



TC TrustCenter

TC ID Store

Statement of Service

TC ID Store
Version 1.8.1

Hamburg, Germany
July 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

Table of Contents

| | | |
|----------|--|-----------|
| 1 | Web-based Registration Authority (RA) | 5 |
| 2 | Managing Users | 6 |
| 2.1 | Adding Users | 6 |
| 2.1.1 | User Roles | 7 |
| 2.1.2 | Administering User Groups | 11 |
| 2.2 | Searching, Modifying, Removing Users or disabling User Login | 11 |
| 3 | Managing Certificates | 13 |
| 3.1 | Certificate Validity | 13 |
| 3.2 | Number of Certificates per User | 13 |
| 3.3 | PIN-Methods | 13 |
| 3.4 | Key Generation Policy | 14 |
| 3.5 | Key Provider | 15 |
| 3.6 | Product Options | 15 |
| 3.7 | Requesting Certificates | 15 |
| 3.7.1 | Issuance of non-recoverable Client Certificates for “Basic Users” | 16 |
| 3.7.2 | Issuance of recoverable Client Certificates for “Basic Users” | 17 |
| 3.7.3 | Issuance of non-recoverable Client Certificates for “Privileged Users” | 18 |
| 3.7.4 | Issuance of recoverable Client Certificates for “Privileged Users” | 19 |
| 3.7.5 | Requesting Certificates by Anonymous Users | 21 |
| 3.8 | Triggering Certificate Requests for Other Users | 21 |
| 3.8.1 | Single mode certificate invite process for non-recoverable certificates | 22 |
| 3.8.2 | Single mode certificate invite process for recoverable certificates | 23 |
| 3.8.3 | Batch mode certificate invite process for non-recoverable certificates | 24 |
| 3.8.4 | Batch mode certificate invite process for recoverable certificates | 25 |
| 3.9 | Revoking, Suspending or Unsuspending certificates or Initiating Key Recovery | 25 |
| 3.9.1 | Revocation/Suspension of Certificates | 26 |
| 3.9.2 | Unsuspending of Certificates | 28 |
| 3.9.3 | Key Recovery | 28 |
| 3.10 | Key Escrow | 29 |
| 3.11 | Change Certificate Owner | 30 |
| 3.12 | Verify SSL Server Installation | 31 |
| 4 | Reports | 33 |
| 4.1 | Activity Report | 33 |
| 4.2 | Certificate Report | 33 |
| 4.3 | Audit Report | 34 |
| 5 | Configuration | 35 |
| 5.1 | Edit Settings | 35 |
| 5.2 | Affiliates | 36 |
| 5.3 | Pre-Vetted Domains | 37 |
| 5.4 | Contracts | 38 |
| 5.5 | E-Mail Templates | 38 |



| | | |
|-----------|------------------------------------|-----------|
| 6 | <i>Directory Services</i> | 39 |
| 6.1 | LDAP Services | 39 |
| 6.2 | Validation Services | 39 |
| 7 | <i>SCEP Enrollment</i> | 40 |
| 8 | <i>Certificate Profiles</i> | 41 |
| 8.1 | CA Hierarchy | 41 |
| 8.2 | Certificate Products | 41 |
| 9 | <i>Service Levels</i> | 43 |
| 10 | <i>Glossary</i> | 44 |
| 11 | <i>List of Figures</i> | 48 |

Statement of Services TC ID Store

This document describes the features of TC ID Store.

1 Web-based Registration Authority (RA)

The TC ID Store web portal provides all functions required to administrate the Managed PKI Services platform. The Users as well as the Administrators will be using the web portal to enroll for certificates and manage the certificates throughout their life-cycle.

All technical infrastructure components required to control the processes as described below, including installation and administration of certificates, are hosted and managed at the TC TrustCenter data center. Administrators and Users are not required to install any additional software on their respective computers. Administrators and / or Users who optionally wish to store their certificates on smart cards or USB tokens need to install a smart card reader with its respective driver software for the reader and the token.

Figure 1: Overall Architecture shows a high level and schematic overview of the entities and architecture involved.

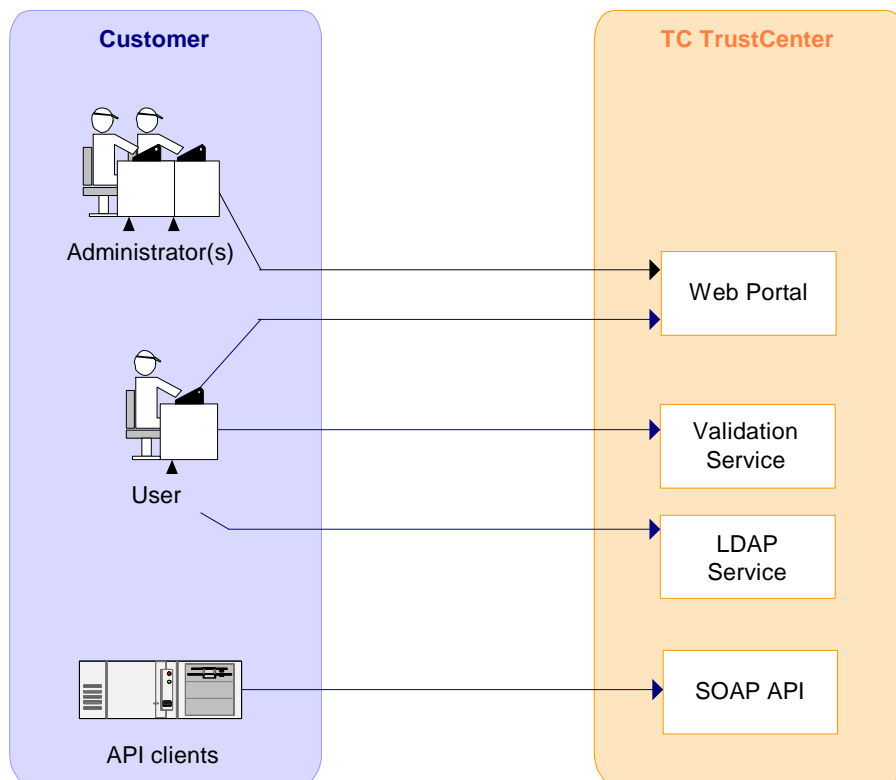


Figure 1: Overall Architecture

2 Managing Users

All individuals getting a certificate from TC ID Store or using the web portal to request certificates or receive certificate invites as well as to revoke, to suspend or to unsuspend certificates or to initiate key recovery are referred to as “Users”, regardless of their role.




The web portal supports the following user management tasks:

1. Adding Users
2. Searching, Modifying or Removing Users

An Administrator has to create Users, i.e. make Users known to the web portal, before they can use it.

Users can be assigned to groups to simplify their management, see section 2.1.2 for details.

2.1 Adding Users

| | |
|---|---|
| Role required to perform the task | “PKI Superadministrator”, “PKI Administrator” or “Registration Officer” |
| Precondition | None |
| Formal requirements | <ul style="list-style-type: none"> • Need identity proof of the new User • First name and Last name of the User must be according to the identity document. • Vetting of users must be in accordance with the relevant Certificate Policy Definitions (CPD). |
| Implicit action(s) | E-mail with login data (username as specified and an automatically generated password) will be sent to each new User |
| Where to find this task in the GUI |   (add single User)  (add batch User) |

Every user is linked to an affiliate. The fields organization name, country, state or province and city will be used for the respective certificate fields.

The account can be configured to support private addresses of users.

Affiliates must be registered before they can be used. The affiliate registration form is available for download on the web site.



To simplify the mapping from users in TC ID Store to existing user accounts in corporate systems the field „External ID“ can be used to store a unique employee number. This number will be written into *Client Certificates* in field “serialNumber“ of the subject name.

Users can be added in single or in batch mode. The batch mode can be used to add Users based on information exported from other IT systems, e.g. the HR system. Using batch mode with automatically generated CSV files significantly reduces the number of typing errors when adding new Users – especially for large numbers of Users.

Once a user has been added an e-mail containing his login data will be sent.

Note: The PIN method can be defined on a per product basis. It will be used for certificate issuance and key recovery. If the *ePIN*-method (see section 3.3) is used, the PIN will be sent via e-mail by default. This default can be changed to SMS when adding or modifying users.

Note: *Users* need to be vetted in accordance with the TC Certificate Policy Definitions ([CPD](#)). In a typical corporate environment the vetting level will be Class 2 for employees as Class 1 for external partners. The vetting level must be specified accordingly.

2.1.1 User Roles

Each User has at least one and optionally multiple roles. The existing roles are described in the following table.

To be entitled to request certificates one of the following roles must be enabled:

- “Basic User”
- “Privileged User”
- “PKI Administrator”

The officer roles need to be combined with “Privileged User” or “Basic User” to be able to request certificates.

The role “PKI Superadministrator” is always combined with “PKI Administrator”.

| Role name | Description |
|--|---|
| “PKI Superadministrator” This role can only be assigned by TC TrustCenter. Special training is mandatory. | <ul style="list-style-type: none"> • Accept certificate invites • Add, search, modify or remove Users. The “PKI Superadministrator” can assign or remove the roles “PKI Administrator”, “Registration Officer”, “Enrollment Officer”, “Revocation Officer”, “Unsuspension Officer”, “Key Recovery Officer”, “Privileged User”, “Basic User”, “External User” and “NoLogin User”. • Disable login for users |
| “PKI Administrator” This role can only be assigned by the “PKI Superadministrator” or TC TrustCenter. | <ul style="list-style-type: none"> • Accept certificate invites • Add, search, modify or remove Users (up to vetting level Class 2). The “PKI |



| Role name | Description |
|--|---|
| | <p>Administrator” can assign or remove the roles “Revocation Officer”, “Key Recovery Officer”, “Privileged User”, “Basic User”, “External User” and “NoLogin User”.</p> <ul style="list-style-type: none"> • Disable login for users • Request a certificate without requiring an approval by another “PKI Administrator” or “Enrollment Officer”. • Create certificate invites for arbitrary Users and approve certificate requests for arbitrary Users. • Revoke or suspend arbitrary certificates • Unsuspend arbitrary certificates • Initiate key recovery for arbitrary (recoverable) certificates • Lookup requests • Modify web portal configuration • Modify e-mail-templates • Create certificate report • Create activity report • Read audit report • Administrate user groups • Change <i>Certificate Owner</i> • Run TC SSL Certificate Discovery Tool |
| <p>“Key Escrow Administrator (Request)” This role can only be assigned by TC TrustCenter.</p> | <ul style="list-style-type: none"> • Initiate <i>Key Escrow</i> requests |
| <p>“Key Escrow Administrator (PSE)” This role can only be assigned by TC TrustCenter.</p> | <ul style="list-style-type: none"> • Has permission to access the escrowed <i>PKCS#12 PSE</i> using the API. |
| <p>“PIN Letter Administrator” This role can only be assigned by TC TrustCenter.</p> | <ul style="list-style-type: none"> • Print PIN letters |
| <p>“Registration Officer” (delegated role) This role can only be assigned by the “PKI Superadministrator” or TC TrustCenter.</p> | <ul style="list-style-type: none"> • Accept certificate invites • Add, search, modify or remove Users (“NoLogin Users”, “External Users”, “Basic Users” and “Privileged Users” only) • Disable login for users • Lookup requests • Create certificate report • Create activity report |



