können auch mehrere Zeilen ausgewählt werden. In dem Fall muss die zugehörige Schaltfläche am Ende der Ergebnistabelle gedrückt werden.

Hinweis: Bei Verwendung des Verfahrens *Externe PIN* (siehe Abschnitt 3.3) ist Batch Key Recovery nicht möglich.

3. TC TrustCenter erzeugt Einmal-PINs zum Schutz der *PKCS#12 PSEs* gegen ungewünschten Zugriff und schickt sie an die Benutzer.
4. TC TrustCenter schickt E-Mails mit der URL zum Herunterladen der *PKCS#12 PSEs* an die Benutzer. Diese URLs sind mit Einmal-PINs geschützt.
5. Der Benutzer importiert die *PKCS#12 PSE* mit dem privaten Schlüssel und dem Zertifikat. Dabei muss die Einmal-PIN erneut eingegeben werden. Für diesen Vorgang ist keine Anmeldung am Web-Portal erforderlich.


Hinweis: Bei allen Key-Recovery Varianten wird die URL zum Herunterladen der *PKCS#12 PSE* an die ursprüngliche (also bei Zertifikats-Beantragung eingestellte) E-Mail-Adresse des *Zertifikatsbesitzers* geschickt. Die Einmal-PIN wird an die aktuelle Adresse geschickt.

3.10 Key Escrow

Benötigte Rolle	„Key Escrow Administrator (Request)“
Voraussetzungen	Der Benutzer muss mindestens ein wiederherstellbares Zertifikat besitzen.
Formale Anforderungen	<ul style="list-style-type: none"> • Der Kunde muss die TC TrustCenter Key Escrow Requirements erfüllen. • Zusätzliche Anforderungen können sich aus den jeweiligen gesetzlichen Vorgaben und den gültigen Firmenrichtlinien ergeben.
Implizite Aktionen	<ul style="list-style-type: none"> • Die PIN wird an die unter „Key Escrow E-Mail (PIN)“ eingetragene Adresse und der Link zum Herunterladen der <i>PKCS#12 PSE</i> an die unter „Key Escrow E-Mail (PSE)“ eingetragene Adresse geschickt.


Benutzeroberfläche




Klicken Sie auf das zugehörige Symbol in der Ergebnistabelle: 

Key Escrow, also das Wiederherstellen von privatem Schlüssel und Zertifikat ohne Mitwirkung des Besitzers, wird durch den „Key Escrow Administrator (Request)“ initiiert.

Der Wiederherstellungsprozess im Einzelverfahren läuft wie folgt ab:

1. Die wiederherzustellenden Schlüssel/Zertifikate können mittels verschiedener Kriterien, z.B. Seriennummer oder Benutzername gesucht werden. Die Wiederherstellung wird durch den Klick auf das Symbol für „Wiederherstellen“ () initiiert.
2. Falls ein Benutzer mehr als ein Zertifikat besitzt muss jedes Zertifikat einzeln wiederhergestellt werden.
3. TC TrustCenter erzeugt eine Einmal-PIN zum Schutz der *PKCS#12 PSE* gegen ungewünschten Zugriff und schickt sie an die unter Konfiguration | Einstellungen | Key Escrow E-Mail (PIN) angegebene Adresse.
4. TC TrustCenter schickt eine E-Mail mit der URL zum Herunterladen der *PKCS#12 PSE* an die unter Konfiguration | Einstellungen | Key Escrow E-Mail (PSE) angegebene Adresse. Diese URL ist mit der Einmal-PIN geschützt.
5. Der „Key Escrow Administrator“ importiert die *PKCS#12 PSE* mit dem privaten Schlüssel und dem Zertifikat. Dabei muss die Einmal-PIN erneut eingegeben werden. Für diesen Vorgang ist keine Anmeldung am Web-Portal erforderlich.

Der *Key Escrow*-Prozess im Batchverfahren läuft wie folgt ab:



1. Wählen Sie den Menüeintrag „Zertifikate“ im Web-Portal.
2. Der „Key Escrow Administrator (Request)“ kann eine Batch-Suche durch Hochladen einer CSV-Datei mit den Benutzernamen oder E-Mail-Adressen durchführen. Die Wiederherstellung wird durch einen Klick auf das zugehörige Aktionssymbol „Wiederherstellen“ () mit *ePIN* initiiert. Es können auch mehrere Zeilen ausgewählt werden. In dem Fall muss die zugehörige Schaltfläche am Ende der Ergebnistabelle gedrückt werden.
3. TC TrustCenter erzeugt Einmal-PINs zum Schutz der *PKCS#12 PSEs* gegen ungewünschten Zugriff und schickt sie an die unter Konfiguration | Einstellungen | Key Escrow E-Mail (PIN) angegebene Adresse.
4. TC TrustCenter schickt E-Mails mit der URL zum Herunterladen der *PKCS#12 PSEs* an die unter Konfiguration | Einstellungen | Key Escrow E-Mail (PSE) angegebene Adresse. Diese URLs sind mit Einmal-PINs geschützt.

- Der „Key Escrow Administrator“ importiert die *PKCS#12 PSE* mit dem privaten Schlüssel und dem Zertifikat. Dabei muss die jeweilige Einmal-PIN erneut eingegeben werden. Für diesen Vorgang ist keine Anmeldung am Web-Portal erforderlich.

Hinweis: *Key Escrow* ist ein sicherheitsrelevanter Prozess. Eine strikte Rollentrennung dem „Key Escrow Administrator (Request)“ und dem „Key Escrow Administrator (PSE)“ wird empfohlen. Siehe Dokument *Key Escrow Requirements* für weitere Details.

Hinweis: Der *Zertifikatsbesitzer* wird nicht über den *Key Escrow* Vorgang informiert.


3.11 Zertifikatsbesitzer wechseln

Benötigte Rolle	„PKI Administrator“ oder eine delegierte Rolle (siehe Tabelle 1 für eine genaue Beschreibung)
Voraussetzungen	Der Benutzer muss mindestens ein Zertifikat besitzen.
Formale Anforderungen	<ul style="list-style-type: none"> Es muss geprüft werden, ob der neue Besitzer die notwendigen Bedingungen für den Besitz des Zertifikates erfüllt.
Implizite Aktionen	<ul style="list-style-type: none"> Keine
Benutzeroberfläche	 <p>Klicken Sie auf das zugehörige Symbol in der Ergebnistabelle: </p>


Jedes Zertifikat ist einem Besitzer zugeordnet. Im Fall von *Team- bzw. Applikationszertifikaten*, also z.B. TC Team Certificate ist das der Applikationsverantwortliche bzw. der Teamverantwortliche.

Bevor Benutzer gelöscht werden können müssen alle *Team- bzw. Applikationszertifikate* einem neuen *Zertifikatsbesitzer* zugewiesen werden.




Der Prozess im Einzelverfahren läuft wie folgt ab:

- Die einem neuen Besitzer zuzuweisenden Zertifikate können mittels verschiedener Kriterien, z.B. Seriennummer oder Benutzername suchen. Die Zuordnung zu einem neuen Benutzer wird durch den Klick auf das Symbol für „Besitzer wechseln“ () initiiert.
- Falls ein Benutzer der Besitzer von mehreren *Team- bzw. Applikationszertifikaten* ist muss jedes Zertifikat einzeln einem neuen Besitzer zugewiesen werden.
- Der neue Besitzer wird ausgewählt.

Der Prozess im Batchverfahren läuft wie folgt ab:

1. Wählen Sie den Menüeintrag „Zertifikate“ im Web-Portal.
2. Der „PKI Administrator“ oder der „Registration Officer“ kann eine Batch-Suche durch Hochladen einer CSV-Datei mit den Benutzernamen oder E-Mail-Adressen durchführen. Die Zuweisung zu einem neuen Besitzer wird durch einen Klick auf das zugehörige Aktionssymbol „Besitzer wechseln“  initiiert. Es können auch mehrere Zeilen ausgewählt werden. In dem Fall muss die zugehörige Schaltfläche am Ende der Ergebnistabelle gedrückt werden.
3. Der neue Besitzer wird ausgewählt.

3.12 Überprüfen der SSL Server Installation

Benötigte Rolle	„PKI Administrator“, „Enrollment Officer“ bzw. „Privilegierter Benutzer“ oder „Basisbenutzer“ wenn <i>Zertifikatsbesitzer</i> .
Voraussetzungen	<ul style="list-style-type: none"> ▪ Es muss mindestens ein SSL Server Zertifikat ausgestellt worden sein. ▪ Funktioniert nur mit Microsoft Internet Explorer
Formale Anforderungen	Keine
Implizite Aktionen	Keine
Benutzeroberfläche	<div style="text-align: center;">   </div> <p>Klicken Sie auf das zugehörige Symbol in der Ergebnistabelle: </p>

Durch Klick auf das Icon wird eine Microsoft ClickOnce Applikation gestartet. Es wird nur der Microsoft Internet Explorer als Web Browser unterstützt.

Die öffnet eine SSL Verbindung zu dem betreffenden Web Server und führt folgende Prüfungen durch:

- Ist der Server erreichbar?
- Ist das Zertifikat korrekt installiert?

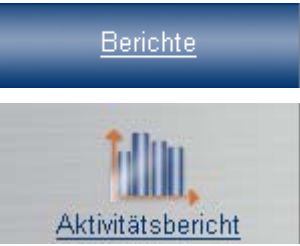
4 Berichte

4.1 SLA Reports

SLA Reports werden auf monatlicher Basis erstellt. Sie sind nur für autorisierte Administratoren zugänglich.

4.2 Aktivitätsberichte

Aktivitätsberichte können interaktiv über das Web-Portal erstellt werden.

Benötigte Rolle	„PKI Administrator“ oder eine delegierte Rolle
Voraussetzungen	Keine
Formale Anforderungen	Keine
Implizite Aktionen	Keine
Benutzeroberfläche	

Folgende Einzelberichte sind enthalten:


- Anzahl der Zertifikatsanträge nach Datum
- Anzahl erzeugter Zertifikatseinladungen nach Datum
- Anzahl hinzugefügter Benutzer nach Datum
- Anzahl ausgestellter Zertifikate pro Zertifikatsprodukt

Berichte können wahlweise im HTML Format oder als PDF Datei erzeugt werden.

