



TC TrustCenter

TC ID Store

Administrator Manual

TC ID Store
Version 1.8

Hamburg, Germany
April 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 BOFADE33

TC TrustCenter GmbH

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, „TC QSign“ und „TC ID Store“ 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, „TC QSign“ and „TC ID Store“ 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 | <i>Introduction</i> | 5 |
| 2 | <i>Setting Up Users</i> | 6 |
| 2.1 | Configuration Verification | 6 |
| 2.2 | Setting up Users and Groups | 7 |
| 2.2.1 | Setting up Groups | 7 |
| 2.2.2 | Setting up Users | 7 |
| 3 | <i>Deploying Client Certificates</i> | 10 |
| 3.1 | Deploying Client Certificates to Employees | 10 |
| 3.2 | Deploying Client Certificates to External Partners | 14 |
| 4 | <i>Requesting Server Certificates</i> | 22 |
| 5 | <i>Deploying Certificates via SCEP</i> | 24 |
| 5.1 | Overview | 24 |
| 5.1.1 | Pre-Authorized Certificate Requests for SCEP | 24 |
| 5.1.2 | Anonymous SCEP Requests | 24 |
| 5.2 | Sample SCEP Configuration | 25 |
| 5.2.1 | Configuring the VPN Server (Cisco ASA 55xx) | 25 |
| 5.2.2 | Configuring the VPN client (Apple iPad) | 28 |
| 5.3 | Futher reading | 32 |
| 6 | <i>Deploying Certificates on Smart Cards</i> | 33 |
| 7 | <i>Fundamentals</i> | 36 |
| 7.1 | Request Workflow: Certificate Request or Certificate Invite | 36 |
| 7.1.1 | Certificate Request | 36 |
| 7.1.2 | Certificate Invite | 36 |
| 7.2 | Grouping Users | 36 |
| 7.3 | Managing Certificates for “Affiliates” | 36 |
| 7.4 | Number of Certificates per User | 37 |
| 7.4.1 | Signing | 37 |
| 7.4.2 | Authentication | 37 |
| 7.4.3 | Encryption | 37 |
| 7.4.4 | Number of Certificates | 37 |
| 7.5 | Login Policy | 38 |
| 7.6 | Key Generation Policy | 39 |
| 7.7 | Administrator Hierarchy | 39 |
| 7.8 | PIN Methods | 40 |
| 7.9 | Billing Certificates to Cost-Centers | 41 |
| 7.10 | Customizing E-Mail-Templates | 42 |
| 7.10.1 | Account specific vs. product specific E-Mail Templates | 42 |
| 7.10.2 | Customizing E-Mail-Templates | 42 |
| 7.10.3 | Customizing E-Mail-Templates with Variables | 43 |
| 7.10.4 | E-Mail Automation | 45 |
| 8 | <i>The TC ID Store API</i> | 48 |
| 8.1 | Preparations for using the API | 48 |



| | |
|---|-----------|
| 8.2 Using the API in Custom Applications | 48 |
| 9 Glossary | 49 |
| 10 List of Figures | 52 |

TC ID Store Administrator Manual

You have purchased a TC ID Store (TC ID Store) for your Organization; this means you have accepted the certificate policy definitions of TC TrustCenter. As a TC ID Store Administrator you will be identified and registered accordingly and you'll get access to the TC ID Store Web Portal. The login credentials will be sent to you via e-mail. We recommend using certificates for portal login.

1 Introduction

TC ID Store is a system for issuing and managing certificates. It provides two basic issuance mechanisms, certificate requests and certificate invites. Only registered Users can receive an invite, or issue a request, so the first step is to register all Users who need to receive a certificate.

Once a User is registered in the system, they receive a UID and a password via e-mail. This will permit them to logon to the portal and request certificates. Once they are registered as Users, the Administrator will also be able to send them an enrollment invitation via e-mail as well.

The specific enrollment mechanisms vary, depending on the type of certificate requested. The sections that follow discuss User registration and certificate enrollment in more detail.

Some of the examples you will find later in this manual are based on the following company hierarchy.

This hierarchy will be used for demonstrating some typical use cases for the grouping of Users and the management of administrative granularity.