| Role name | Description |
|---|--|
| | <ul style="list-style-type: none"> • Administrate user groups • Change <i>Certificate Owner</i> • Modify web portal configuration (settings only) |
| <p>“Enrollment Officer” (delegated role) This role can only be assigned by the “PKI Superadministrator” or TC TrustCenter.</p> | <ul style="list-style-type: none"> • Accept certificate invites • Search Users • Create certificate invites for arbitrary Users and approve certificate requests for arbitrary Users. • Lookup requests • Modify web portal configuration (only pre-vetted domains and product configuration) • Create certificate report • Create activity report • Run TC SSL Certificate Discovery Tool |
| <p>“Enrollment Agent”(delegated role) This role can only be assigned by the “PKI Superadministrator” or TC TrustCenter.</p> | <ul style="list-style-type: none"> • Personalize smart cards or cryptographic tokens on behalf of users |
| <p>“Revocation Officer” (delegated role) This role can only be assigned by the “PKI Superadministrator”, the “PKI Administrator” or TC TrustCenter.</p> | <ul style="list-style-type: none"> • Accept certificate invites • Search Users • Revoke or suspend arbitrary certificates • Lookup requests • Create certificate report • Create activity report • Lookup web portal settings |
| <p>“Unsuspension Officer” (delegated role) This role can only be assigned by the “PKI Superadministrator” or TC TrustCenter.</p> | <ul style="list-style-type: none"> • Accept certificate invites • Search Users • Unsuspend arbitrary certificates • Lookup requests • Create certificate report • Create activity report • Lookup web portal settings • Unblock tokens |
| <p>“Key Recovery Officer” (delegated role) This role can only be assigned by the “PKI Superadministrator” or TC TrustCenter.</p> | <ul style="list-style-type: none"> • Accept certificate invites • Search Users • Initiate key recovery for arbitrary (recoverable) certificates • Lookup requests |

| Role name | Description |
|-------------------|--|
| | <ul style="list-style-type: none"> • Create certificate report • Create activity report • Lookup web portal settings |
| "Privileged User" | <ul style="list-style-type: none"> • Accept certificate invites • Request a certificate without requiring an approval by the "PKI Administrator" or "Enrollment Officer". For EV certificates the approval is still required. • Revoke or suspend own certificates • Initiate key recovery for own (recoverable) certificates • Lookup certificates within own group • Lookup web portal settings • Lookup own requests |
| "Basic User" | <ul style="list-style-type: none"> • Accept certificate invites • Request a certificate but the request needs to be approved by the "PKI Administrator" or "Enrollment Officer" • Revoke or suspend own certificates • Initiate key recovery for own certificates • Lookup certificates within own group • Lookup web portal settings • Lookup own requests |
| "External User" | <ul style="list-style-type: none"> • Accept certificate invites • Revoke or suspend own certificates • Initiate key recovery for own certificates • Lookup own certificates • Lookup own requests |
| "NoLogin User" | <ul style="list-style-type: none"> • Accept certificate invites |
| "SCEP User" | <ul style="list-style-type: none"> • All anonymously requested certificates through <i>SCEP</i> will be owned by this user. • No other roles might be combined with this role. |

Table 1 Description of Roles

Note: In the following sections we will denote with Administrator any administrative role, e.g. "PKI Superadministrator", "PKI Administrator" or any delegated role (see Glossary).

The initial role has to be assigned when adding the User; it defaults to “Basic User”. The role can be changed afterwards.

Note: Dual control for issuing certificates can be achieved by using the “Registration Officer” to create the User and the “Enrollment Officer” to approve the certificate request or create the certificate invite.

Note: Due to the comprehensive permissions assigned to the “PKI Superadministrator” special “PKI Superadministrator” training is required.

2.1.2 Administrating User Groups


Users can be assigned to a group. When searching Users the search can be filtered by a group. User groups are an additional method of structuring data.

Users with roles “Privileged User” or “Basic User” can only search certificates belonging to their group. If the User is not assigned to any group, certificates belonging to any group can be found and displayed.

Delegated roles, i.e. “Registration Officer”, “Enrollment Officer”, “Enrollment Agent”, “Revocation Officer”, “Unsuspendation Officer” and “Key Recovery Officer” can only access and manage users belonging to their group. If a user with a delegated role is not assigned to any group, he can access and manage users belonging to any group. This means that delegated roles can be restricted to be responsible for a single group by assigning them to that group.

The Administrators, (e.g. “PKI Superadministrator” and “PKI Administrator”) can manage users belonging to any group.

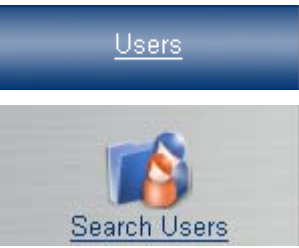
Users can only belong to one or no group.

| | |
|---|--|
| Role required to perform the task | “PKI Superadministrator”, “PKI Administrator” or “Registration Officer” |
| Precondition | None |
| Formal requirements | None |
| Implicit action(s) | When a group is deleted, all members will be removed from that group, and will no longer be assigned to a group. |
| Where to find this task in the GUI |  |

2.2 Searching, Modifying, Removing Users or disabling User Login

| | |
|--|---|
| Role required to perform the task | “PKI Superadministrator”, “PKI Administrator” or “Registration Officer” |
| Precondition | None |



| | |
|---|---|
| Formal requirements | For modifying Users the same formal requirements apply as for adding new Users. |
| Implicit action(s) | None |
| Where to find this task in the GUI |  |

Note: *User* login can be disabled and enabled. When the user login is disabled the *User* cannot login anymore. Certificates are not affected by this operation.

Note: Before deleting a User the *Certificate Owner* role for all *Team-Certificates* and *Application-Certificates* owned by that User must be changed to another *User*.

Note: *Client Certificates* will be automatically revoked when the related User is being deleted.

Note: The PIN method can be defined on a per product basis. It will be used for certificate issuance and key recovery. If the *ePIN-method* (see section 3.3) is used, the PIN will be sent via e-mail by default. This default can be changed to SMS when adding or modifying users.

3 Managing Certificates

The following certificate management tasks are supported by the web portal:

1. Requesting certificates
2. Creating certificate invites
3. Revoking, suspending or unsuspending certificates, initiating key recovery or initiating Key Escrow.

Requesting certificates is the process where the designated *Certificate Holder* initiates the certificate enrollment.

In the case of a certificate invite, the Administrator initiates the certificate enrollment process. The data required for certificates is either (a) taken from the login data of the designated *Certificate Holder* or (b) has to be entered by the Administrator when initiating the certificate enrollment.

Revoking and suspending certificates or initiating key recovery are processes which can be initiated by an Administrator or by the *Certificate Owner*.

All certificate management tasks have to be performed in accordance with the respective Certificate Policy Definition (CPD) and Certification Practice Statement (CPS). For all certificates chained to a TC TrustCenter CA certificate the TC TrustCenter [CPD](#) and [CPS](#) apply.

3.1 Certificate Validity

Certificates are usually issued for 1-3 years. The validity period can be chosen when selecting the certificate product (see section 8.2).

In the case of renewing SSL certificates the remaining validity period (*but not more than 90 days*) will be added to the new certificate, if the existing certificate (with the same common name) has been issued by either TC TrustCenter or a listed competitor.

3.2 Number of Certificates per User

The average number of certificates per User can be 1, 2 or 3. This is specified in the contract. The pre-defined certificate products support an appropriate partitioning of certificate purposes (see section 8.2) appropriate for the different number of certificates per User.

3.3 PIN-Methods

The PIN method to be used on certificate issuance and key recovery can be defined on a per product base.

By default the PINs will be delivered by e-mail or SMS to the User (*ePIN* method).

| |
|---|
| <p>Note: Not all mobile networks are covered by the SMS PIN delivery option. Especially in the US only a very limited number of mobile networks are supported. Please ask our support for details.</p> |
|---|

Alternatively the PIN setting can be changed by the “PKI Administrator” to *External PIN* or *PIN-Letter* for particular certificate products. With External-PINs the Administrator has to provide the PIN to the web portal for each request. The Administrator is also responsible for delivering the External-PIN to the Users. The *PIN-Letter Administrator* is responsible for

printing PIN-Letters. The PDF document containing PIN-Letters is automatically generated based on the template specified in the portal.

Note: The web portal doesn't deliver *External PINs*, they must be delivered out of band by the Administrator. The lengths of *External PINs* must not exceed 125 characters. Only printable ASCII characters are allowed (i.e. ASCII codes 32 – 126).

In the case of the *ePIN* method the PIN will be delivered via e-mail by default. This default method can be changed to SMS for individual Users (see sections 2.1 and 2.2).

See section 5.4 regarding the configuration of PIN method *External PIN*.

Note: When using *External PINs* key recovery cannot be done in batch mode.

Note: The method *PIN-Letter* cannot be used in conjunction with certificate invites (see section 3.8).

Note: When doing key recovery the same PIN method will be used, as was used for requesting this certificate (either *ePIN* or *External PIN*). If a certificate has been issued using the *ePIN* method it will be recovered using the *ePIN* method – even if the PIN method has been changed in between to *External PIN* for that product.

In the following sections all processes described are using the *ePIN* method.

3.4 Key Generation Policy

The key generation policy can be defined. It supports the following properties:

1. Minimum Key Length
2. Private Key Exportable
3. Strong Key Protection (i.e. user will be notified whenever the private key is accessed).
4. Allowed CSPs (i.e. the names of the Cryptographic Service Providers (CSPs) being used to generate the key).
5. Allow only MSIE (i.e. browser based key generation is allowed with Microsoft Internet Explorer only to obey key generation policy).

Note: Only Microsoft Internet Explorer supports a fine granular key generation policy. For other web browsers only the minimum key length can be enforced.

Note: For recoverable certificates (i.e. certificates with *PKCS#12 PSE* delivery) only the minimum key length is relevant.

Note: Depending on the certificate product some of the key generation policy properties might be pre-defined by TC TrustCenter. In this case these properties can no longer be changed.

3.5 Key Provider

By default public keys for certificates have to be provided by the requester (e.g. generated by the web browser). However, for certain products the "PKI Administrator" can specify the *Key Provider* to be the "Enrollment Agent" instead.

In that case the "Enrollment Agent" will be required to specify the public key for certificate requests using the TC PersoClient, i.e. a tool to personalize smart cards or USB tokens. The "Enrollment Agent" must use certificate based login in order to use the TC PersoClient (see also description of *Login Policy* in section 5.1).

Note: PIN method must be set to *PIN-Letter* and the *Key Generation Method* must be SMARTCARD in order to use TC PersoClient for the particular certificate product. The *Key Generation Method* cannot be modified by the "PKI Administrator", but only by TC TrustCenter.

Note: If multiple certificates are to be personalized to a single token using TC PersoClient this must be done in a single batch, i.e. marking all requests for that token and then triggering the personalization using the button



Note: TC PersoClient does not support personalization of recoverable certificates to tokens.

Note: TC PersoClient is a ClickOnce application and only supports Microsoft Internet Explorer on Windows.

3.6 Product Options

For some products (e.g. SSL certificates) additional product options (e.g. number of server licenses or number of Subject-Alt-Names) can be specified.

For such products, the person requesting certificates or creating the certificate invite will be asked to select these product options.

Note: Product options might be price relevant.

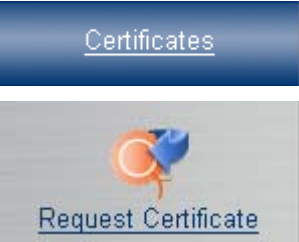
3.7 Requesting Certificates

The User can actively request a certificate without requiring any external trigger. This function can be used to either request a *Client Certificate* for the current User or to request Team Certificates or *Application Certificates*. The processes to request Team Certificates or

Application Certificates are similar to the processes to request *Client Certificates*. The difference is the key generation method. In the case of *Application Certificates* a *PKCS#10* certificate request must be uploaded. In the case of *Client Certificates* the key generation is performed by the web browser.

In the case of *Client Certificates* the *Certificate Holder* is also the *Certificate Owner*. In the case of *Application Certificates* the application is the *Certificate Holder*, the *Certificate Owner* is usually someone in charge of the application.

All workflows depicted below describe the certificate request process for *Client Certificates*. The workflows depicted in sections 3.7.3 and 3.7.4 are similar to the workflows for certificates for *Administrators*.

| | |
|---|---|
| Role required to perform the task | “PKI Administrator”, “Privileged User”, or “Basic User” |
| Precondition | User must have been added to the web portal |
| Formal requirements | None |
| Implicit action(s) | In the case of the role “Basic User” either a “PKI Administrator” or a “Registration Officer” has to approve the certificate request prior to certificate issuance. |
| Where to find this task in the GUI |  |

3.7.1 Issuance of non-recoverable Client Certificates for “Basic Users”

Steps 1 and 2 are preparational steps, they don’t have to be repeated for subsequent certificate issuance processes.