Hinweis: Berichte beziehen sich immer auf Vorgänge für alle Gruppen. Sie sind nicht auf eine bestimmte Gruppe beschränkt.

4.3 Zertifikatsberichte

Zertifikatsberichte können interaktiv über das Web Portal erstellt werden.

Benötigte Rolle	„PKI Administrator“ oder eine beliebige delegierte Rolle.
Voraussetzungen	Keine
Formale Anforderungen	Keine
Implizite Aktionen	Keine
Benutzeroberfläche	

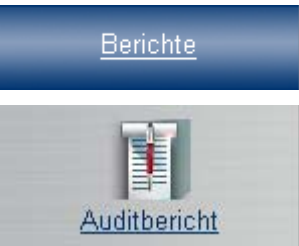


Der Zertifikatsbericht enthält alle Zertifikate für den jeweiligen Account, die in dem angegebenen Zeitraum ausgestellt wurden. Die Zertifikate sind gemäß der Gruppen der jeweiligen *Zertifikatsbesitzer* aufgeteilt.

Die Auflistung enthält den Namen des Zertifikatsproduktes, den Ausstellungszeitpunkt sowie den Preis.

4.4 Auditberichte


Auditberichte können interaktiv über das Web Portal erstellt werden.

Benötigte Rolle	„PKI Administrator“ oder „PKI Superadministrator“
Voraussetzungen	Keine
Formale Anforderungen	Keine
Implizite Aktionen	Keine
Benutzeroberfläche	

Der Auditbericht enthält die Informationen über die für den jeweiligen Account durchgeführten Aktionen, u.a. Anmeldungen, Erzeugen und Ändern von Benutzern, etc.

Hinweis: Auditberichte sind für 6 Monate online zugreifbar. Sie können für lokale Archivierung heruntergeladen werden.

5 Konfiguration

Benötigte Rolle	<p>„PKI Administrator“ (Einstellungen und „Verträge“ (s. Abschnitt 5.4) ändern, Anträge für Pre-Vetted Domains stellen).</p> <p>Delegierte Rollen (Einstellungen und „Verträge“ einsehen, Anträge für Pre-Vetted Domains stellen)</p> <p>„Basisbenutzer“ und „Privilegierte Benutzer“ (Einstellungen einsehen)</p>
Voraussetzungen	Keine
Formale Anforderungen	Keine
Implizite Aktionen	Keine
Benutzeroberfläche	

5.1 Einstellungen

Folgende Details können über das Menü „Einstellungen“ bzw. „Verträge“ in den jeweiligen Verträgen verwaltet werden:

Feld	Eigenschaft	Beschreibung
Firmenkontakt	Nur Lesen	Der Firmenkontakt enthält den „PKI Administrator“ (Name) und die juristische Person der Organisation (Firma und Adresse gemäß Registereintrag). Der „PKI Administrator“ ist verantwortlich für die Einhaltung der Vorgaben für die

Feld	Eigenschaft	Beschreibung
		Registrierung beim Hinzufügen von Benutzern und Ausstellen von Zertifikaten. Er wird vor der Einrichtung der TC Enterprise ID-Umgebung gemäß den Vorgaben registriert. Zusätzlich erhält der „PKI Administrator“ Zugriff auf das Self-Service Portal und ist berechtigt Support-Anfragen über das Self-Service Portal sowie die telefonische Hotline zu stellen.
Geschäftskontakt	Editierbar	Der Geschäftskontakt bezeichnet die für den kaufmännischen Teil zuständige Person, z.B. Vertragsverlängerung.
Technischer Kontakt	Editierbar	Der Technische Kontakt sollte mit den technischen Gegebenheiten der Implementierung / Applikationen auf Kundenseite vertraut sein. Der Technische Kontakt erhält Zugriff auf das Self-Service Portal und ist berechtigt Support-Anfragen über Self-Service Portal sowie die telefonische Hotline zu stellen.
Anmelderichtlinie	Editierbar	Die zertifikatsbasierte Anmeldung kann für alle administrativen Rollen oder alle Benutzer vorgeschrieben werden. Alternativ kann auch die Anmeldung mit Benutzername und Passwort erlaubt werden. Alle über den Account ausgestellten und für Authentisierung nutzbaren Benutzerzertifikate können zur Anmeldung verwendet werden.
Benutzer haben eine private Adresse	Editierbar	Die Unterstützung für die Privatadresse von Benutzern kann auf „Keine“, „Optional“ oder „Pflicht“ gestellt werden. Die Felder der Privatadresse können in E-Mail-Benachrichtigungen oder Dokumenten im Rahmen der Personalisierung von Chipkarten genutzt werden.
„Key Escrow E-Mail (PIN)“	Nur Lesen	Die PIN wird bei <i>Key Escrow</i> an die unter „Key Escrow E-Mail (PIN)“ eingetragene Adresse geschickt. Siehe Abschnitt 3.10.
„Key Escrow E-Mail (PSE)“	Nur Lesen	Der PKCS#12 PSE wird bei <i>Key Escrow</i> an die unter „Key Escrow E-Mail (PSE)“ eingetragene Adresse geschickt. Siehe Abschnitt 3.10.

Die folgenden Adressen können über das Menü „Verträge“ bearbeitet werden:

Feld	Eigenschaft	Beschreibung
Rechnungskontakt	Editierbar	Bezeichnet den auf der Rechnung benannten Empfänger.
Rechnungsadresse	Editierbar	Gibt die Adresse an, an die die Rechnung geschickt wird.

5.2 „Affiliates“

Jeder Benutzer ist genau einer Gesellschaft bzw. einer „Affiliate“ zugeordnet. Die Liste aller eingerichteten „Affiliates“ ist unter dem Menüpunkt „Affiliates“ einsehbar. Der PKI Administrator kann weitere „Affiliates“ und die gewünschte Registrierungsklasse hinzufügen.

Nach erfolgreicher Registrierung wird die gewünschte Registrierungsklasse dem „Affiliate“ zugewiesen.

Wenn ein beantragtes Zertifikat eine höhere Registrierungsklasse benötigt als derzeit vorhanden ist, wird der Antrag vom System bis zur erfolgreichen Registrierung zurückgehalten.

Pro „Affiliate“ werden folgende Angaben hinterlegt:

- Daten zur Organisation
 - Anzeigename
 - Land
 - Organisationsname
 - Bundesland
 - Ort
 - Unternehmenstyp
 - Strasse und Hausnummer
 - Postleitzahl
 - Telefonnummer der Zentrale
- Daten der Unternehmensregistrierung
 - Land des Unternehmensregisters
 - Bundesland des Unternehmensregisters (sofern das Unternehmensregister nicht auf nationaler Ebene arbeitet)
 - Stadt des Unternehmensregisters (sofern das Unternehmensregister nicht auf nationaler oder Bundesland-Ebene arbeitet)
 - Registrierungsnummer (z.B: Handelsregisternummer)
 - Datum des Registerauszugs
- Allgemeine Daten
 - Geprüfte Registrierungsklasse

Der Anzeigename wird in Auswahlfeldern verwendet. Die weiteren Angaben müssen mit dem Registereintrag übereinstimmen. „Affiliates“ können erst nach erfolgreicher Prüfung durch TC TrustCenter verwendet werden.

Die Angaben „Land“, „Organisation“, „Bundesland“ und „Ort“ werden entsprechend in die Zertifikate übernommen.

Einige Zertifikatsprodukte übernehmen zusätzliche Felder, z.B. „Unternehmenstyp“, „Strasse und Hausnummer“, „Postleitzahl“ und „Registrierungsnummer“.

Hinweis: In TC Personal ID wird der Organisationsname nicht aufgeführt. Eine Prüfung der Organisationszugehörigkeit ist hier nicht gegeben.

Hinweis: Der Registrierungsstatus eines „Affiliates“ ist nur für eine bestimmte Zeit gültig. Diese Zeit bezieht sich auf das Datum des Registerauszugs und hängt von der Registrierungsklasse ab.



5.3 Pre-Vetted Domains


Zertifikate können unterschiedliche, durch TC TrustCenter zu prüfende Felder enthalten. Um die Ausstellung von Zertifikaten zu beschleunigen, können zulässige Werte für derartige Felder vorab geprüft werden.

Folgende Zertifikatsfelder müssen durch TC TrustCenter geprüft werden:

- Servername bei TC Trust SSL, TC Trust SSL Wildcard, TC Extended Trust SSL, TC Domain Controller ID.
- Der optionale Benutzeranmeldename (UPN = User Principal Name) bei TC Personal ID und TC Business ID
- E-Mail Adressen bei TC Trust SSL, TC Trust SSL Wildcard, TC Domain Controller ID, TC RAS and IAS Server ID und TC Team Certificate, da diese von den E-Mail-Adressen der Zertifikatsbesitzer abweichen dürfen.

Wenn eines der oben angegebenen Zertifikatsprodukte beantragt wird, muss die in einem der oben angegebenen Felder enthaltene Domain entweder

- (a) bereits in der Liste der pre-vetted Domains aufgeführt sein oder
- (b) es wird automatisch ein pre-vetting Antrag gestellt. Der zugehörige Zertifikatsantrag wird solange nicht bearbeitet, bis der pre-vetting Antrag genehmigt wurde.

Der pre-vetting Status einer Domain ist nur für eine bestimmte Zeitspanne gültig. Falls eine Domain weiterhin benötigt wird, kann eine Verlängerung beantragt werden (.

TC Enterprise ID unterstützt sowohl Windows Domänen (z.B. meinname.local) als auch öffentlich registrierte Domains (z.B. meineFirma.de).

Hinweis: Domains müssen für jeden Affiliate getrennt geprüft werden.

5.4 „Verträge“

Die verfügbaren Zertifikatsprodukte sind im Web-Portal in sog. „Verträgen“ organisiert. „Verträge“ haben ein Anfangs- und ein Enddatum. Es kann immer nur ein „Vertrag“ aktiv sein.

Das Restguthaben gibt an für welchen Betrag stückbasiert abzurechnende Zertifikate beantragt werden können.