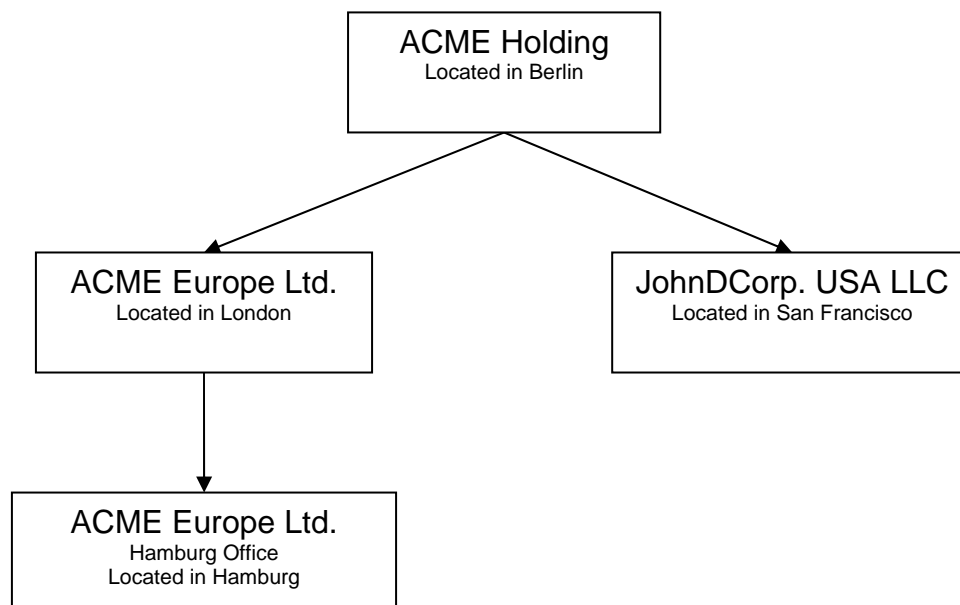


Figure 1: Hierarchy of our Sample-Company

2 Setting Up Users

Before you can deploy certificates the first time, you have to verify the configuration and setup the Users.

2.1 Configuration Verification

As a first step, please verify that the service has been setup the way you requested it. Please select the menu item “Configuration” in the left menu bar and select the sub-menu “Affiliates”. You should find your organization and all other requested affiliates properly listed here. You can request additional “Affiliates” at any time. Please also check in sub-menu ”Edit Contracts“ whether the appropriate contract is listed as *active*.



The screenshot shows the 'Edit Contracts' page in the TrustCenter interface. The page title is 'Edit Contracts' and it includes a navigation menu on the left with options like Home, Certificates, Users, Configuration, Edit Settings, Affiliates, Pre-Vetted Domains, Edit Contracts, and Reports. The main content area displays a table of contracts with the following data:

| Name | Amount | Reserved Balance | Currency | Created | Expires | Active |
|---------------------------------|----------|------------------|----------|---------|---------|--------|
| TC ID Store Class 3, 15,000 EUR | 15000.00 | 0.00 | EUR | 11/5/08 | 11/5/10 | true |
| ID Store Demo | 0.00 | 0.00 | USD | 11/4/08 | 11/5/08 | false |

Below the table, there are 'Export options' for CSV and Excel. A message above the table states: 'To edit a contract please click on the Name.'

Figure 2 Verifying the Contract History

Click on the active contract to verify the contract details.

Edit Contract
[Logout](#) [My Profile](#)

| Contract Details | Billing Contact | Billing Address |
|--|--|-----------------|
| Name*: TC ID Store Class 3, 15.000 EUR | VAT-ID: DE123456789 | |
| Billing Mode: Deposit | PO-Number: 2009001 | |
| Setup Fee*: 0.00 | Supplier-ID: LIE200901 | |
| Annual Fee*: 0.00 | Acc.Receivable No.: | |
| Currency: EUR | Start: 11/5/08 | |
| Amount*: 15000.00 | End: 11/5/10 | |
| Reserved Balance*: 0.00 | Contract Period*: 24 | |
| Initial Deposit*: 15000.00 | Auto Renewal: <input type="checkbox"/> | |
| Overdrawable: <input type="checkbox"/> | | |

[Submit](#) [Back](#)

Figure 3 Contract Details and Status

At the bottom on the “Contract Details” page the available certificate products are listed. Please check whether the requested certificate products are listed here and have been activated. You can deactivate certificate products which are not required. Deactivated certificate products are not shown when requesting certificates. You can re-activate deactivated certificate products at any time.

2.2 Setting up Users and Groups

Users have to be made known to system before they can request certificates or receive an invite. Users can be assigned to groups in order to restrict their visibility to other members of that group.