1. The “PKI Administrator” or “Registration Officer” has to create the User, i.e. make the User known to the web portal. The Administrator has to verify the User’s identity prior to this step. The User’s role has to be set to “Basic User”.
2. The User will receive a notification e-mail containing his data and the username + password required to login to the web portal.

Note: The “PKI Administrator” or “Registration Officer” can correct the User data using the web portal.

3. The User can login into the web portal and request a certificate. Depending on the certificate product certain data fields might have to be entered by the User. The key pair will be generated as part of this process.
4. The “PKI Administrators” or “Enrollment Officers” will be notified about the pending request waiting for approval.
5. Any “PKI Administrator” or “Registration Officer” can approve (or reject) the request.
6. TC TrustCenter generates the certificate and sends a download URL to the User. Since the certificate isn’t a secret object the download URL will not be PIN protected.

- The User installs the certificate by clicking on the link. No web portal login is required for this step.

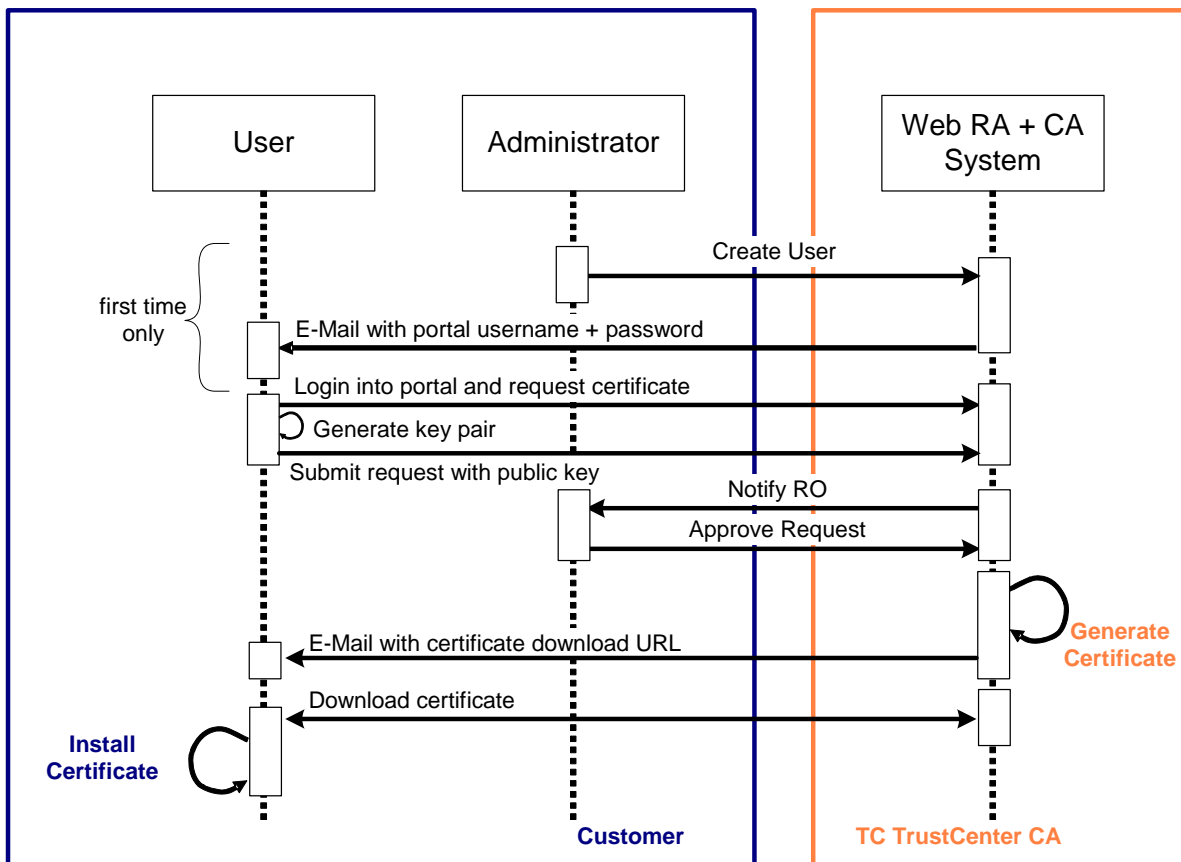


Figure 2: Request Approval Process Flow for Non-Recoverable Client Certs for “Basic Users”

Smart cards or USB Tokens can be used. Please select the appropriate cryptographic service provider (CSP) for key generation or install the appropriate *PKCS#11* library in the web browser. The list of appropriate CSPs can be configured using the key generation policy (see section 3.4).

3.7.2 Issuance of recoverable Client Certificates for “Basic Users”

Steps 1 and 2 are preparational steps, they don't have to be repeated for subsequent certificate issuance processes.

- The “PKI Administrator” or “Registration Officer” has to create the User, i.e. make the User known to the web portal. The “PKI Administrator” or “Registration Officer” has to verify the User's identity prior to this step. The User's role has to be set to “Basic User”
- The User will receive a notification e-mail containing his data and the username + password required to login to the web portal.

Note: The “PKI Administrator” or “Registration Officer” can correct the User data using the web portal.

- The User can login into the web portal and request a certificate. Depending on the certificate product, certain data fields might have to be entered by the User.
- The “PKI Administrators” or “Enrollment Officers” will be notified about the request pending for approval.
- Any “PKI Administrator” or “Registration Officer” can approve (or reject) the request.

6. TC TrustCenter generates a one-time PIN to protect the certificate/*PKCS#12 PSE* against unauthorized usage and sends it to the User.
7. TC TrustCenter generates the Personal Security Environment (PSE).
8. TC TrustCenter sends a delivery e-mail containing a *PKCS#12 PSE* URL.

Note: For security reasons this URL is only valid for 30 days and will be deactivated after 3 wrong PIN entries. If this should happen, a key recovery procedure can be initiated to get a new pickup invitation for the *PKCS#12 PSE* installation.

9. The User downloads and imports the *PKCS#12 PSE* containing the private key and the certificate. The one-time PIN is required for both steps. No web portal login is required for the PSE download.

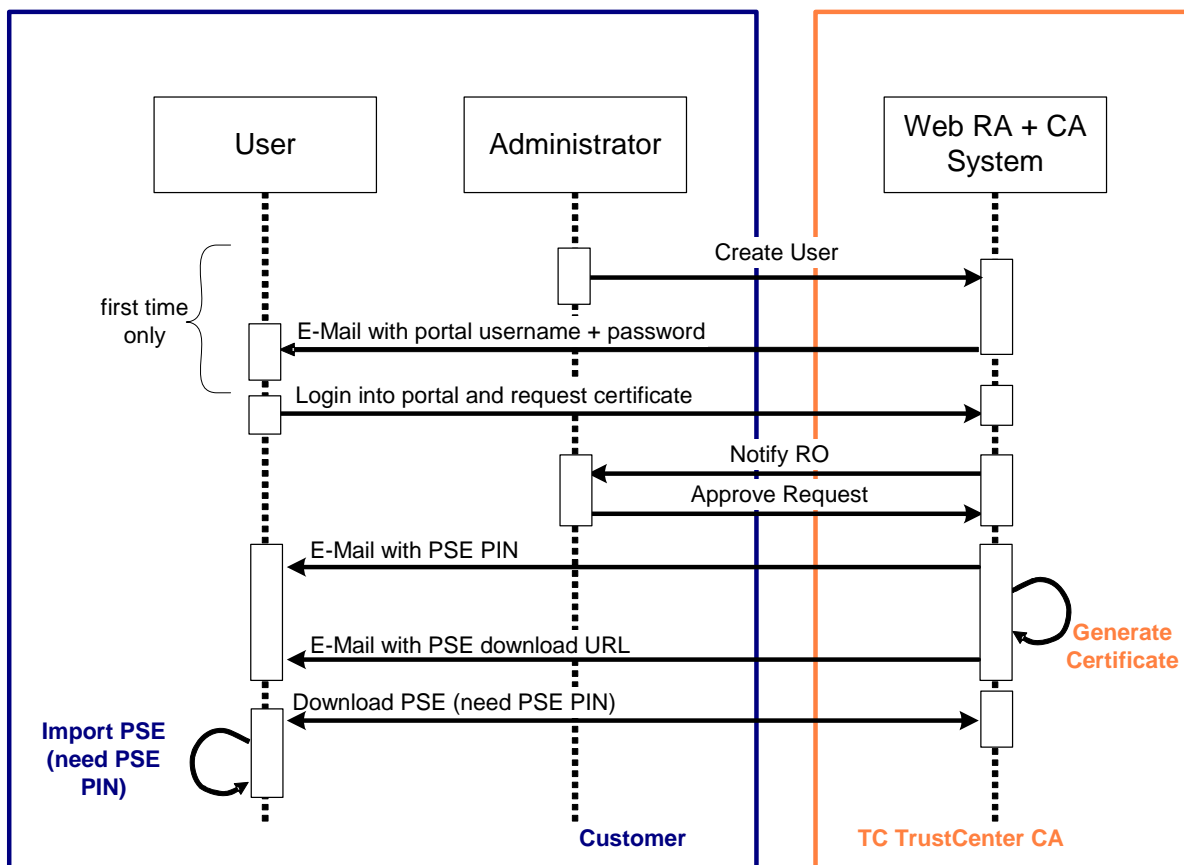


Figure 3: Request Approval Process Flow for Recoverable Client Certs for “Basic Users”

Smart cards or USB Tokens can be used. Please use the tool provided by the manufacturer to import the *PKCS#12 PSE* into the smart card / USB Token.

3.7.3 Issuance of non-recoverable Client Certificates for “Privileged Users”

Steps 1 and 2 are preparational steps, they don't have to be repeated for subsequent certificate issuance processes.

1. The “PKI Administrator” or “Registration Officer” has to create the User, i.e. make the User known to the web portal. The “PKI Administrator” or “Registration Officer” has to verify the User's identity prior to this step. The User's role has to be set to “Privileged User”
2. The User will receive a notification e-mail containing his data and the username + password required to login to the web portal.

Note: The “PKI Administrator” or “Registration Officer” can correct the User data using the web portal.

3. The User can login into the web portal and request a certificate. Depending on the certificate product certain data fields might have to be entered by the User. The key pair will be generated as part of this process.
4. TC TrustCenter generates the certificate and sends a download URL to the User. Since the certificate isn't a secret object the download URL will not be PIN protected.
5. The User installs the certificate by clicking on the link. No web portal login is required for this step.