In der Detailansicht der „Verträge“ sind die in einem „Vertrag“ enthaltenen Zertifikatsprodukte aufgeführt. Zertifikatsprodukte mit Stückpreis größer 0 werden stückbasiert abgerechnet. Zertifikatsprodukte mit Stückpreis 0 werden benutzerbasiert abgerechnet.

Nur die als „aktiv“ gekennzeichneten Zertifikatsprodukte werden bei der Beantragung zur Auswahl angeboten. Der *Administrator* kann durch gezieltes Deaktivieren von Zertifikatsprodukten steuern, welche Zertifikate beantragt werden können. Alle Zertifikatsprodukte sind standardmäßig aktiv.

Das PIN Verfahren *Externe PIN* kann pro Produkt eingestellt werden.



5.5 E-Mail-Vorlagen

Für unterschiedliche Vorgänge (z.B. Zertifikatsauslieferung, Zertifikatssperrung, etc.) werden Benachrichtigungen vom System erzeugt und verschickt. Die Vorlagen für diese E-Mails können durch den „PKI Administrator“ angepasst werden.

Kundenspezifische Anpassungen können durch Entfernen der Anpassungen auf ihren Standardwert zurückgesetzt werden.

6 Verzeichnisdienste

Die Zertifikate sind über die TC TrustCenter Webseite suchbar und herunterladbar wenn sie auch im LDAP Service sichtbar sind (siehe Abschnitt 6.1).

Sperrlisten (CRLs) können von der TC TrustCenter Webseite heruntergeladen werden.

6.1 LDAP Service

Folgende Zertifikatsprodukte können über das TC TrustCenter LDAP Verzeichnis heruntergeladen werden:

- TC Business ID Demo
- TC Personal ID
- TC Business ID, recoverable und TC Business ID, recoverable enc.
(TC Business ID, sign+auth und sign sind nicht für die Verschlüsselung nutzbar. Eine Veröffentlichung im LDAP ist daher nicht vorgesehen.)
- TC Team Certificate
- TC Enrollment Agent ID

Aufbau des Directory Information Tree (DIT): ou=publiccertgroup, dc=trustcenter, dc=de



Option

EID-LDAP/TC-O2-TC Directory with Sub Tree

TC LDAP Directory mit einem kundenspezifischen Aufbau (DIT):

- Die oben angegebenen Zertifikate werden über den TC TrustCenter LDAP Service mit einer kundenspezifischen DIT-Struktur veröffentlicht.
- DIT-Struktur: o=<meineFirma>, ou=pkigroups, dc=trustcenter, dc=de

6.2 LDAP Replikation

Option

EID-LDAP/Cust-O1-LDAP Replication: TC/Customer LDAP

Zur Nutzung der LDAP Replikation muss der TC LDAP Replication Client lokal installiert werden. Der TC LDAP Replication Client lädt regelmäßig neue ausgestellte Zertifikate und CRLs von dem zugehörigen TC Enterprise ID Account und fügt diese in den Ziel-LDAP ein.

- Microsoft Active Directory Server wird als Ziel-LDAP unterstützt.

6.3 Validierungsdienst

TC TrustCenter ermöglicht die Validierung sowohl über Sperrlisten (CRLs) als auch über den OCSP-Service.

Für die CRL gilt:

- CRLs werden mindestens einmal pro Woche erzeugt und sind über die TC TrustCenter Webseite zugreifbar.
- Die Zertifikate enthalten die URL der jeweiligen CRL als Erweiterungsfeld (Certificate Extension).
- Das Format für CRLs ist v2.

Der OCSP-Service hat folgende Eigenschaften:

- Konform zu RFC2560 (OCSP v1).
- OCSP-Requests müssen nicht signiert sein. Der OCSP-Service verlangt keine Authentifizierung des Anfragenden.
- Die URL des jeweiligen OCSP-Service ist im Zertifikat als Erweiterungsfeld (Certificate Extension) enthalten.



Option

EID-VAL/TC-O1-Premium-Validation

Premium validation Option für eine Branded CA (siehe Abschnitt 10.1).

- 1 Stunde Prozesszeit für Sperrungen,
- Alle anderen SLA Parameter bleiben unverändert.
- Diese Option ist nur für Branded CA, Branded Certificate Profiles oder Custom Certificate Products verfügbar.
- Diese Option setzt die Option EID-VAL/TC-O2-OCSP-for-Branded-CA voraus, falls OCSP Validierung benötigt wird.

Option

EID-VAL/TC-O2-OCSP-for-Branded-CA

OCSP Service für eine Branded CA (siehe Abschnitt 10.1).

- OCSP Service kompatibel zu RFC2560 (OCSPv1)
- OCSP Requests müssen nicht signiert sein. Es wird keine Authentifizierung für die Übermittlung von OCSP-Requests durchgeführt.
- Die URL des OCSP Responders sollte als Extension in den Zertifikaten enthalten sein.

7 Beantragung über SCEP

Zertifikate können über das Simple Certificate Enrollment Protocol (*SCEP*) beantragt werden. Dieses Protokoll wird typischerweise von Netzwerkgeräten unterstützt.

Die *SCEP* Beantragung kann gemäß der in Abschnitt 3.7 und 3.8 beschriebenen Abläufe erfolgen.

Hinweis: Nur Zertifikatsprodukte, deren Namen mit *SCEP* beginnen, sind für die Beantragung über das *SCEP* Protokoll geeignet,

Einige Apple Produkte unterstützen das *SCEP* Protokoll. TC Enterprise ID liefert zusätzlich zum Benutzerzertifikat noch zwei weitere Konfigurationsnachrichten (configuration payload) an das Gerät. Dies sind standardmäßig VPN Konfiguration und ein Web Clip.

Option

EID-VAL/TC-O1-MDM-Customized-Payload

Anpassung der zwei oben beschriebenen Konfigurationsnachrichten (configuration payload) für iPhones or iPads.

Hinweis: Die „Antrags-URL (*SCEP*)“ ermöglicht das Beantragen von Zertifikate ohne die Eingabe zusätzlicher Daten. Diese „Antrags-URI (*SCEP*)“ ist nicht im Zusammenhang mit der Zertifikatsbeantragung für Apple Produkte nutzbar. Der „Link für anonyme Zertifikatsanträge“ (siehe Abschnitt 3.7.5) ist für Produkte mit einer „Antrags-URL (*SCEP*)“ nicht verfügbar.

8 Beantragung über CMP

Zertifikate können über das „Certificate Management Protocol“ (CMPv2) beantragt werden. Dieses Protokoll wird typischerweise von Netzwerkgeräten (z.B. LTE eNodeBs gemäß 3GPP Standard) genutzt.

Der Ablauf der Zertifikatsbeantragung beginnt wie in den Abschnitten 3.8.1 und 3.8.3 beschrieben, gefolgt vom eigentlichen *CMP* Request. Es gelten folgende Abweichungen:

- Es wird keine Einmal-PIN verschickt,
- Die Antrags-URL ist statisch
- Jeder *CMP*-Request muss von einem „Enrollment Agent“ freigegeben werden.

Der in den Abschnitten 3.8.1 und 3.8.3 referenzierte Benutzer muss für das CMP-fähige Gerät verantwortlich sein. Er wird als Zertifikatsbesitzer eingetragen. Das Zertifikat selbst enthält Informationen über das Gerät. Das Gerät ist formal der Zertifikatsinhaber.

Hinweis: Es können nur benutzerspezifische und nicht recover-fähige Zertifikatsprodukte über *CMP* beantragt werden.

Hinweis: *CMP*. Requests müssen mit dem Hersteller Gerätezertifikat signiert sein. Das Hersteller spezifische CA Zertifikat muss vorab von TC TrustCenter konfiguriert werden.

Hinweis: The *CMP* Requesttypen *ir* (Initialization Request), *cr* (CertificationRequest), *kur* (Key Update Request), *pollreq* (Polling Request), und *certconf* (Certification Confirm) werden unterstützt. Die *CMP* Antworttypen *ip* (Initialization Response), *cp* (Certification Response), *kup* (Key Update Response), *pollrep* (Polling Response), *pkiconf*(Confirmation), und *error* (Error Message) werden unterstützt.

Hinweis: Der *CMP* Request muss die eindeutige Geräte-ID im Feld *CertTemplate.SubjectDN.CommonName*. beinhalten.

Option

EID-CMP/TC-O1-CMP-IP-Range-Restriction

Konfiguration einer Liste von IP Addressbereichen für *CMP* Geräte. Diese List wird einem „Enrollment Agent“ zugeordnet. Es können unterschiedlichen „Enrollment Agents“ genutzt werden, sofern sich die IP Adressen nicht überlappen.

Die *CMP* Antworten werden mit einem von einer der TC Root untergeordneten CA (intermediate CA) ausgestellten Zertifikat signiert.

Option**EID-CMP/TC-O2-CMP-Custom-Signing-Certificate**

Es wird ein kundenspezifisches Zertifikat zum signieren von *CMP* Nachrichten verwendet.. Benötigt die Optionen EID-CA/TC-O1-Branded-CA, EID-CA/TC-O2-Private-Root oder EID-CA/TC-O3-Private-Intermediate-CA. Das Signierzertifikat wird auf Basis des standardmäßigen TC TrustCenter *CMP* RA Zertifikatprofils unterhalb eine kundenspezifischen CA ausgestellt.

9 AutoEnrollment

AutoEnrollment ist ein optionales Leistungsmerkmal von TC Enterprise ID. Es ist nur verfügbar, wenn es explizit im Vertrag aufgeführt ist.

Option

EID-CA/TC-O1-MS-AutoEnrollment

- Unterstützung von Auto-Enrollment gemäß der Beschreibung in diesem Abschnitt.

TC Enterprise ID für Microsoft Auto-Enrollment kombiniert die schnelle Installation und gute Integration in die Microsoft Windows Umgebung mit hoher Sicherheit und geringen Betriebsaufwänden.

Auto Enrollment von Benutzer- und Systemzertifikaten vereinfacht das Ausrollen von Zertifikaten entscheidend. Dabei werden bereits verfügbare Authentisierungsmöglichkeiten für Benutzer und Computer verwendet.

Der Auto-Enrollment Server authentisiert sich selbst als API-Benutzer mittels Zertifikat. Dieser API-Benutzer benötigt die Rollen „PKI Administrator“ und ggf. „AE Server Production“. Dieser Benutzer wird von TC TrustCenter eingerichtet.

Die vordefinierten Zertifikatstemplates werden automatisch in das Active Directory publiziert. Sie decken die typischen Verwendungszwecke von Zertifikaten innerhalb der Microsoft Windows Umgebung ab.

Die Aktivierung von Auto Enrollment kann gruppenspezifisch mit dem Gruppenrichtlinien Snap-In für die Microsoft Management Console (MMC) erfolgen.

Die Anzahl der unterschiedlichen Zertifikatstypen pro Benutzer kann dabei durch das MMC Snap-In vorgegeben werden (siehe Abschnitt 9.1.2).

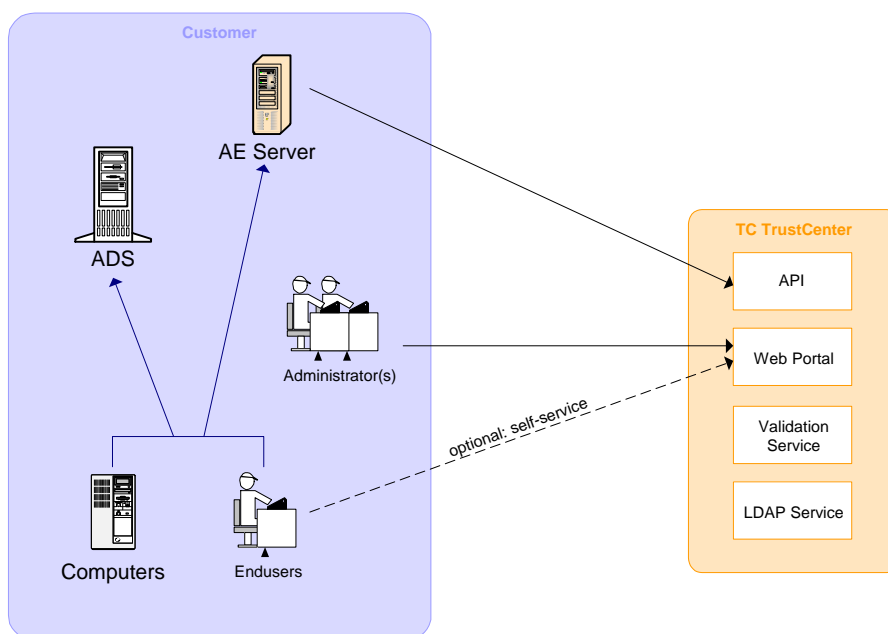


Abbildung 10 Auto-Enrollment Architektur

Nach der Aktivierung werden die jeweiligen Benutzer und Computer automatisch Zertifikate über das Microsoft Auto Enrollment Protokoll beantragen. Zertifikate können zusätzlich auch manuell mittels MMC Snap-In beantragt werden.

Zur Nutzung von Auto Enrollment ist keine zusätzliche Client-Software notwendig. Die Installation von Chipkartentreibern (CSP) bzw. PC/SC Treibern kann erforderlich sein, wenn die Zertifikate auf Chipkarte bzw. USB-Token gespeichert werden sollen.

9.1 Beantragen von Zertifikaten mittels Auto Enrollment

Benutzer- und Applikationszertifikate werden entweder automatisch oder manuell mit dem MMC Snap-In beantragt.

Benutzerzertifikate werden in TC Enterprise ID entweder dem bereits eingerichteten Benutzer zugewiesen oder es wird automatisch ein neuer Benutzer angelegt. Wird ein neuer Benutzer angelegt, so wird er nach folgender Regel einem „Affiliate“ (siehe Abschnitt 5.2) zugewiesen:

1. „Affiliate“, dessen Anzeigename mit dem im Active Directory Service (ADS) hinterlegten Unternehmensnamen übereinstimmt (wenn ein übereinstimmender „Affiliate“ gefunden wird)
2. „Affiliate“, dem der API Benutzer zugeordnet ist.

Applikationszertifikate werden immer dem API Benutzer selbst zugewiesen, d.h. der API Benutzer ist der *Zertifikatsbesitzer* für alle über Auto Enrollment beantragten Nicht-Benutzer-Zertifikate.

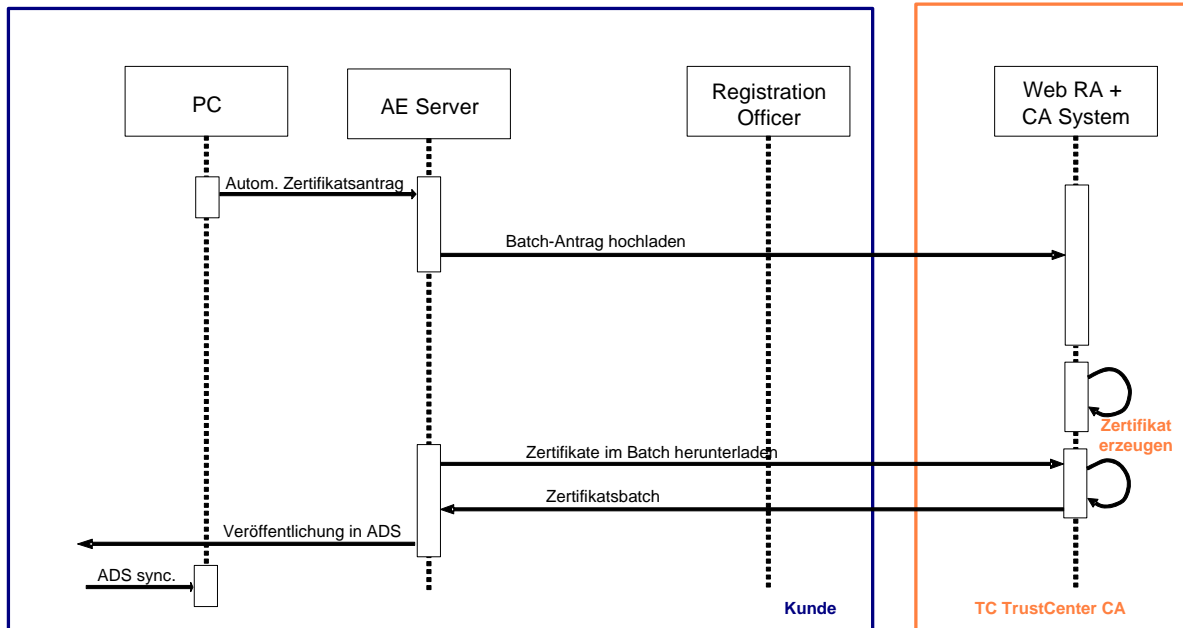


Abbildung 11 Auto-Enrollment Ablauf

9.1.1 Schlüsselarchivierung (Key Archiving)

Key Recovery ist für alle Zertifikatstemplates mit voreingestelltem Key Archival Flag möglich. In diesem Fall werden die Schlüsselpaare automatisch vom Client-System erzeugt und verschlüsselt an die CA übermittelt. Das dabei verwendete Schlüsselarchivierungszertifikat wird sicher von TC TrustCenter verwaltet. Der Wiederherstellungsprozess (Key Recovery) kann dann durch den *Administrator* eingeleitet werden (siehe Abschnitt 3.9.3).

9.1.2 Certificate Templates for AutoEnrollment

Die Zertifikatstemplates spiegeln die aktuelle PKI Konfiguration wieder. Einige dieser Zertifikatstemplate-Einstellungen können vom Kunden angepasst werden. TC Enterprise ID AutoEnrollment stellt viele vordefinierte Zertifikatstemplates bereit.

Die folgenden Screenshots wurden auf einem Microsoft Windows 2003 Server erstellt. Sie zeigen das Standard Microsoft Certificate Template Snap-In für die MMC. Alle vom Kunden änderbaren Einstellungen werden links neben dem Bild explizit aufgeführt.

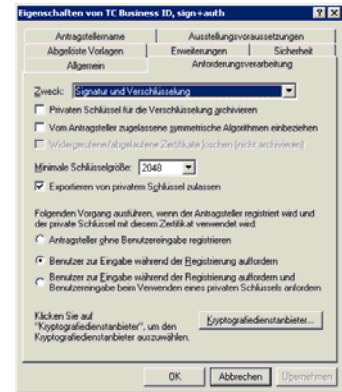
Registerkarte „Allgemein“

- „Erneuerungszeitraum“
- „Nicht automatisch neu registrieren, wenn ein identisches Zertifikat bereits in Active Directory vorhanden ist“



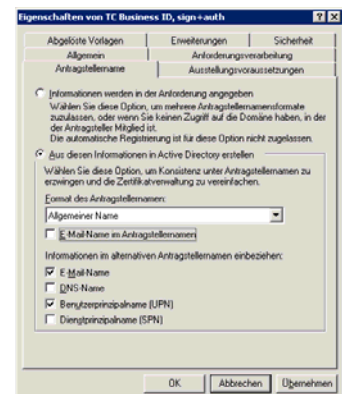
Registerkarte „Anforderungsverarbeitung“

- „Minimale Schlüsselgröße“
- „Exportieren von privatem Schlüssel zulassen“.
Achtung: Diese Einstellung muss für alle Templates mit Key Recovery aktiviert bleiben.
- „Antragsteller ohne Benutzereingabe registrieren“.
Achtung: Einige CSPs für Chipkarten bzw. USB-Token unterstützen keine Verwendung ohne Benutzereingaben.
- „Benutzer zur Eingabe während der Registrierung auffordern“
- „Benutzer zur Eingabe während der Registrierung auffordern und Benutzereingabe beim Verwenden eines privaten Schlüssels anfordern“.
- „Kryptografiedienstanbieter“, hier kann die Liste der zulässigen Kryptografiedienstanbieter/ Cryptographic Service Provider (CSPs) spezifiziert werden.