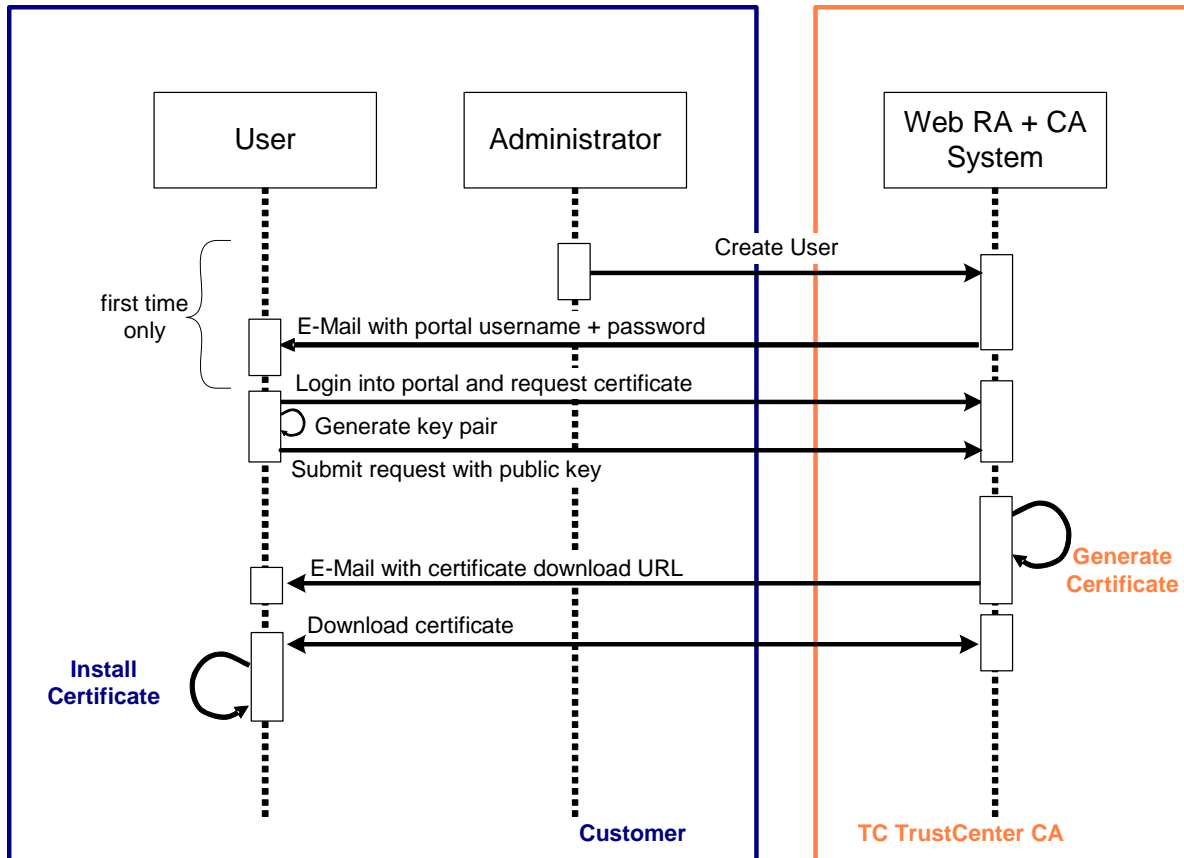


Figure 4: Request Process Flow for Non-Recoverable Client Certs for “Privileged Users”

Smart cards or USB Tokens can be used. Please select the appropriate cryptographic service provider (CSP) for key generation or install the appropriate *PKCS#11* library in the web browser. The list of appropriate *CSPs* can be configured using the key generation policy (see section 3.4).

This process is similar to the request process for non recoverable certificates for an Administrator. See Table 1 for a detailed description of the roles.

3.7.4 Issuance of recoverable Client Certificates for “Privileged Users”

Steps 1 and 2 are preparational steps, they don't have to be repeated for subsequent certificate issuance processes.

1. The “PKI Administrator” or “Registration Officer” has to create the User, i.e. make the User known to the web portal. The “PKI Administrator” or “Registration Officer” has to verify the User's identity prior to this step. The User's role has to be set to “Privileged User”

- The User will receive a notification e-mail containing his data and the username + password required to login to the web portal.

Note: The “PKI Administrator” or “Registration Officer” can correct the User data using the web portal.

- The User can login into the web portal and request a certificate. Depending on the certificate product certain data fields might have to be entered by the User.
- TC TrustCenter generates a one-time PIN to protect the certificate/*PKCS#12 PSE* against unauthorized usage and sends it to the User.
- TC TrustCenter generates the Personal Security Environment (PSE).
- TC TrustCenter sends a delivery e-mail containing a *PKCS#12 PSE* URL.

Note: For security reasons this URL is only valid for 30 days and will be deactivated after 3 wrong PIN entries. If this should happen, a key recovery procedure can be initiated to get a new pickup invitation for the *PKCS#12 PSE* installation.

- The User downloads and imports the *PKCS#12 PSE* containing the private key and the certificate. The one-time PIN is required for both steps. No web portal login is required for the PSE download.

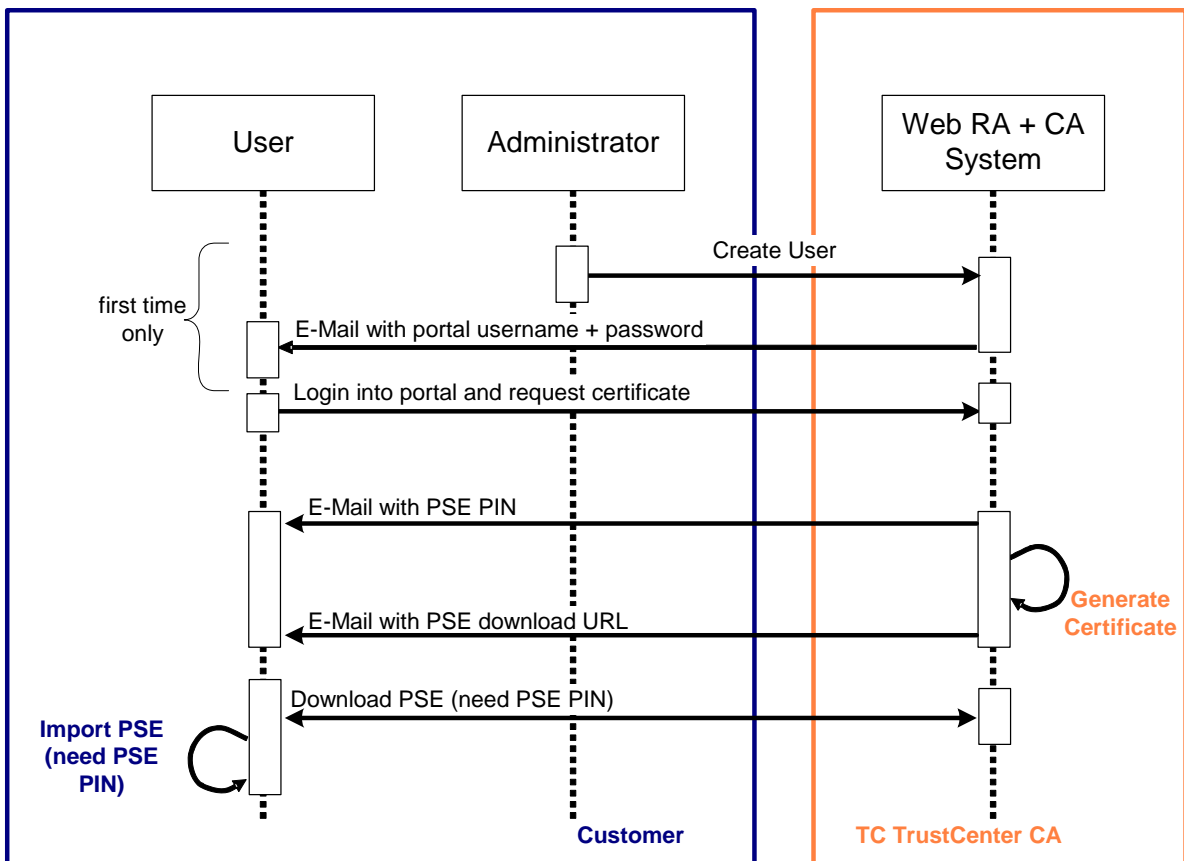


Figure 5: Request Process Flow for Recoverable Client Certs for “Privileged Users”

Smart cards or USB Tokens can be used. Please use the tool provided by the manufacturer to import the *PKCS#12 PSE* into the smart card / USB Token.

This process is similar to the request process for non recoverable certificates for an Administrator. See Table 1 for a detailed description of the roles.

3.7.5 Requesting Certificates by Anonymous Users

Certificates can also be requested by users without any authentication. This “Anonymous Request” feature must be enabled before it can be used.

Special URLs for “Anonymous Requests” have to be generated. These URLs have to be published to the potential user group. We recommend publishing anonymous request URLs to internal web sites only.

Note: Every person with access to that URL can anonymously submit certificate requests. It is the task of the “PKI Administrator” or “Enrollment Officer” to either approve or reject such requests after an out-of-band verification of the requester.

Note: In order to prevent search engines from publishing such URLs if published to internet sites, a robots.txt file should be present indicating not to follow or publish the link.

Each URL can only be used for a specific product and a single affiliate.

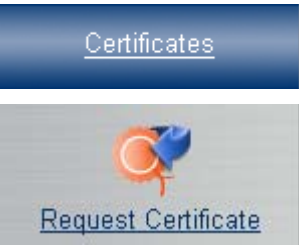
“Anonymous Requests” are clearly marked in the GUI. Details of the requester are stored as part of the request. The approval process is similar to the approval process for certificate requests from “Basic Users”.

The *Certificate Owner* for anonymously requested certificates will be set as follows:

1. to the requester (which will be created as a new user) in the case of *Client Certificates*.
2. to the user specified when generating the Enrollment URL (*SCEP*) in the case of non-client *SCEP* certificates.

3.8 Triggering Certificate Requests for Other Users

Certificate requests can be triggered by the Administrator. This process is called “Certificate Invite”, as the user receives an e-mail as the trigger. The certificate invite process can be used in single or in batch mode. The batch mode can be used to send certificate invites based on information exported from other IT system, e.g. an HR system. Using batch mode with automatically generated CSV files can significantly reduce the number of typing errors.

| | |
|---|---|
| Role required to perform the task | “PKI Administrator” or “Enrollment Officer” |
| Precondition | User must have been added to the web portal |
| Formal requirements | None |
| Implicit action(s) | E-mail notification will be sent to the User |
| Where to find this task in the GUI |  |



The certificate invite process is identical for “External User”, “Basic User” and “Privileged Users”.

3.8.1 Single mode certificate invite process for non-recoverable certificates

Steps 1 and 2 are preparational steps, they don't have to be repeated for subsequent certificate issuance processes.

1. The “PKI Administrator” or “Registration Officer” has to create the User, i.e. make the User known to the web portal. This can be done for each User separately using the GUI (Single) or by uploading a CSV file for multiple Users (Batch). The “PKI Administrator” or “Registration Officer” has to verify the User's identity prior to this step. The User's role has to be set to either “Basic User” or “Privileged User”.
2. The User will receive a notification e-mail containing his data and the username + password required to login to the web portal.

Note: The “PKI Administrator” or “Registration Officer” can correct the User data using the web portal.

3. The “PKI Administrator” or “Registration Officer” creates a certificate invite to initiate the certificate issuance process.
4. TC TrustCenter generates a one-time PIN to authenticate the User performing the key generation and sends it and the key generation URL to the User.
5. The User clicks on the link, enters the PIN and lets the browser perform the key generation. The public key will be uploaded to TC TrustCenter.
6. TC TrustCenter generates the certificate.
7. TC TrustCenter generates the certificate and sends a download URL to the User. Since the certificate isn't a secret object the download URL will not be PIN protected.
8. The User installs the certificate by clicking on the link. No web portal login is required for this step.