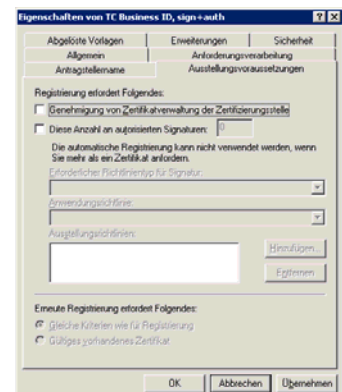
Registerkarte „Antragstellername“

- In dieser Registerkarte dürfen keine Änderungen vorgenommen werden. TC TrustCenter verwaltet diese Einträge zentral.



Registerkarte „Ausstellungsvoraussetzungen“

- In dieser Registerkarte dürfen keine Änderungen vorgenommen werden. TC TrustCenter verwaltet diese Einträge zentral.



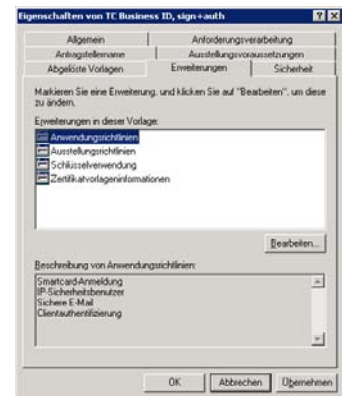
Registerkarte „Abgelöste Vorlagen“

- „Zertifikatvorlagen“.
Achtung: Einige Windows Services versuchen automatisch Zertifikate zu beantragen (z.B. Domain Controller). Neue Zertifikatvorlagen (Zertifikatstemplates) werden nur dann automatisch verwendet, wenn in diesen die ursprünglichen Vorlagen an dieser Stelle aufgeführt sind.



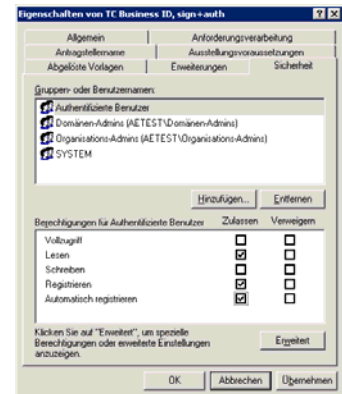
Registerkarte „Erweiterungen“

- In dieser Registerkarte dürfen keine Änderungen vorgenommen werden. TC TrustCenter verwaltet diese Einträge zentral.



Registerkarte „Sicherheit“

- „Gruppen- oder Benutzernamen“
- „Berechtigungen“ für Gruppen bzw. Benutzer. Mit diesen Einträgen kann die automatische Beantragung von Zertifikaten gesteuert werden. Die automatische Beantragung erfolgt, wenn die Rechte „Lesen“, „Registrieren“ und „Automatisch registrieren“ zugelassen sind.



Nicht aufgeführte Einstellungen dürfen nicht verändert werden, da TC TrustCenter die maßgeblichen Einstellungen verwaltet. Die ursprünglichen Werte können durch „Fetch Config“ des „AutoEnrollment Configuration“ Programmes wiederhergestellt werden.

Folgende Zertifikatstemplates sind für die Verwendung mit AutoEnrollment oder API-Enrollment vordefiniert.

9.1.2.1 AE TC Client Computer ID

Anwendungsfelder	Für EAP-TLS Authentisierung von Client-Rechnern am IAS Server. Kann zur Absicherung von WLAN Zugängen verwendet werden.
Schlüsselverwendung	Clientauthentifizierung
Abgelöste Templates	Keine
Beantragungsart	Antragsteller ohne Benutzereingabe registrieren

Zulässige CSPs	Microsoft RSA SChannel Cryptographic Provider
Gültigkeit	1 Jahr, 2 Jahre, 3 Jahre

9.1.2.2 AE TC Domain Controller Authentication

Anwendungsfelder	Microsoft Domänen Controller (KDC). Notwendig, um Smartcard-Anmeldung zu ermöglichen.
Schlüsselverwendung	Clientauthentifizierung, Serverauthentifizierung, Smartcard-Anmeldung
Abgelöste Templates	Domain Controller, Domain Controller Authentication
Beantragungsart	Antragsteller ohne Benutzereingabe registrieren
Zulässige CSPs	Microsoft RSA SChannel Cryptographic Provider
Gültigkeit	1 Jahr, 2 Jahre, 3 Jahre

9.1.2.3 AE TC RAS and IAS Server ID

Anwendungsfelder	EAP-TLS Authentisierung von IAS Servern. Kann zur Absicherung von WLAN Zugängen verwendet werden.
Schlüsselverwendung	Serverauthentifizierung
Abgelöste Templates	Keine
Beantragungsart	Antragsteller ohne Benutzereingabe registrieren
Zulässige CSPs	Microsoft RSA SChannel Cryptographic Provider
Gültigkeit	1 Jahr, 2 Jahre, 3 Jahre

9.1.2.4 AE TC Business ID

Anwendungsfelder	Microsoft Internet Explorer (SSL-Client Authentisierung), Microsoft Outlook (Sichere E-Mail), Smartcard-Anmeldung, ...
Schlüsselverwendung	Verschlüsselndes Dateisystem, Sichere E-Mail, Clientauthentifizierung
Abgelöste Templates	Keine
Beantragungsart	Benutzer zur Eingabe während der Registrierung auffordern
Zulässige CSPs	Keine Einschränkung
Gültigkeit	1 Jahr, 2 Jahre, 3 Jahre

9.1.2.5 AE TC Business ID, recoverable

Anwendungsfelder	Microsoft Internet Explorer (SSL-Client Authentisierung), Microsoft Outlook (Sichere E-Mail), Smartcard-Anmeldung, ...
Schlüsselverwendung	Verschlüsselndes Dateisystem, Sichere E-Mail,

	Clientauthentifizierung
Abgelöste Templates	Keine
Beantragungsart	Benutzer zur Eingabe während der Registrierung auffordern. Privaten Schlüssel zur Verschlüsselung archivieren.
Zulässige CSPs	Keine Einschränkung
Gültigkeit	1 Jahr, 2 Jahre, 3 Jahre

9.1.2.6 AE TC Business ID, sign+auth

Anwendungsfelder	Microsoft Internet Explorer (SSL-Client Authentisierung), Microsoft Outlook (Sichere E-Mail), ...
Schlüsselverwendung	Sichere E-Mail, Clientauthentifizierung, Smartcard- Anmeldung
Abgelöste Templates	Keine
Beantragungsart	Benutzer zur Eingabe während der Registrierung auffordern
Zulässige CSPs	Keine Einschränkung
Gültigkeit	1 Jahr, 2 Jahre, 3 Jahre

9.1.2.7 AE TC Business ID, sign

Anwendungsfelder	Microsoft Outlook (Sichere E-Mail), ...
Schlüsselverwendung	Sichere E-Mail
Abgelöste Templates	Keine
Beantragungsart	Benutzer zur Eingabe während der Registrierung auffordern
Zulässige CSPs	Keine Einschränkung
Gültigkeit	1 Jahr, 2 Jahre, 3 Jahre

9.1.2.8 AE TC Business ID, auth

Anwendungsfelder	Microsoft Internet Explorer (SSL-Client Authentisierung),
Schlüsselverwendung	Clientauthentifizierung, Smartcard-Anmeldung
Abgelöste Templates	Keine
Beantragungsart	Benutzer zur Eingabe während der Registrierung auffordern
Zulässige CSPs	Keine Einschränkung
Gültigkeit	1 Jahr, 2 Jahre, 3 Jahre

9.1.2.9 AE TC Business ID, recoverable enc

Anwendungsfelder	Microsoft Encrypting File System, Microsoft Internet Explorer (SSL-Client Authentisierung), Microsoft Outlook (Sichere E-
-------------------------	--

	Mail), ...
Schlüsselverwendung	Verschlüsselndes Dateisystem, Sichere E-Mail, Clientauthentifizierung
Abgelöste Templates	Keine
Beantragungsart	Benutzer zur Eingabe während der Registrierung auffordern. Privaten Schlüssel zur Verschlüsselung archivieren.
Zulässige CSPs	Keine Einschränkung
Gültigkeit	1 Jahr, 2 Jahre, 3 Jahre

10 Zertifikatsprofile

Dieser Abschnitt beschreibt die Zertifikatshierarchie und den Aufbau der Zertifikate.

10.1 Zertifikatshierarchie

Alle Zertifikate sind von einem der folgenden Root-Zertifikate ausgestellt:

- „TC Class 2 CA II“ Root-Zertifikat, über „TC Class 2 L1CA XI“ Sub-CA Zertifikat oder
- „TC Universal I“ Root-Zertifikat, über „TC Class 1 L1CA IX“ Sub-CA Zertifikat
- Adobe Root Zertifikat (CDS), über „TC TrustCenter CA for Adobe I“ Sub-CA Zertifikat.

Option

EID-CA/TC-O1-Branded-CA

Branded CA unterhalb der TC Root.

- Das Profil des CA Zertifikats muss spezifiziert und abgenommen werden.
- Diese Option beinhaltet keine Einrichtung von Zertifikatsprofilen (siehe Abschnitt 10.2)
- Die TC TrustCenter **CPD** / **CPS** sind maßgeblich.
- OCSP Service ist nicht Bestandteil dieser Option (siehe Abschnitt 6.3).

Option

EID-CA/TC-O2-Private-Root

Privates selbst-signiertes Root-Zertifikat. Dieses Root-Zertifikat ist in keinerlei Root-Store vorinstalliert.

- Das Profil des CA Zertifikats muss spezifiziert und abgenommen werden.
- Entweder sind die TC TrustCenter **CPD** / **CPS** oder kundenspezifische CPD / CPS maßgeblich. Das Schreiben von kundenspezifischen CPD / CPS ist nicht in dieser Option enthalten.

Option

EID-CA/TC-O3-Private-Intermediate-CA

Branded CA ausgestellt von einer Privaten Root.

- Das Profil des CA Zertifikats muss spezifiziert und abgenommen werden.
- Diese Option beinhaltet keine Einrichtung von Zertifikatsprofilen (siehe Abschnitt 10.2)
- Die CPD / CPS der zugehörigen Root sind maßgeblich.
- OCSP Service ist nicht Bestandteil dieser Option (siehe Abschnitt 6.3).

10.2 Zertifikatsprodukte

Die folgenden Zertifikatsprodukte sind generell in TC Enterprise ID verfügbar. Die für einen speziellen Account verfügbaren Zertifikatsprodukte sind im jeweiligen „Vertrag“ aufgeführt.

Basisname	Art	Gültigkeit	CA	Kommentar
TC Business ID Demo	Wiederherstellbar und nicht wiederherstellbar	30 Tage	Class 1	Nur zum Testen
TC Business ID for Adobe Demo	PDF Signatur	30 Tage	CDS	Nur zum Testen
TC Trust SSL Demo		30 Tage	Class 0	Nur zum Testen
TC Personal ID		1 Jahr, 2 Jahre, 3 Jahre	Class 1	Ein Zertifikat für 3 Zwecke: Signieren, Authentisieren und Verschlüsseln. Das O-Feld muss leer sein. Dieser Typ ist für externe Partner gedacht.
TC Business ID	Wiederherstellbar und nicht wiederherstellbar	1 Jahr, 2 Jahre, 3 Jahre	Class 2	Ein Zertifikat für 3 Zwecke: Signieren, Authentisieren und Verschlüsseln
	Signieren und Authentifizieren (sign+auth)	1 Jahr, 2 Jahre, 3 Jahre	Class 2	Nur zum Signieren und Authentifizieren
	Signieren	1 Jahr, 2 Jahre, 3 Jahre	Class 2	Nur zum Signieren

Basisname	Art	Gültigkeit	CA	Kommentar
	Authentisierung (Authentication)	1 Jahr, 2 Jahre, 3 Jahre	Class 2	Nur zum Authentifizieren
	Wiederherstellbar nur für Verschlüsselung (recoverable enc)	1 Jahr, 2 Jahre, 3 Jahre	Class 2	Nur für Verschlüsselung
TC Business ID for Adobe	PDF Signatur	1 Jahr, 2 Jahre, 3 Jahre	CDS	Nur für PDF Signatur
TC Enrollment Agent ID		1 Jahr, 2 Jahre, 3 Jahre	Class 2	Für „Enrollment Agents“ benötigt
TC Domain Controller ID		1 Jahr, 2 Jahre, 3 Jahre	Class 2	Wird benötigt um Smartcard Logon implementieren zu können.
TC RAS and IAS Server ID		1 Jahr, 2 Jahre, 3 Jahre	Class 2	Für sicheren WLAN Zugang benötigt
TC Client Computer ID		1 Jahr, 2 Jahre, 3 Jahre	Class 2	Für sicheren WLAN Zugang benötigt
TC Team Certificate		1 Jahr, 2 Jahre, 3 Jahre	Class 2	Ein Zertifikat für ein Team. Es ist für 3 Zwecke nutzbar: Signieren, Authentifizieren und Verschlüsseln.
TC Publisher ID for Adobe AIR		1 Jahr, 2 Jahre, 3 Jahre	Class 2	Code Signing Zertifikat
TC Publisher ID for Java Desktop		1 Jahr, 2 Jahre, 3 Jahre	Class 2	Code Signing Zertifikat
TC Publisher ID for Microsoft Authenticode		1 Jahr, 2 Jahre, 3 Jahre	Class 2	Code Signing Zertifikat

Alle wiederherstellbaren Zertifikate werden als *PKCS#12 PSEs* ausgestellt und verteilt. Für alle anderen Zertifikate erfolgt die Schlüsselgenerierung entweder durch den Web-Browser oder extern durch Hochladen des *PKCS#10 Requests* (TC Trust SSL, TC Trust SSL Wildcard, TC Extended Trust SSL, TC Domain Controller ID, TC Client Computer ID und TC RAS and IAS Server ID).

Der *Administrator* kann Zertifikatsprodukte als inaktiv kennzeichnen. Inaktive Zertifikatsprodukte können beim „Zertifikat anfordern“ und Erstellen einer Zertifikatseinladung nicht ausgewählt werden.

Option

EID-CA/TC-O3-Branded-Certificate-Product

Anpassen eines Standard Zertifikatsproduktes, so dass es von einer Branded CA ausgestellt wird (siehe oben).

- Keine weiteren Änderungen des Zertifikatsproduktes sind möglich (siehe Abschnitt 10.1).
- Für dieses Zertifikatsprodukt sind entweder die TC TrustCenter **CPD / CPS** oder kundenspezifische CPD / CPS maßgeblich. Das Schreiben von kundenspezifischen CPD / CPS ist nicht in dieser Option enthalten.

Option

EID-CA/TC-O4-Custom-Certificate-Product

Zertifikatsprodukt mit kundenspezifisch angepasstem Profil.

- Das Zertifikatsprofil muss spezifiziert und abgenommen werden.
- Das Zertifikat wird von einer bereits eingerichteten CA ausgestellt.

11 Service Levels

Der Standard Service Level ist „Bronze“. Einzelheiten finden Sie in der untenstehenden SLA Übersicht.

Die Support Service Level (inkl. Antwortzeiten und Fehlerprioritäten) sind in dem Dokument [Support SLA](https://www.verisign.com/repository/service_description) erhältlich unter https://www.verisign.com/repository/service_description beschrieben.

Option EID-SLA/TC-O1-Platinum-SLA „Platinum“ Service Level anstelle von „Gold“. Einzelheiten wie in der untenstehenden SLA Übersicht beschrieben.

SLA Übersicht	Wert "Bronze"	Wert "Platin"
Ausstellen von Zertifikaten		
Betriebszeit		
Betriebszeit: Einzelbeantragung von Zertifikaten	Mo–So: 0:00 – 24:00 UTC; mit Ausnahme des Wartungsfensters entweder Fr: 16:00 – 21:00 UTC oder Samstag 8:00- 16:00 UTC	Mo–So: 0:00 – 24:00 UTC; mit Ausnahme des Wartungsfensters entweder Fr: 16:00 – 21:00 UTC oder Samstag 8:00- 16:00 UTC
Betriebszeit: Batchbeantragung von Zertifikaten	Mo–So: 0:00 – 24:00 UTC; mit Ausnahme des Wartungsfensters entweder Fr: 16:00 – 21:00 UTC oder Samstag 8:00- 16:00 UTC	Mo–So: 0:00 – 24:00 UTC; mit Ausnahme des Wartungsfensters entweder Fr: 16:00 – 21:00 UTC oder Samstag 8:00- 16:00 UTC
Betriebszeit: Einzelausstellung von Zertifikaten	Mo–So: 0:00 – 24:00 UTC; mit Ausnahme des Wartungsfensters entweder Fr: 16:00 – 21:00 UTC oder Samstag 8:00- 16:00 UTC	Mo–So: 0:00 – 24:00 UTC; mit Ausnahme des Wartungsfensters entweder Fr: 16:00 – 21:00 UTC oder Samstag 8:00- 16:00 UTC
Betriebszeit: Batchausstellung von Zertifikaten	Mo–So: 0:00 – 24:00 UTC; mit Ausnahme des Wartungsfensters entweder Fr: 16:00 – 21:00 UTC oder Samstag 8:00- 16:00 UTC	Mo–So: 0:00 – 24:00 UTC; mit Ausnahme des Wartungsfensters entweder Fr: 16:00 – 21:00 UTC oder Samstag 8:00- 16:00 UTC
Betriebszeit: Freischaltung von Zertifikatsanträgen	Mo–So: 0:00 – 24:00 UTC; mit Ausnahme	Mo–So: 0:00 – 24:00 UTC; mit Ausnahme

	des Wartungsfensters entweder Fr: 16:00 – 21:00 UTC oder Samstag 8:00- 16:00 UTC	des Wartungsfensters entweder Fr: 16:00 – 21:00 UTC oder Samstag 8:00- 16:00 UTC
Verfügbarkeit		
Verfügbarkeitsgrad: Einzelbeantragung von Zertifikaten	98.5% pro Monat	99.5% pro Monat
Verfügbarkeitsgrad: Batchbeantragung von Zertifikaten	98.5% pro Monat	99.5% pro Monat
Verfügbarkeitsgrad: Freischaltung von Zertifikatsanträgen	98.5% pro Monat	99.5% pro Monat
Maximale zusammenhängende Nichtverfügbarkeitszeit: Einzelbeantragung von Zertifikaten	8 Stunden	3 Stunden
Maximale zusammenhängende Nichtverfügbarkeitszeit: Batchbeantragung von Zertifikaten	8 Stunden	3 Stunden
Maximale zusammenhängende Nichtverfügbarkeitszeit: Freischaltung von Zertifikatsanträgen	8 Stunden	3 Stunden
Prozesszeit / Performance		
Maximale Prozesszeit: Einzelbeantragung von Zertifikaten	95% in 90 Minuten	95% in 60 Minuten
Maximale Prozesszeit: Batchbeantragung von Zertifikaten	Alle bis 15:00 Uhr erhaltenen Batches werden bis 12:00 Uhr am folgenden Arbeitstag bearbeitet.	Alle bis 15:00 Uhr erhaltenen Batches werden bis 12:00 Uhr am folgenden Arbeitstag bearbeitet
Reservierte Kapazität		
Maximale Anzahl pro Zeiteinheit: Einzelbeantragung von Zertifikaten	500 pro Tag und 1 pro Minute	1000 pro Tag und 1 pro Minute
Maximale Anzahl pro Zeiteinheit: Batchbeantragung von Zertifikaten	10 Batches/ Tag, 1 Batch/ Minute, max. 100 Anträge pro Batch	15 Batches/ Tag, 1 Batch/ Minute, max. 100 Anträge pro Batch
Maximale Online Datenhaltungszeit von wiederherstellbaren privaten Schlüsseln (PKCS#12 PSEs)	10 Jahre, wenn ein ununterbrochenes Vertragsverhältnis für den betreffenden Account besteht.	10 Jahre, wenn ein ununterbrochenes Vertragsverhältnis für den betreffenden Account besteht.
Verwaltung von Zertifikaten		
Betriebszeit		
Betriebszeit: Sperrung und Suspendierung von Zertifikaten	Mo–So: 0:00 – 24:00 UTC; mit Ausnahme des Wartungsfensters entweder Fr: 16:00 – 21:00 UTC oder	Mo–So: 0:00 – 24:00 UTC; mit Ausnahme des Wartungsfensters entweder Fr: 16:00 – 21:00 UTC oder