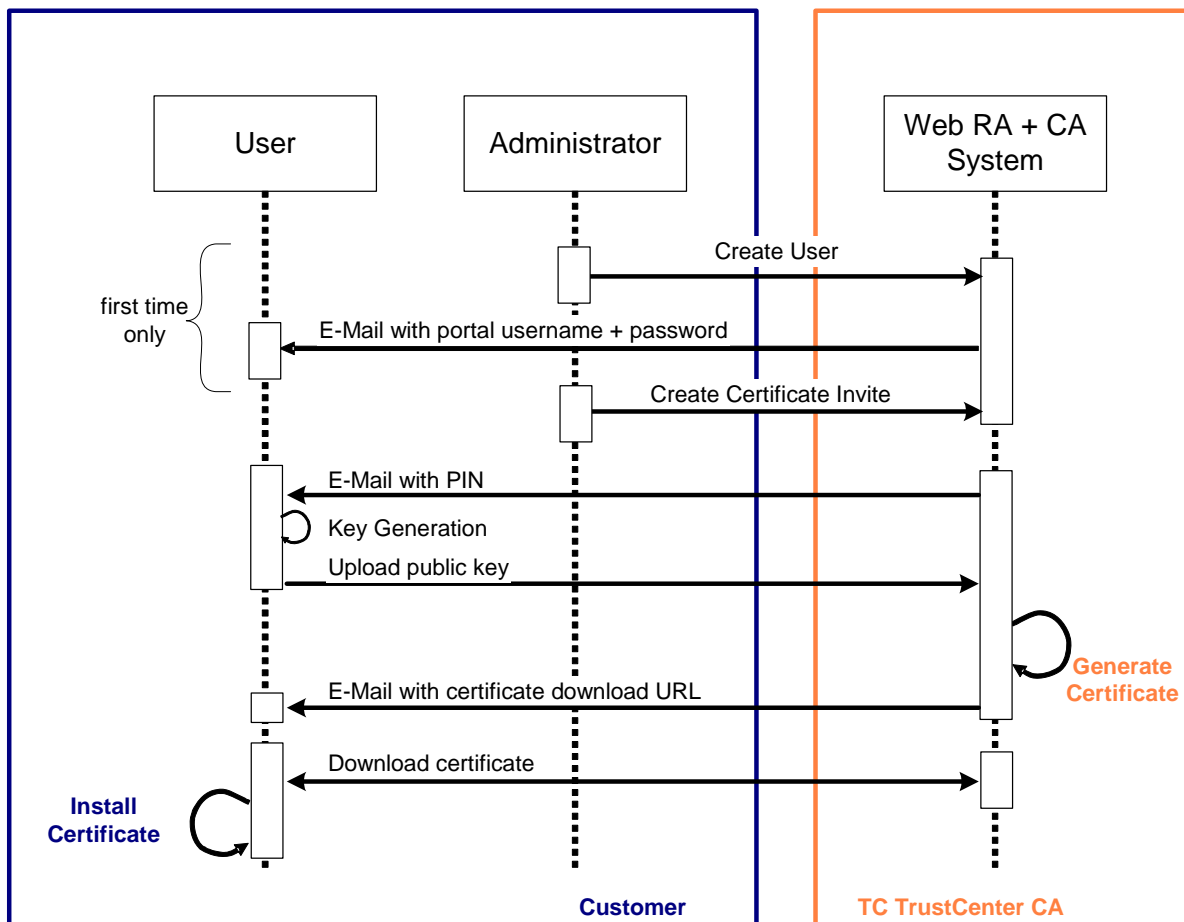


Figure 6: Single Mode Certificate Invite Process Flow for Non-Recoverable Certificates

Smart cards or USB Tokens can be used. Please select the appropriate cryptographic service provider (CSP) for key generation or install the appropriate *PKCS#11* library in the web browser. The list of appropriate *CSPs* can be configured using the key generation policy (see section 3.4).

3.8.2 Single mode certificate invite process for recoverable certificates

Steps 1 and 2 are preparation steps, they don't have to be repeated for subsequent certificate issuance processes.

1. The "PKI Administrator" or "Registration Officer" has to create the User, i.e. make the User known to the web portal. This can be done for each User separately using the GUI (Single) or by uploading a CSV file for multiple Users (Batch). The "PKI Administrator" or "Registration Officer" has to verify the User's identity prior to this step. The User's role has to be set to either "Basic User" or "Privileged User".
2. The User will receive a notification e-mail containing his data and the username + password required to login to the web portal.

Note: The "PKI Administrator" or "Registration Officer" can correct the User data using the web portal.

3. The "PKI Administrator" or "Registration Officer" creates a certificate invite to initiate the certificate issuance process.
4. TC TrustCenter generates a one-time PIN to protect the certificate/*PKCS#12 PSE* against unauthorized usage and sends it to the User.
5. TC TrustCenter generates the Personal Security Environment (PSE).

- TC TrustCenter sends a delivery e-mail containing a *PKCS#12 PSE* URL.

Note: For security reasons this URL is only valid for 30 days and will be deactivated after 3 wrong PIN entries. If this should happen, a key recovery procedure can be initiated to get a new pickup invitation for *the PKCS#12 PSE* installation.

- The User downloads and imports the *PKCS#12 PSE* containing the private key and the certificate. The one-time PIN is required for both steps. No web portal login is required for the PSE download.

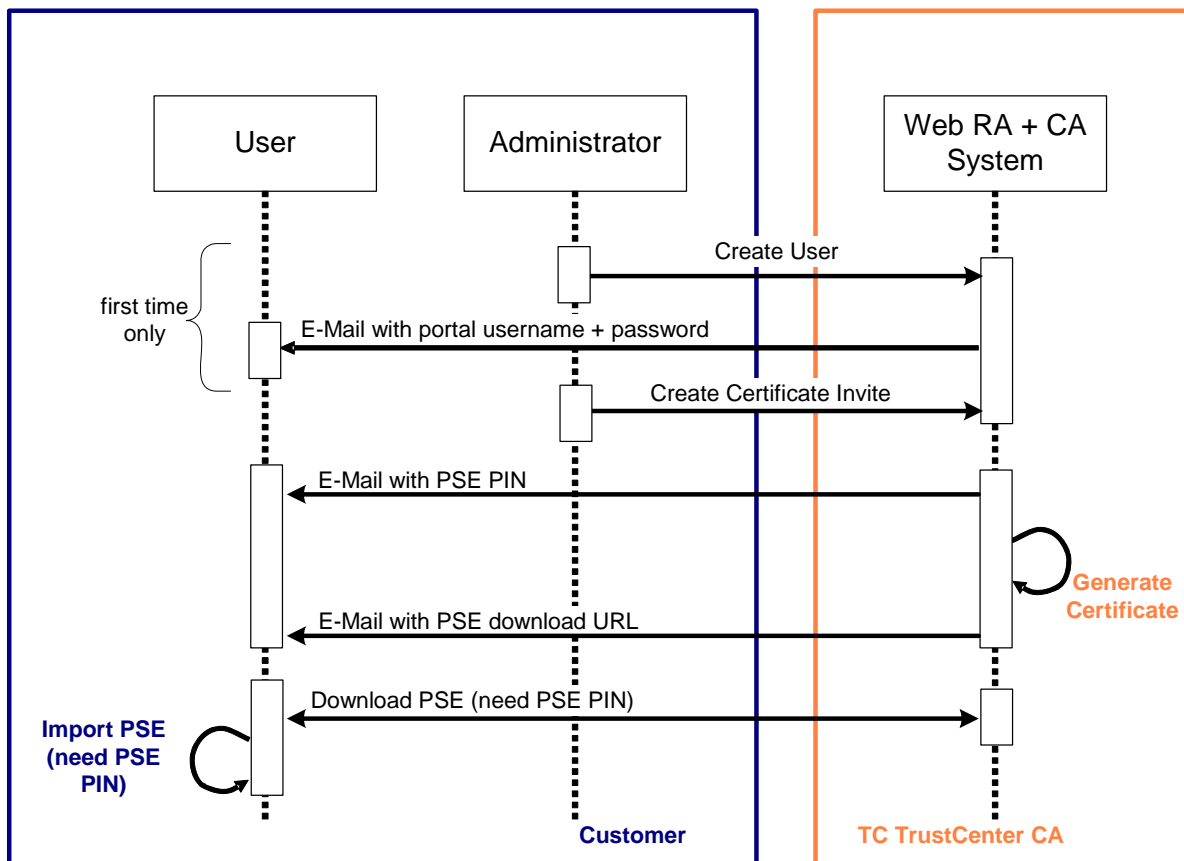


Figure 7: Single Mode Certificate Invite Process Flow for Recoverable Certificates

Smart cards or USB Tokens can be used. Please use the tool provided by the manufacturer to import the *PKCS#12 PSE* into the smart card / USB Token.

3.8.3 Batch mode certificate invite process for non-recoverable certificates

- The “PKI Administrator” or “Registration Officer” can either create certificate invites in batch mode for existing Users or he can add the Users and create a certificate invite in one step.
- The “PKI Administrator” or “Registration Officer” uploads a CSV file containing the usernames or e-mail addresses of the related Users or the complete User data in the case of adding Users and creating certificate invites in a one-step process.
- TC TrustCenter generates a one-time PIN to authenticate the User performing the key generation and sends it and the key generation URL to the User.
- The User clicks on the link, enters the PIN and lets the browser perform the key generation. The public key will be uploaded to TC TrustCenter.



5. TC TrustCenter generates the certificate and sends a download URL to the User. Since the certificate isn't a secret object the download URL will not be PIN protected.
6. The User installs the certificate by clicking on the link. No web portal login is required for this step.

Smart cards or USB Tokens can be used. Please select the appropriate cryptographic service provider (CSP) for key generation or install the appropriate *PKCS#11* library in the web browser. The list of appropriate CSPs can be configured using the key generation policy (see section 3.4).

3.8.4 Batch mode certificate invite process for recoverable certificates

1. The "PKI Administrator" or "Registration Officer" can either create certificate invites in batch mode for existing Users or he can add the Users and create a certificate invite in one step.
2. The "PKI Administrator" or "Registration Officer" uploads a CSV file containing the usernames or e-mail addresses of the related Users or the complete User data in the case of adding Users and creating Certificate Invites in a one-step process.
3. TC TrustCenter generates a one-time PIN to protect the certificate/*PKCS#12 PSE* against unauthorized usage and sends it to each User.
4. TC TrustCenter generates the Personal Security Environment (PSE).
5. TC TrustCenter sends a delivery e-mail containing a *PKCS#12 PSE* URL to each User.







Note: For security reasons this URL is only valid for 30 days and will be deactivated after 3 wrong PIN entries. If this should happen, a key recovery procedure can be initiated to get a new pickup invitation for *the PKCS#12 PSE* installation.

6. The User downloads and imports the *PKCS#12 PSE* containing the private key and the certificate. The one-time PIN is required for both steps. No web portal login is required for the PSE download.

Smart cards or USB Tokens can be used. Please use the tool provided by the manufacturer to import the *PKCS#12 PSE* into the smart card / USB Token.

3.9 Revoking, Suspending or Unsuspending certificates or Initiating Key Recovery



| | |
|--|--|
| Role required to perform the task | "PKI Administrator" (all tasks), Delegated roles (some tasks, see Table 1 for a detailed description) <i>Certificate Owner</i> with role "Privileged User" (except unsuspension) or "Basic User" (except unsuspension), |
| Precondition | User must have at least one certificate |
| Formal requirements | Unsuspending: make sure that the User is still in possession of the private key and eligible to have such a certificate |
| Implicit action(s) | <ul style="list-style-type: none"> • Key Recovery: the User (= <i>Certificate Holder</i>) will receive an e-mail containing the download link for |

| | |
|---|--|
| | the <i>PKCS#12 PSE</i> and a second e-mail containing the PIN to (a) download and (b) import the <i>PKCS#12</i> file. |
| Where to find this task in the GUI |   Then select appropriate action icon in result table:  ,  ,  , or  |

3.9.1 Revocation/Suspension of Certificates

This process provides a revocation/suspension mechanism for certificates. Revocation/suspension is performed by the “PKI Administrator”, the “Revocation Officer” or the *Certificate Owner*.

The single mode certificate administration process is as follows:

1. The web portal provides a web page for certificate administration.
2. The “PKI Administrator”, the “Revocation Officer” or the *Certificate Owner* may search for certificates using various search criteria, e.g. the certificate serial number or subject name. Revocation/suspension is initiated by selecting the appropriate icon for the action “Revocation” () / “Suspension” (). Alternatively multiple rows can be selected and the appropriate managed task can be initiated by pressing the associated button.
3. In the case where more than one certificate is issued per User, each single certificate has to be revoked / suspended separately.
4. The serial numbers of the revoked/suspended certificates are included in the next CRL.
5. TC TrustCenter sends a confirmation e-mail to the *Certificate Owner* after successful certificate revocation / suspension.

The batch mode certificate administration process is as follows:

1. The web portal provides a web page for certificate administration.
2. The “PKI Administrator”, the “Revocation Officer” or the *Certificate Owner* may perform a batch search for certificates by uploading a CSV file containing the User names or e-mail addresses. Revocation / suspension is initiated by selecting the relevant certificates matching the search criteria and pushing the appropriate button.
3. The serial numbers of the revoked/suspended certificates are included in the next CRL.
4. TC TrustCenter sends a confirmation e-mail to the *Certificate Owner* after successful certificate revocation/suspension.