	Samstag 8:00- 16:00 UTC	Samstag 8:00- 16:00 UTC
Betriebszeit: Validieren von Zertifikaten (OCSP)	Mo–So: 0:00 – 24:00 UTC; mit Ausnahme des Wartungsfensters entweder Fr: 16:00 – 21:00 UTC oder Samstag 8:00- 16:00 UTC	Mo-Su: 0:00 – 24:00
Betriebszeit: LDAP Replikation	Mo–So: 0:00 – 24:00 UTC; mit Ausnahme des Wartungsfensters entweder Fr: 16:00 – 21:00 UTC oder Samstag 8:00- 16:00 UTC	Mo–So: 0:00 – 24:00 UTC; mit Ausnahme des Wartungsfensters entweder Fr: 16:00 – 21:00 UTC oder Samstag 8:00- 16:00 UTC
Verfügbarkeit		
Verfügbarkeitsgrad: Sperren von Zertifikaten	98.5% pro Monat	99.5% pro Monat
Verfügbarkeitsgrad: Validieren von Zertifikaten (OCSP)	98.5% pro Monat	99.5% pro Monat
Verfügbarkeitsgrad: Directory Service (LDAP)	98.5% pro Monat	99.5% pro Monat
Maximale zusammenhängende Nichtverfügbarkeitszeit: Sperrung und Suspendierung von Zertifikaten	8 Stunden	3 Stunden
Maximale zusammenhängende Nichtverfügbarkeitszeit: Certificate Validation (OCSP)	8 Stunden	3 Stunden
Maximale zusammenhängende Nichtverfügbarkeitszeit: Directory Service (LDAP)	8 Stunden	3 Stunden
Prozesszeit / Performance		
Maximale Prozesszeit: Einzel-Sperrung und -Suspendierung von Zertifikaten	25 Stunden	25 Stunden
Maximale Prozesszeit: Batch-Sperrung und -Suspendierung von Zertifikaten	49 Stunden	49 Stunden
Reservierte Kapazität		
Maximale Anzahl pro Zeiteinheit: Einzel-Sperrung und -Suspendierung von Zertifikaten	100/Tag, 1/Minute	200/Tag, 1/Minute
Maximale Anzahl pro Zeiteinheit: Batch-Sperrung und -Suspendierung von Zertifikaten	10 Batches/ Tag, 1 Batch/ Minute, max. 100 Anträge pro Batch	15 Batches/ Tag, 1 Batch/ Minute, max. 100 Anträge pro Batch
Maximale Anzahl pro Zeiteinheit: Validierung von Zertifikaten (OCSP)	170 pro Benutzer und Jahr (1 Zert. pro Benutzer) 200 pro Benutzer und Jahr (2 Zert. pro	170 pro Benutzer und Jahr (1 Zert. pro Benutzer) 200 pro Benutzer und Jahr (2 Zert. pro



	Benutzer) 300 pro Benutzer und Jahr (3 Zert. pro Benutzer)	Benutzer) 300 pro Benutzer und Jahr (3 Zert. pro Benutzer)
Maximale Anzahl pro Zeiteinheit: Directory Service (LDAP)	130 pro Benutzer und Jahr	130 pro Benutzer und Jahr

11.1 Verletzung von SLA-Werten

Gegenstand von SLA-Werten können Betriebszeiten, Prozesszeiten, Kapazitäten oder messbare Verfügbarkeitsgrade seitens TC TrustCenter für Beantragung, Freischaltung, Sperrung oder Verwaltung der Zertifikate sowie LDAP-Replikation innerhalb des Bemessungszeitraumes sein.

Die Parteien vereinbaren eine abschließende Kompensationszahlung für die Verletzung von SLA-Werten. Wurde in drei aufeinander folgenden Betriebsmonaten derselbe SLA-Wert verletzt, beträgt die Kompensationszahlung 2 % des monatlichen Betriebsentgeltes zuzüglich des möglichen SLA-Entgeltes. Die Kompensationszahlungen können vom Kunden kumuliert über alle Monate und SLA-Werte einmal jährlich am Ende des Betriebsjahres geltend gemacht werden. Die Höhe der maximalen monatlichen Kompensationszahlung beträgt höchstens 10 % der gesamten Betriebsentgeltes zuzüglich des möglichen SLA-Entgeltes. Sind keine monatlichen Entgeltzahlungen vereinbart, ist die monatliche Vergütung anteilig aus den vereinbarten Entgelten zu errechnen.

TC TrustCenter ist gesetzlich verpflichtet, die Vorgaben zur Ausführungkontrolle einzuhalten. In Zweifelsfällen können sich die Aktionen, wie z.B. die Ausstellung von Zertifikaten, durch eine notwendige manuelle Prüfung der Daten verzögern. Eine derartige Verzögerung stellt keine SLA-Verletzung im Sinne dieses Abschnitts dar.

11.1.1 Unangekündigte Unterbrechungen

Unter bestimmten Umständen kann es notwendig sein, dass TC TrustCenter dringende Maßnahmen wie die vorübergehende Unterbrechung der Dienste oder die Sperrung des Zugangs vom und zum Internet ergreifen muss, um die Sicherheit des Rechenzentrums oder die Behebung von betriebsbedingten Störungen zu gewährleisten. TC TrustCenter wird den Kunden in angemessener Weise frühzeitig über die Absicht, die Dienste vorübergehend zu unterbrechen, benachrichtigen und die Dauer der Unterbrechung so gering wie möglich halten.

In den Fällen, dass TC TrustCenter einen Sicherheitsverstoß feststellt, wie etwa die Nutzung der Systeme des Kunden zum Ausspähen oder Angreifen von anderen Kunden von TC TrustCenter, oder den Fällen einer festgestellten Bedrohung der Einrichtungen von TC TrustCenter ausgehend von Systemen des Kunden, wird TC TrustCenter sofortige Maßnahmen zur vorübergehenden Sperrung des Zugangs des Kunden einleiten. In diesen Fällen wird TC TrustCenter den Kunden möglichst umgehend nach Einleiten der Maßnahme hierüber in Kenntnis setzen. Andere unangekündigte Unterbrechungen, wie solche die durch den Ausfall von Geräten und Maschinen verursacht werden, wird TC TrustCenter dem Kunden umgehend nach ihrer Entdeckung melden.

Umgekehrt wird der Kunde TC TrustCenter über jede Unterbrechung benachrichtigen, die noch nicht durch TC TrustCenter gemeldet wurde. TC TrustCenter wird so schnell wie möglich die notwendigen Maßnahmen für die Wiederaufnahmen der unterbrochenen Leistungen einleiten. Im Fall etwaiger Ausfälle von Datenübermittlungssystemen wird TC TrustCenter angemessene Maßnahmen ergreifen, um die Verfügbarkeit der Datenübermittlungssysteme wieder herzustellen; allerdings übernimmt TC TrustCenter keine Verantwortung für die Verfügbarkeit von Datenübermittlungssystemen Dritter.

12 Glossar

Administrator	Dies kann ein „PKI Superadministrator“, ein „PKI Administrator“ oder eine beliebige delegierte Rolle („Registration Officer“, „Enrollment Officer“, „Unsuspendation Officer“, „Revocation Officer“, „Key Recovery Officer“) sein. Siehe Abschnitt 2.1.1
Applikationszertifikate	Bei Applikationszertifikaten sind <i>Zertifikatsinhaber</i> und <i>Zertifikatsbesitzer</i> nicht identisch. Beim <i>Zertifikatsinhaber</i> handelt es sich um die Applikation selbst (also z.B. ein Web-Server oder ein E-Mail-Gateway oder eine andere Applikation). Beim <i>Zertifikatsbesitzer</i> handelt es sich typischerweise um den <i>Administrator</i> der Applikation. „TC DomainController ID“ ist ein typisches Beispiel für ein Applikationszertifikat. Siehe Abschnitt 2.2
Basisbenutzer	Eine der möglichen Rollen eines Benutzers. Die Rollen sind in Abschnitt 2.1.1 aufgeführt und erklärt.
Benutzer	Eine Person, die ein Zertifikat aus TC Enterprise ID erhalten hat bzw. eine Person, die das Web-Portal zum Beantragen und zum Sperren, Suspendieren, Desuspendieren sowie zum Initiieren von <i>Key Recovery</i> nutzt, wird als Benutzer bezeichnet – unabhängig von ihrer konkreten Rolle. Siehe Abschnitt 2
Benutzerzertifikate	Bei Benutzerzertifikaten sind <i>Zertifikatsinhaber</i> und <i>Zertifikatsbesitzer</i> identisch. „TC Business ID“ ist ein typisches Beispiel für ein Benutzerzertifikat. Siehe Abschnitt 3.4
Enrollment Agent	Eine der möglichen delegierten Rollen eines Benutzers. Die Rollen sind in Abschnitt 2.1.1 aufgeführt und erklärt. Personalisierung von Chipkarten oder anderen kryptografischen Token für den Benutzer. Diese Rolle kann nur durch den „PKI Superadministrator“ bzw. TC TrustCenter zugewiesen werden.
Enrollment Officer	Eine der möglichen delegierten Rollen eines Benutzers. Die Rollen sind in Abschnitt 2.1.1 aufgeführt und erklärt. Die Officer-Rollen sollten üblicherweise in Kombination mit dem „Privilegierten Benutzer“ oder „Basisbenutzer“ vergeben werden, um das Beantragen von eigenen Zertifikaten zu ermöglichen.