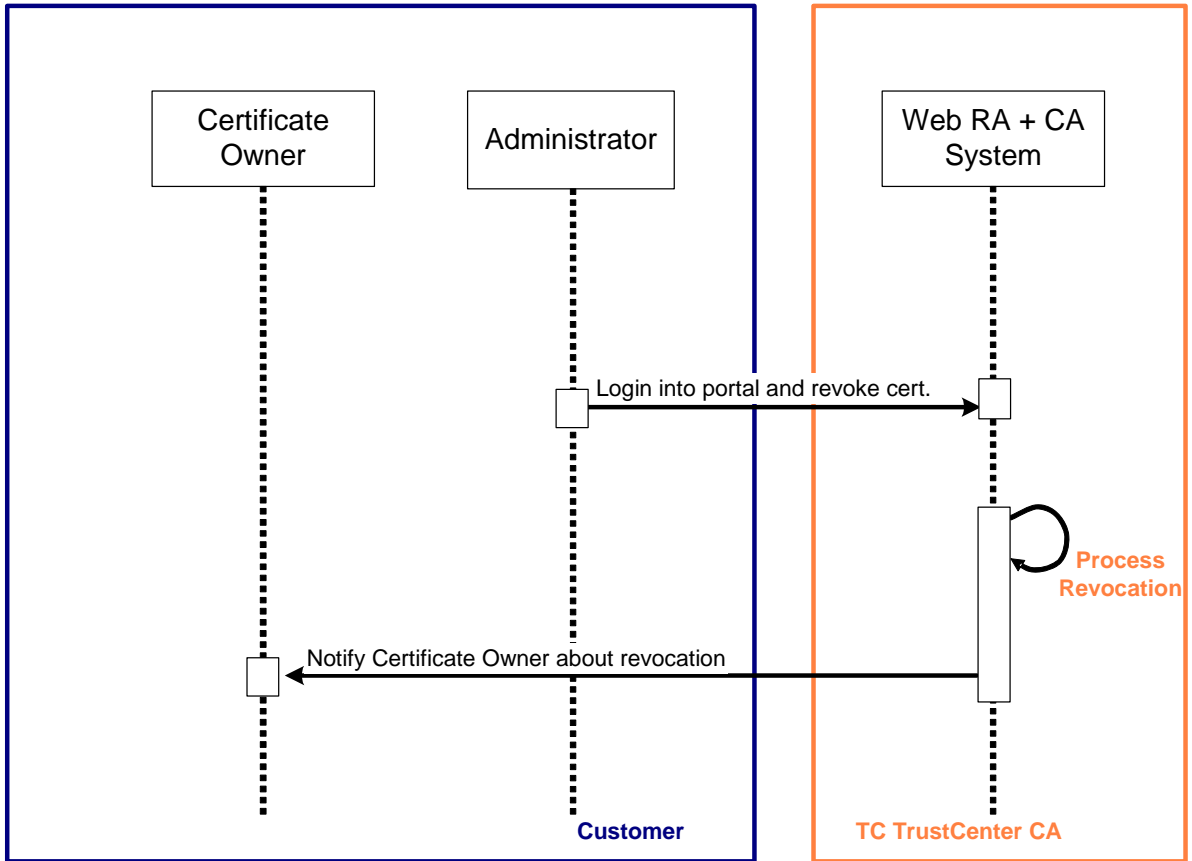


Figure 8: Revocation/Suspension Process Flow for “PKI Administrators”/“Revocation Officers”

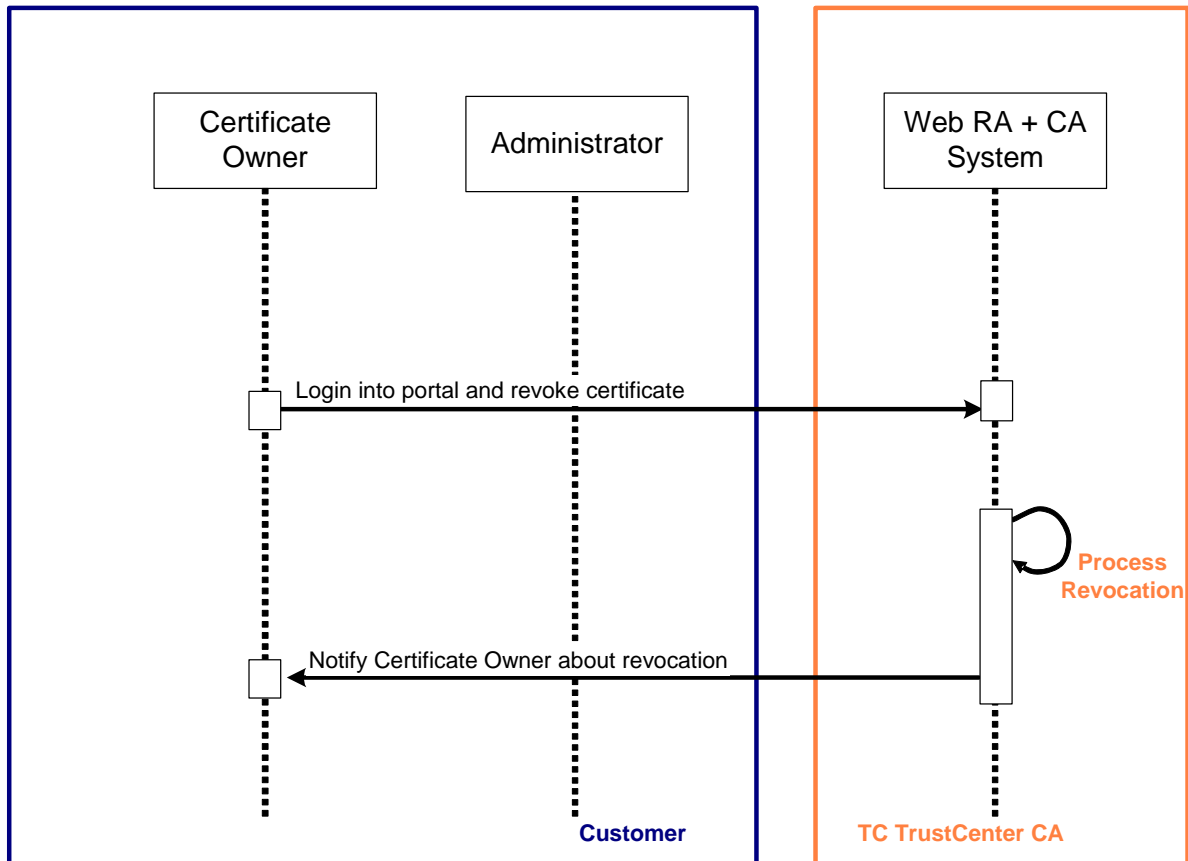



Figure 9: Revocation/Suspension Process Flow for Certificate Owners

3.9.2 Unsuspension of Certificates

Unsuspension is the reverse of suspension, i.e. it makes a certificate valid again. Unsuspension is performed by the “PKI Administrator” or the “Unsuspension Officer” only.


Note: After unsuspending a certificate it is treated the same as if it had been valid since the initial certificate issuance date.

The certificate unsuspension processes are identical to the certificate revocation/suspension processes except that only the “PKI Administrator” and the “Unsuspension Officer” have the permission to initiate that action. The action icon for unsuspension is .

3.9.3 Key Recovery

This process provides a key recovery mechanism for certificates. Key recovery is initiated by the “PKI Administrator”, the “Key Recovery Officer” or the *Certificate Owner*.

The single mode key recovery process is as follows:

1. The certificates to be recovered can be searched using various search criteria, e.g. the certificate serial number or subject name. Key recovery is initiated by selecting the appropriate icon for the action “Recover certificate” (.
2. In the case where more than one certificate is issued per User, each single certificate has to be recovered separately.
3. TC TrustCenter generates a one-time PIN to protect the recovered *PKCS#12 PSE* against unauthorized usage and sends it to the User.

4. TC TrustCenter sends a delivery e-mail containing a *PKCS#12 PSE* download URL to the User.
5. The User imports the *PKCS#12 PSE*. The one-time PIN is required for this step. No web portal login is required for this step.

The batch mode key recovery process is as follows:

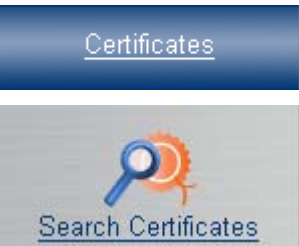


1. The web portal provides a web page for certificate administration.
2. The “PKI Administrator”, “Key Recovery Officer” or the *Certificate Owner* may perform an extended search for certificates by uploading a CSV file containing the User names or e-mail addresses. Recovery is initiated by selecting the relevant certificates matching the search criteria and pushing the button “Recover”.

Note: When using *External PINs* key recovery is not possible in batch mode.

3. TC TrustCenter generates a one-time PIN to protect the recovered *PKCS#12 PSEs* against unauthorized usage and sends it to the Users
4. TC TrustCenter sends a delivery e-mail containing a User-*PKCS#12 PSE* download URL to each User.
5. The Users import the *PKCS#12 PSE*. The one-time PIN is required for this step. No web portal login is required for this step.

Note: For both key recovery methods the *PKCS#12 PSE* download URL will be sent to the *original e-mail address* (i.e. the e-mail address valid when the certificate was initially requested) of the *Certificate Owner*. The one-time PIN will be sent to the *current address*.

3.10 Key Escrow

| | |
|---|--|
| Role required to perform the task | “Key Escrow Administrator (Request)” |
| Precondition | User must have at least one recoverable certificate |
| Formal requirements | <ul style="list-style-type: none"> • Customer must comply with the TC TrustCenter Key Escrow Requirements. • Additional requirements depend on local legislation and company policy. |
| Implicit action(s) | <ul style="list-style-type: none"> • The PIN will be sent to “Key Escrow E-Mail (PIN)”, the escrowed <i>PKCS#12</i> file download link will be sent to “Key Escrow E-Mail (PSE)”. |
| Where to find this task in the GUI | <div style="text-align: center;">   </div> <p>Then select the action icon in result table: </p> |

This process provides a *Key Escrow* mechanism for certificates. *Key Escrow* can only be initiated by the “Key Escrow Administrator (Request)”.

The single mode *Key Escrow* process is as follows:

1. The certificates to be escrowed can be searched using various search criteria, e.g. the certificate serial number or subject name. Key recovery is initiated by selecting the appropriate icon for the action “Key Escrow” (🔑).
2. In the case where more than one certificate is issued per User, each single certificate has to be escrowed separately.
3. TC TrustCenter generates a one-time PIN to protect the escrowed *PKCS#12 PSE* against unauthorized usage and sends it to the address specified in Configuration | Settings | Key Escrow E-Mail (PIN).
4. TC TrustCenter sends a delivery e-mail containing a *PKCS#12 PSE* download URL to the address specified in Configuration | Settings | Key Escrow E-Mail (PSE).
5. Either “Key Escrow Administrator” imports the *PKCS#12 PSE*. The one-time PIN is required for this step. No web portal login is required for this step.

The batch mode *Key Escrow* process is as follows:




1. The web portal provides a web page for certificate administration.
2. The “Key Escrow Administrator (Request)” may perform an extended search for certificates by uploading a CSV file containing the User names or e-mail addresses. *Key Escrow* is initiated by selecting the relevant certificates matching the search criteria and pushing the button “Key Escrow”.
3. TC TrustCenter generates a one-time PIN to protect the recovered *PKCS#12 PSEs* against unauthorized usage and sends it to the “Key Escrow Administrator (Request)”
4. TC TrustCenter sends a delivery e-mail containing a User-*PKCS#12 PSE* download URL to the address specified in Configuration | Settings | Key Escrow e-mail (PSE).
5. The “Key Escrow Administrator” imports the *PKCS#12 PSEs*. The one-time PIN is required for this step. No web portal login is required for this step.

Note: *Key Escrow* is a very sensitive process. A strict role separation between “Key Escrow Administrator (Request)” and “Key Escrow Administrator (PSE)” is recommended. See document Key Escrow Requirements for more details.

Note: The *Certificate Owner* will *not* be notified about a *Key Escrow* process.

3.11 Change Certificate Owner


| | |
|--|---|
| Role required to perform the task | “PKI Administrator”, Delegated roles (see Table 1 for a detailed description) |
| Precondition | User must have at least one certificate |
| Formal requirements | <ul style="list-style-type: none"> • Make sure that the new User is eligible to own the certificate. |

| | |
|---|--|
| Implicit action(s) | <ul style="list-style-type: none"> • None |
| Where to find this task in the GUI |   Then select the action icon in result table:  |


Each certificate belongs to a *Certificate Owner*. In the case of Team Certificates or *Application Certificates*, e.g. TC Team Certificate, the *Certificate Owner* usually is responsible for the application or the team.

Before deleting a User all Team Certificates and *Application Certificates* owned by that User to be deleted must be assigned to another User.

In single mode this process is as follows:

1. The certificates whose owners are to be changed can be searched using various search criteria, e.g. the certificate serial number or subject name. Assigning the certificate to a new User can be initiated by clicking on the appropriate symbol () for “Change *Certificate Owner*”.
2. In the case where a User owns Team Certificates or *Application Certificates* each certificate must be individually assigned to a new User.
3. The new User is selected.

The batch mode process is as follows:


1. The web portal provides a web page for certificate administration.
2. The “PKI Administrator”, “Key Recovery Officer” or the *Certificate Owner* may perform an extended search for certificates by uploading a CSV file containing the User names or e-mail addresses. Assigning the certificate to a new User can be initiated by clicking on the appropriate symbol () for “Change *Certificate Owner*”.
3. The new User is selected.

3.12 Verify SSL Server Installation

| | |
|--|--|
| Role required to perform the task | “PKI Administrator”, Enrollment Officer or the “Privileged User” or “Basic User” if <i>Certificate Owner</i> . |
| Precondition | <ul style="list-style-type: none"> ▪ There must be at least one SSL Server certificate available. ▪ Microsoft Internet Explorer is being used. |
| Formal requirements | None |
| Implicit action(s) | None |

Where to find this task in the GUI



Then select the action icon in result table: 

This action will start an application using Microsoft ClickOnce technology. It only supports Microsoft Internet Explorer as web browser.



This application will open an SSL connection to the web server named in the related SSL Server certificate and perform the following checks:

- Is the server responding?
- Has the certificate been installed properly?

4 Reports

4.1 Activity Report

Activity reports can be generated using the web portal.

| | |
|---|--|
| Role required to perform the task | "PKI Administrator" or any delegated role |
| Precondition | None |
| Formal requirements | None |
| Implicit action(s) | None |
| Where to find this task in the GUI |   |

The following reports are provided:



- Number of certificate requests by date
- Number of certificate invites by date
- Number of added Users by date
- Number of newly issued certificates by product

Reports can either be generated in HTML format or as a PDF document.

Note: Reports cover events for all groups; they are not tied to any specific group.

4.2 Certificate Report

Certificate reports can be generated using the web portal.

| | |
|---|--|
| Role required to perform the task | "PKI Administrator" or any delegated role |
| Precondition | None |
| Formal requirements | None |
| Implicit action(s) | None |
| Where to find this task in the GUI |   |

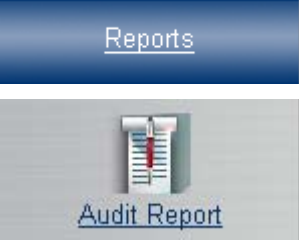
The certificate report lists all certificates for the particular account in the defined time frame. The certificates are grouped by the group of the respective *Certificate Owner*.



The list includes the name of the certificate product, the issuance date and the price.

4.3 Audit Report


Audit reports can be generated using the web portal.

| | |
|---|---|
| Role required to perform the task | “PKI Administrator” or “PKI Superadministrator” |
| Precondition | None |
| Formal requirements | None |
| Implicit action(s) | None |
| Where to find this task in the GUI |  |

The audit report provides information regarding the actions which have been performed in the related account, e.g. login, creation of modification of a user, etc.

Note: Audit Events are only accessible online for 6 months. They can be downloaded for local archiving.

5 Configuration

| | |
|---|--|
| Role required to perform the task | <p>“PKI Administrator” (right to modify settings + “Contracts”).</p> <p>Delegated officers (right to view settings + “Contracts”)</p> <p>“Basic Users” and “Privileged Users” (right to view settings)</p> |
| Precondition | None |
| Formal requirements | None |
| Implicit action(s) | None |
| Where to find this task in the GUI |  <p>The screenshot shows a vertical list of menu items under the 'Configuration' header:</p> <ul style="list-style-type: none"> Configuration Edit Settings Affiliates Pre-Vetted Domains Email Templates Customize Layout Edit Contracts |

5.1 Edit Settings

The following details can be maintained using the “Edit Settings” sub-menu:

| Field | Property | Description |
|-------------------|-----------|--|
| Corporate Contact | Read only | The corporate contact identifies the “PKI Administrator” (name) and the legal entity of the company (company name and address according to official register). He is responsible |

| Field | Property | Description |
|----------------------------|-----------|--|
| | | for following the registration policy for adding Users and issuing certificates. This person is vetted prior to setting up TC ID Store for non-Demo purposes. This person will get access to the self-service portal and is eligible to submit questions to the telephone hotline or to use the self-service portal. |
| Business Contact | Editable | The business contact identifies the person responsible for business related questions, e.g. contract renewal, extending contract to additional Users etc. |
| Technical Contact | Editable | The technical contact is expected to be knowledgeable about the technical aspects of the PKI applications. This person will get access to the self-service portal and is eligible to submit questions to the telephone hotline or to use the self-service portal. |
| Login Policy | Editable | Certificate based authentication can be enforced for administrative roles or all users. Alternatively username and password authentication is permitted. All <i>Client Certificates</i> issued through the related account and suitable for authentication can be used for login. |
| Users have private address | Editable | Support for user private addresses can be set to “No”, “Optional”, or “Mandatory”. Private address fields might be used with E-Mail notifications or documents associated with smart card personalization. |
| Key Escrow E-mail (PIN) | Read only | In the case of <i>Key Escrow</i> the PIN will be sent to this e-mail address. See section 3.10. |
| Key Escrow E-mail (PSE) | Read only | In the case of <i>Key Escrow</i> the <i>PKCS#12 PSE</i> will be sent to this e-mail address. See section 3.10. |

The following addresses can be maintained using the “Edit Contracts” sub-menu

| Field | Property | Description |
|-----------------|----------|--|
| Billing Contact | Editable | This is the formal recipient of the invoice. |
| Billing Address | Editable | This is the address of the mailbox to send the invoice to. |

5.2 Affiliates

Each User is assigned to exactly one affiliate. The list of all registered affiliates can be visited using menu “Affiliates”. The “PKI Administrator” can add more affiliates and select the required vetting class. This vetting class will be assigned to the affiliate once the vetting has been successfully completed.

If a certificate requested for an affiliate requires a higher vetting class than the affiliate has been approved for the request will be queued until the affiliate has been vetted for the required class.

The following data is stored for each affiliate:

- Company related data

- Displayname
- Country
- Organization name
- State or province
- City
- Business Category
- Street and number
- Postal code
- Main telephone number
- Data related to the registration of the company
 - Country of the related register
 - State or province of the related register (if the register is not operating on a national level)
 - Locality of the related register (if the register is not operating on a national or state/province level)
 - Registration number
 - Issuance date of the certificate of registration
- General data
 - Class of vetting which this affiliate has been approved for

The display name is used in select boxes. All other fields must exactly match the official company registration. Affiliates must be registered and vetted by TC TrustCenter before they are available for use.

The fields “Country”, “Organization name”, “State or province”, and “City” are used for the respective fields in certificates.

Some certificate products will include additional data fields, e.g. “business category”, “street and number”, “postal code” and “registration number”.

Note: TC Personal ID and TC Business ID Demo do not contain the organization name. Only TC Class 1 vetting is required for these certificate products.

Note: The vetting status of an affiliate is only valid for a defined time period. The expiration date depends on the issuance date of the certificate of registration and on the vetting class.

5.3 Pre-Vetted Domains

Certain fields in a certificate are subject to being vetted by TC TrustCenter. In order to speed up the certificate issuance process such vetting can be done in advance.


The following certificate fields require vetting by TC TrustCenter:

- Servername in TC Trust SSL, TC Trust SSL Wildcard, TC Extended Trust SSL, and TC Domain Controller ID

- User Principal Name (UPN) as optionally contained in TC Personal ID and TC Business ID
- E-mail addresses contained in TC Trust SSL, TC Trust SSL Wildcard, TC Domain Controller ID, TC RAS and IAS Server ID, and TC Team Certificate, because they might differ from the e-mail address of the *Certificate Owner*.

When requesting one of the above mentioned certificate products the required domain must

- (a) have been pre-vetted already or
- (b) a pre-vetting request will automatically be generated and the certificate will be put on hold until an appropriate pre-vetted domain has been approved.

The pre-vetting status of a domain expires after a certain time period. In the case where a domain is beyond that time period, the pre-vetting status can be renewed (.

TC ID Store supports Windows domains (e.g. myname.local) as well as publicly registered domains (e.g. mycompany.com).

Note: Domains must be pre-vetted for each affiliate individually.

5.4 Contracts

The available certificate products are maintained within “Contracts” in the web portal. “Contracts” do have a start date and an end date. Only one “Contract” can be active at any point in time.

The remaining amount denotes the remaining amount of money available to pay for certificates with a price greater than 0.

In the details view of the “Contracts” all certificate products available in that “Contract” are listed. Certificate products with a price greater than 0 are billed on a per certificate base. All certificate products with price 0 are billed on a per user base.

Only certificate products marked as “active” are listed when requesting certificates. The Administrator can control the available certificate products using this flag. By default all certificate products are marked as “active”.

The PIN method *External PIN* can be configured on a per certificate product basis.

5.5 E-Mail Templates

E-mails can be sent out for the various processes (e.g. certificate delivery, certificate revocation, etc.). These e-mails can be customized by the “PKI Administrator”.

The e-mail templates will revert to the default settings if customization is deleted.

6 Directory Services

Certificates are searchable and accessible via the TC TrustCenter web sites if they are published to the LDAP service (see section 6.1).

All CRLs can be downloaded from the TC TrustCenter web site.

6.1 LDAP Services

The following certificate products are available via the TC TrustCenter LDAP directory:

- TC Business ID Demo
- TC Personal ID
- TC Business ID, recoverable and TC Business ID, recoverable enc.
(TC Business ID, sign+auth and sign are not intended for encryption. Therefore they are not published to the LDAP service.)
- TC Team Certificate

Directory Information Tree structure: ou=publiccertgroup, dc=trustcenter, dc=de

6.2 Validation Services

TC TrustCenter provides a CRL publishing service as well as an OCSP service.

The CRL properties are:

- CRL is generated at least once per week and is available for download via the TC TrustCenter web site.
- The CRL download URL is included in an extension in the certificates.
- The CRL format is v2.

The managed OCSP service has the following properties:

- Compliant to RFC2560 (OCSP v1).
- OCSP requests don't have to be signed. No authentication is required to submit an OCSP request.
- The OCSP responder URL is included as an extension in the certificates.

7 SCEP Enrollment

Certificates can be requested using the simple certificate enrollment protocol (*SCEP*). This protocol is typically used by network devices.

SCEP enrollment is supported using the methods described in sections 3.7 and 3.8.

Note: Only the certificate products starting with *SCEP* can be used in conjunction with *SCEP* enrollment.

Some Apple products support *SCEP* based certificate enrollment. TC ID Store pushes two additional configuration payloads in addition to the *Client Certificate* to the device (i.e. a VPN configuration and a Web Clip by default).