CMP	<p>Certificate Management Protocol. Siehe http://en.wikipedia.org/wiki/Certificate_Management_Protocol für Details.</p> <p>CMP Unterstützung ist in Abschnitt Fehler! Verweisquelle konnte nicht gefunden werden. beschrieben.</p>
CSP	<p>Cryptographic Service Provider. Das ist ein spezieller Treiber zur Nutzung von Chipkarten oder USB-Token durch Anwendungen, wie z.B. MS Internet Explorer oder MS Outlook.</p> <p>Siehe auch PKCS#11.</p>
ePIN	<p>Elektronische PIN. Eine über E-Mail bzw. SMS vom Portal übertragene PIN wird als ePIN bezeichnet.</p> <p>Siehe Abschnitt 3.3</p>
Externe PIN	<p>Eine PIN, die vom <i>Administrator</i> an den Benutzer oder vom <i>Administrator</i> dem Portal übermittelt wird, wird als Externe PIN bezeichnet. Die Verwaltung der Externen PINs erfolgt außerhalb des Systems.</p> <p>Siehe Abschnitt 3.3</p>
Externer Benutzer	<p>Eine der möglichen Rollen eines Benutzers. Die Rollen sind in Abschnitt 2.1.1 aufgeführt und erklärt.</p>
Key Escrow	<p>Das Wiederherstellen von privatem Schlüssel und Zertifikat ohne Mitwirkung des Besitzers.</p>
Key Escrow Administrator (Request)	<p>Eine der möglichen delegierten Rollen eines Benutzers.</p> <p>Initiieren von <i>Key Escrow</i>. Diese Rolle kann nur durch TC TrustCenter vergeben werden.</p>
Key Escrow Administrator (PSE)	<p>Eine der möglichen delegierten Rollen eines Benutzers.</p> <p>Hat das Recht im Rahmen von <i>Key Escrow</i> über die API auf die PKCS#12 PSE zuzugreifen. Diese Rolle kann nur durch TC TrustCenter vergeben werden.</p>
Key Recovery	<p>Das Wiederherstellen von privatem Schlüssel und Zertifikat.</p> <p>Siehe Abschnitt 3.9</p>
Key Recovery Officer	<p>Eine der möglichen delegierten Rollen eines Benutzers. Die Rollen sind in Abschnitt 2.1.1 aufgeführt und erklärt.</p> <p>Die Officer-Rollen sollten üblicherweise in Kombination mit dem „Privilegierten Benutzer“ oder „Basisbenutzer“ vergeben werden, um das Beantragen von eigenen Zertifikaten zu ermöglichen.</p>

NoLogin Benutzer	Eine der möglichen delegierten Rollen eines Benutzers. Die Rollen sind in Abschnitt 2.1.1 aufgeführt und erklärt.
PIN Brief Administrator	<p>Eine der möglichen Rollen eines Benutzers. Die Rollen sind in Abschnitt 2.1.1 aufgeführt und erklärt.</p> <p>Drucken von PIN Briefen. Diese Rolle kann nur durch TC TrustCenter vergeben werden.</p>
PKCS#10	<p>PKCS#10 ist ein Zertifikatsrequest. Er enthält den öffentlichen Schlüssel sowie den beantragten Namen des <i>Zertifikatsinhabers</i>.</p> <p>Die Kodierung kann entweder binär (DER) oder PEM sein. PEM kodierte Dateien enthalten ausschließlich anzeigbare Zeichen und beginnen mit „-----“ (5 '-' Zeichen).</p> <p>Alle wiederherstellbaren Zertifikate werden als <i>PKCS#12 PSEs</i> ausgestellt und verteilt. Für alle anderen Zertifikate erfolgt die Schlüsselgenerierung entweder durch den Web-Browser oder extern durch Hochladen des <i>PKCS#10</i> Requests (TC Trust SSL, TC Trust SSL Wildcard, TC Extended Trust SSL, TC Domain Controller ID, TC Client Computer ID und TC RAS and IAS Server ID)..</p> <p>Siehe Abschnitte 3.4 und 10.2.</p>
PKCS#11	<p>Standard-Schnittstelle zur Verwendung von Chipkarten und USB-Token.</p> <p>Anwendungen, wie z.B. Firefox benutzen derartige Treiber zum Zugriff auf Chipkarten bzw. USB-Token.</p> <p>Siehe auch CSP.</p>
PKCS#12 PSE	<p>Ein Personal Security Environment enthält den privaten Schlüssel sowie das zugehörige Zertifikat. Personal Security Environment kodiert gemäß dem im PKCS#12 Standard beschriebenen Format.</p> <p>In Umgebungen mit Microsoft Windows Betriebssystem wird es üblicherweise als „PFX“-Datei bezeichnet.</p> <p>Alle wiederherstellbaren Zertifikate werden als <i>PKCS#12 PSEs</i> ausgestellt und verteilt. Für alle anderen Zertifikate erfolgt die Schlüsselgenerierung entweder durch den Web-Browser oder extern durch Hochladen des <i>PKCS#10</i> Requests (TC Trust SSL, TC Trust SSL Wildcard, TC Extended Trust SSL, TC Domain Controller ID, TC Client Computer ID und TC RAS and IAS Server ID)..</p> <p>Bei Key Recovery werden die Zertifikate als PKCS#12 PSEs ausgestellt und verteilt (siehe Abschnitte 3.9 und 3.9.3).</p>
PKI Administrator	<p>Eine der möglichen Rollen eines Benutzers. Die Rollen sind in Abschnitt 2.1.1 aufgeführt und erklärt.</p> <p>Der „PKI Administrator“ kann anderen Benutzern folgende delegierte</p>

Rollen zuweisen: „Revocation Officer“, „Key Recovery Officer“.

PKI Superadministrator	<p>Eine der möglichen Rollen eines Benutzers. Die Rollen sind in Abschnitt 2.1.1 aufgeführt und erklärt.</p> <p>Der „PKI Superadministrator“ kann anderen Benutzern folgende delegierte Rollen zuweisen: „Registration Officer“, „Enrollment Officer“, „Unsuspendation Officer“, „Revocation Officer“, „Key Recovery Officer“.</p>
Privilegierter Benutzer	<p>Eine der möglichen Rollen eines Benutzers. Die Rollen sind in Abschnitt 2.1.1 aufgeführt und erklärt.</p>
Registration Officer	<p>Eine der möglichen delegierten Rollen eines Benutzers. Die Rollen sind in Abschnitt 2.1.1 aufgeführt und erklärt.</p> <p>Die Officer-Rollen sollten üblicherweise in Kombination mit dem „Privilegierten Benutzer“ oder „Basisbenutzer“ vergeben werden, um das Beantragen von eigenen Zertifikaten zu ermöglichen.</p>
Revocation Officer	<p>Eine der möglichen delegierten Rollen eines Benutzers. Die Rollen sind in Abschnitt 2.1.1 aufgeführt und erklärt.</p> <p>Die Officer-Rollen sollten üblicherweise in Kombination mit dem „Privilegierten Benutzer“ oder „Basisbenutzer“ vergeben werden, um das Beantragen von eigenen Zertifikaten zu ermöglichen.</p>
SCEP	<p>Simple Certificate Enrollment Protocol. Siehe http://en.wikipedia.org/wiki/Simple_Certificate_Enrollment_Protocol.</p> <p>Die Unterstützung von <i>SCEP</i> ist in Abschnitt 7 beschrieben.</p>
SCEP Benutzer	<p>Eine der möglichen Rollen eines Benutzers. Die Rollen sind in Abschnitt 2.1.1 aufgeführt und erklärt.</p> <p>Dieser Benutzer ist der Besitzer aller anonym über <i>SCEP</i> beantragten Zertifikate. Diese Rolle darf mit keinen weiteren Rollen kombiniert werden.</p>
Unsuspendation Officer	<p>Eine der möglichen delegierten Rollen eines Benutzers. Die Rollen sind in Abschnitt 2.1.1 aufgeführt und erklärt.</p> <p>Die Officer-Rollen sollten üblicherweise in Kombination mit dem „Privilegierten Benutzer“ oder „Basisbenutzer“ vergeben werden, um das Beantragen von eigenen Zertifikaten zu ermöglichen.</p>
Zertifikatsbesitzer	<p>Das ist der Benutzer, dem ein Zertifikat zugeordnet ist.</p> <p>Es kann der <i>Administrator</i> der Applikation sein (Applikationszertifikate) oder der <i>Zertifikatsinhaber</i> (Benutzerzertifikate).</p> <p>Bei Benutzerzertifikaten sind <i>Zertifikatsinhaber</i> und <i>Zertifikatsbesitzer</i> identisch. Bei Applikationszertifikaten ist der <i>Zertifikatsinhaber</i> die Applikation selbst, der <i>Zertifikatsbesitzer</i> ist in der Regel der</p>

Administrator der Applikation.

Siehe Abschnitte 3.10, 3.4

Zertifikatsinhaber

Das ist die im Zertifikat genannte Entität.

Es kann eine natürliche Person sein (Benutzerzertifikate), ein Team (Team Zertifikate) oder eine Anwendung bzw. ein Server (Applikationszertifikate).

Bei Benutzerzertifikaten sind *Zertifikatsinhaber* und *Zertifikatsbesitzer* identisch. Bei Applikationszertifikaten ist der Zertifikatsinhaber die Applikation selbst, der *Zertifikatsbesitzer* ist in der Regel der *Administrator* der Applikation.

Siehe Abschnitt 3.4

13 Abbildungsverzeichnis

Abbildung 1 Architekturübersicht _____	5
Abbildung 2 Antragsprozess nicht wiederherstellbarer Benutzerzertifikate für „Basisbenutzer“ _____	18
Abbildung 3 Antragsprozess wiederherstellbarer Benutzerzertifikate für „Basisbenutzer“ _____	20
Abbildung 4 Antragsprozess nicht wiederherstellbarer Benutzerzertifikate für „Privilegierte Benutzer“ _____	21
Abbildung 5 Antragsprozess wiederherstellbarer Benutzerzertifikate für „Privilegierte Benutzer“ _____	22
Abbildung 6 Zertifikatseinladung für nicht wiederherstellbare Zertifikate im Einzelverfahren _____	25
Abbildung 7 Zertifikatseinladung für wiederherstellbare Zertifikate im Einzelverfahren _____	26
Abbildung 8 Ablauf des Sperrens bzw. Suspendierens durch „PKI Administrator“ / „Revocation Officer“ _____	29
Abbildung 9 Ablauf des Sperrens bzw. Suspendierens durch den <i>Zertifikatsbesitzer</i> _____	30
Abbildung 10 Auto-Enrollment Architektur _____	49
Abbildung 11 Auto-Enrollment Ablauf _____	50