Note: The “Enrollment URL (*SCEP*)” allows for requesting certificates without entering additional information as required for network devices. This “Enrollment URL (*SCEP*)” is not available in conjunction with *SCEP* enrollment for Apple products. The “Anonymous request link” (see section 3.7.5 for details) is not available for certificate products providing the “Enrollment URL (*SCEP*)”.

8 Certificate Profiles

This section describes the certificate hierarchy and the profile of the certificates.

8.1 CA Hierarchy

All certificates will be chained to either the

- “TC Class 2 CA II” Root certificate via the “TC Class 2 L1 CA XI” Sub-CA
- “TC Universal I” Root certificate via the “TC Class 1 L1 CA IX” Sub-CA certificate
- Adobe Root certificate (CDS) via the “TC TrustCenter CA for Adobe I” Sub-CA certificate.

8.2 Certificate Products

The following certificate products are generally available with TC ID Store. The certificate products available for a specific account are stated in the particular “Contract”.

| Base name | Kind | Validity Period | CA | Comment |
|-------------------------------|---|--------------------|---------|---|
| TC Business ID Demo | Recoverable and non-recoverable | 30 days | Class 1 | Demo purposes only |
| TC Business ID for Adobe Demo | PDF Signature | 30 days | CDS | Demo purposes only |
| TC Trust SSL Demo | | 30 days | Class 0 | Demo purposes only |
| TC Personal ID | | 1 yr, 2 yrs, 3 yrs | Class 1 | O-Field empty. This certificate is intended for external partners |
| TC Business ID | Recoverable and non-recoverable | 1 yr, 2 yrs, 3 yrs | Class 2 | Single certificate for signing, authentication and encryption |
| | Signing and authentication (Sign+auth) | 1 yr, 2 yrs, 3 yrs | Class 2 | Signing and Authentication only |
| | Signing | 1 yr, 2 yrs, 3 yrs | Class 2 | Signing only |
| | Authentication | 1 yr, 2 yrs, 3 yrs | Class 2 | Authentication only |
| | Recoverable encryption (recoverable enc). | 1 yr, 2 yrs, 3 yrs | Class 2 | Encryption only. |
| TC Business ID for Adobe | PDF Signature | 1 yr, 2 yrs, 3 yrs | CDS | For PDF signing only |



| Base name | Kind | Validity Period | CA | Comment |
|--|------|--------------------|---------|--|
| TC Domain Controller ID | | 1 yr, 2 yrs, 3 yrs | Class 2 | Required for using Smart Card Logon |
| TC RAS and IAS Server ID | | 1 yr, 2 yrs, 3 yrs | Class 2 | Required for secure WLAN access. |
| TC Client Computer ID | | 1 yr, 2 yrs, 3 yrs | Class 2 | Required for secure WLAN access. |
| TC Team Certificate | | 1 yr, 2 yrs, 3 yrs | Class 2 | Certificate can be shared among a team |
| TC Publisher ID for Adobe AIR | | 1 yr, 2 yrs, 3yrs | Class 2 | Code Signing certificate |
| TC Publisher ID for Java Desktop | | 1 yr, 2 yrs, 3yrs | Class 2 | Code Signing certificate |
| TC Publisher ID for Microsoft Authenticode | | 1 yr, 2 yrs, 3yrs | Class 2 | Code Signing certificate |

All recoverable certificates will be issued as *PKCS#12 PSEs*. All other certificates will be requested using either web browser based key generation or copy&paste of a *PKCS#10* request (TC Domain Controller ID, TC Client Computer ID and TC RAS and IAS Server ID).

The Administrator can mark certain certificate products as "deactivated". Deactivated certificate products will not be selectable when requesting certificates or creating certificate invites.

9 Service Levels

TC ID Store includes “Bronze” support.

The support service levels (incl. response times and severity definitions) are defined in the [Support SLA](https://www.verisign.com/repository/service_description) document see https://www.verisign.com/repository/service_description.

10 Glossary

| | |
|---------------------------------|---|
| Administrator | <p>“PKI Superadministrator”, “PKI Administrator” or any delegated role (“Registration Officer”, “Enrollment Officer”, “Unsuspendation Officer”, “Revocation Officer”, “Key Recovery Officer”).</p> <p>See section 2.1.1</p> |
| Application Certificates | <p>In the case of <i>Application Certificates</i> the <i>Certificate Owner</i> and the <i>Certificate Holder</i> are not identical.</p> <p>The application (e.g. web server or domain controller) is the <i>Certificate Holder</i>. The <i>Certificate Owner</i> is usually someone in charge of the application, e.g. web server administrator.</p> <p>TC DomainController ID is a typical example of an <i>Application Certificate</i>.</p> <p>See section 2.2</p> |
| Basic User | <p>One of the possible roles for Users. The roles are described in section 2.1.1.</p> |
| Certificate Holder | <p>This denotes the entity mentioned in the certificate.</p> <p>It can be a natural person (<i>Client Certificate</i>), a team or an application or a web server (<i>Application Certificate</i>).</p> <p>In the case of <i>Client Certificates</i> the <i>Certificate Holder</i> is also the <i>Certificate Owner</i>. In the case of <i>Application Certificates</i> the application is the <i>Certificate Holder</i>, the <i>Certificate Owner</i> is usually someone in charge of the application.</p> <p>See section 3.4</p> |
| Certificate Owner | <p>This is the person responsible for the certificate, i.e. <i>Certificate Holder</i> in case of <i>Client Certificates</i> and the server administrator in case of server and other <i>Application Certificates</i>.</p> <p>In the case of <i>Client Certificates</i> the <i>Certificate Holder</i> is also the <i>Certificate Owner</i>. In the case of <i>Application Certificates</i> the application is the <i>Certificate Holder</i>, the <i>Certificate Owner</i> is usually someone in charge of the application.</p> <p>See sections 3.11, 3.4</p> |
| Client Certificate | <p>In the case of <i>Client Certificates</i> the <i>Certificate Holder</i> is also the <i>Certificate Owner</i>. TC Business ID is a typical example for <i>Client Certificates</i>.</p> <p>See section 3.4</p> |
| CSP | <p>Cryptographic Service Provider. This is specific middleware required to use smart cards or USB tokens with applications like MS Internet Explorer or MS Outlook.</p> |

See also *PKCS#11*.

| | |
|---|---|
| Enrollment Agent | <p>One of the possible delegated roles for Users. The roles are described in section 2.1.1.</p> <p>Personalize smart cards or cryptographic tokens on behalf of users. This role can only be assigned by the “PKI Superadministrator” or TC TrustCenter.</p> |
| Enrollment Officer | <p>One of the possible delegated roles for Users. The roles are described in section 2.1.1.</p> <p>The officer roles need to be combined with “Privileged User” or “Basic User” to be able to request certificates.</p> |
| ePIN | <p>Electronic PIN. A PIN which is being delivered by e-mail or SMS is denoted as ePIN.</p> <p>See section 3.3</p> |
| External PIN | <p>A PIN which is delivered by the Administrator to the User or to the web portal is denoted as <i>External PIN</i>. <i>External PINs</i> are administrated outside the system.</p> <p>See section 3.3</p> |
| External User | <p>One of the possible roles for Users. The roles are described in section 2.1.1.</p> <p>This is the identity mapped to the certificate as denoted in the Subject-DN of the certificate. It might be a natural person, a server or a team depending on the certificate type.</p> |
| Key Escrow | <p>The process to give an Administrator access to a private key and a certificate is called <i>Key Escrow</i>. The <i>Certificate Owner</i> is not informed of this process.</p> <p><i>Key Escrow</i> is a very sensitive process. Usually the required administrative roles are split between two persons.</p> |
| Key Escrow Administrator (Request) and (PSE) | <p>Possible roles. The roles are described in section 2.1.1.</p> |
| Key Recovery | <p>The process to make the private key and the certificate accessible again to the Certificate Owner is called Key Recovery.</p> |
| Key Recovery Officer | <p>One of the possible delegated roles for Users. The roles are described in section 2.1.1.</p> |
| NoLogin User | <p>One of the possible delegated roles for Users. The roles are described in section 2.1.1.</p> |
| PIN Letter | <p>One of the possible delegated roles for Users. The roles are</p> |

Administrator described in section 2.1.1.
Print PIN letters. This role can only be assigned by TC TrustCenter.

PKCS#10 Certificate request. It includes the public key as well as the requested subject name.
The encoding can either be binary (DER) or PEM. PEM encoded files only contain printable characters and start with "-----" (5 times '-').
All recoverable certificates will be issued as *PKCS#12 PSEs*. All other certificates will be requested using either web browser based key generation or copy&paste of a *PKCS#10* request (TC Domain Controller ID, TC Client Computer ID and TC RAS and IAS Server ID).
See sections 3.4 and 8.2

PKCS#11 This is a standard for middleware used for smart card or USB token access.
Applications like Firefox use this standard based middleware for smart card or USB token usage.
See also *CSP*.

PKCS#12 PSE A Personal Security Environment which contains the private key and the associated X509 certificate.
The PSE (Personal Security Environment) is encoded using the file format specified in the *PKCS#12* standard.
In Microsoft environments it is usually referred to as PFX.
All recoverable certificates will be issued as *PKCS#12 PSEs*. All other certificates will be requested using either web browser based key generation or copy&paste of a *PKCS#10* request (TC Domain Controller ID, TC Client Computer ID and TC RAS and IAS Server ID).
See sections 8.2, 3.9

PKI Administrator One of the possible delegated roles for Users. The roles are described in section 2.1.1.
The "PKI Administrator" can assign the following roles: "Revocation Officer", "Key Recovery Officer".

PKI Superadministrator One of the possible delegated roles for Users. The roles are described in section 2.1.1.
The "PKI Superadministrator" can assign the following roles: "PKI Administrator", "Registration Officer", "Enrollment Officer", "Unsuspending Officer", "Revocation Officer" and "Key Recovery Officer".

| | |
|-----------------------------|--|
| Privileged User | One of the possible roles for Users. The roles are described in section 2.1.1. |
| Registration Officer | One of the possible delegated roles for Users. The roles are described in section 2.1.1. The officer roles need to be combined with “Privileged User” or “Basic User” to be able to request certificates. |
| Revocation Officer | One of the possible delegated roles for Users. The roles are described in section 2.1.1. The officer roles need to be combined with “Privileged User” or “Basic User” to be able to request certificates. |
| SCEP | Simple Certificate Enrollment Protocol. See http://en.wikipedia.org/wiki/Simple_Certificate_Enrollment_Protocol for more details. Support for <i>SCEP</i> is described in section 7. |
| SCEP User | One of the possible roles for Users. The roles are described in section 2.1.1. All anonymously requested certificates through <i>SCEP</i> will be owned by this user. No other roles might be combined with this role. |
| Unsuspending Officer | One of the possible delegated roles for Users. The roles are described in section 2.1.1. The officer roles need to be combined with “Privileged User” or “Basic User” to be able to request certificates. |
| User | All individuals getting a certificate from TC ID Store or using the web portal to request certificates or receive certificate invites as well as to revoke, to suspend or to unsuspend certificates or to initiate key recovery are referred to as “Users”, regardless of their role. See section 2 |

11 List of Figures

| | |
|---|----|
| Figure 1: Overall Architecture | 5 |
| Figure 2: Request Approval Process Flow for Non-Recoverable Client Certs for “Basic Users” | 17 |
| Figure 3: Request Approval Process Flow for Recoverable Client Certs for “Basic Users” | 18 |
| Figure 4: Request Process Flow for Non-Recoverable Client Certs for “Privileged Users” | 19 |
| Figure 5: Request Process Flow for Recoverable Client Certs for “Privileged Users” | 20 |
| Figure 6: Single Mode Certificate Invite Process Flow for Non-Recoverable Certificates | 23 |
| Figure 7: Single Mode Certificate Invite Process Flow for Recoverable Certificates | 24 |
| Figure 8: Revocation/Suspension Process Flow for “PKI Administrators”/”Revocation Officers” | 27 |
| Figure 9: Revocation/Suspension Process Flow for <i>Certificate Owners</i> | 28 |