2.2.1 Setting up Groups

Grouping of Users is independent from the „Affiliates“. You can create and administrate Groups using the sub-menu ”Users“ | ”Groups“.

| Edit Group | Logout | My Profile |
|---|--|------------|
| Name*: ACME Europe Ltd. - Hamburg | User groups can be assigned indepently from affiliates | |
| Members: 1 | | |
| Submit Cancel | | |

Figure 4 Adding Groups

2.2.2 Setting up Users

In order to add users they have to be properly registered. Please select ”Users“ | ”Add User“ to open the ”Add User“ dialog. Fields marked with a red (*) are mandatory.

Note: Use the User’s e-mail address as the username.

The User's group must have been already created and is selected from a drop down menu.

You can provide user data in the following tabs. To save the user, press the 'Submit' button. Please note that all users must have been vetted according to the [CPD/CPS](#).

User Details
User Roles
Authentication Details

| | |
|---|---|
| Username*: <input type="text" value="Jane.Doe@trustcenter.de"/> | Title*: <input type="text" value="Mrs."/> |
| First Name*: <input type="text" value="Jane"/> | Middle Initials: <input type="text"/> |
| Last Name*: <input type="text" value="Doe"/> | User Principal Name: <input type="text" value="jado@trustcenter.de"/> |
| Email*: <input type="text" value="Jane.Doe@trustcenter.de"/> | External ID: <input type="text"/> |
| Affiliate*: <input type="text" value="ACME Europe Ltd. - London"/> | |
| Department: <input type="text" value="Sales"/> | |
| Language*: <input type="text" value="English (United States)"/> PIN via SMS: <input type="checkbox"/> | |
| User group: <input type="text" value="London_-_Sales"/> | Mobile Phone: <input type="text"/> |

Figure 5 Add User

The login credentials will be sent to the User via e-mail after clicking "Submit".

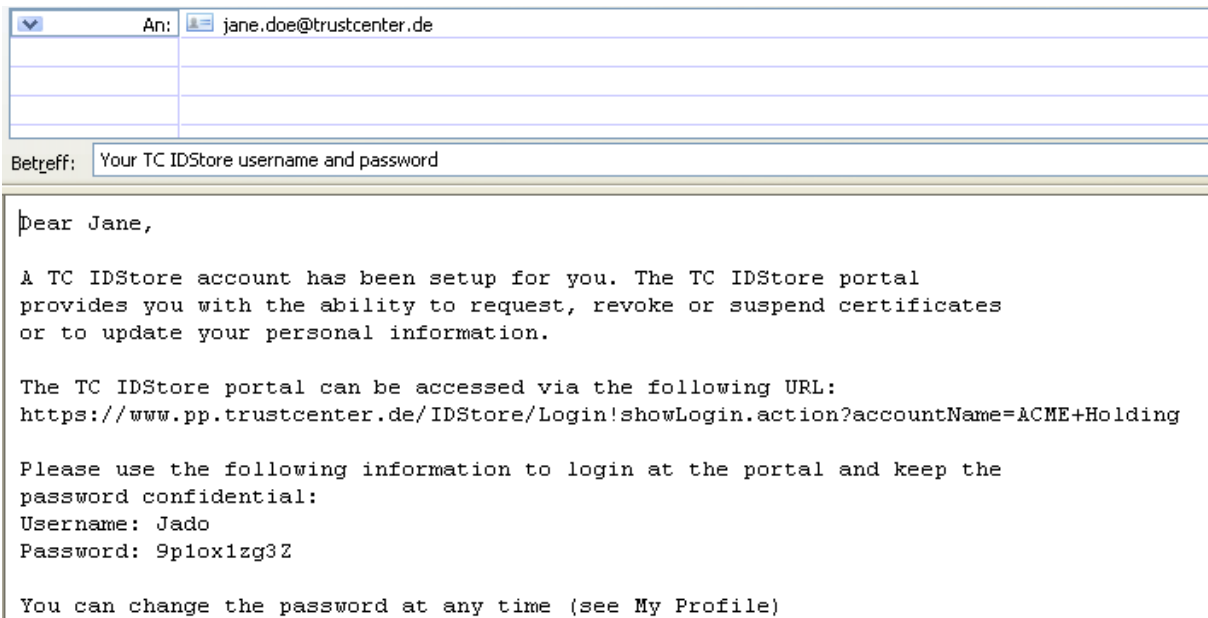


Figure 6 E-mail containing Login Credentials

TC ID Store provides a batch interface for adding larger numbers of Users. The format of the CSV file is displayed in the web portal.

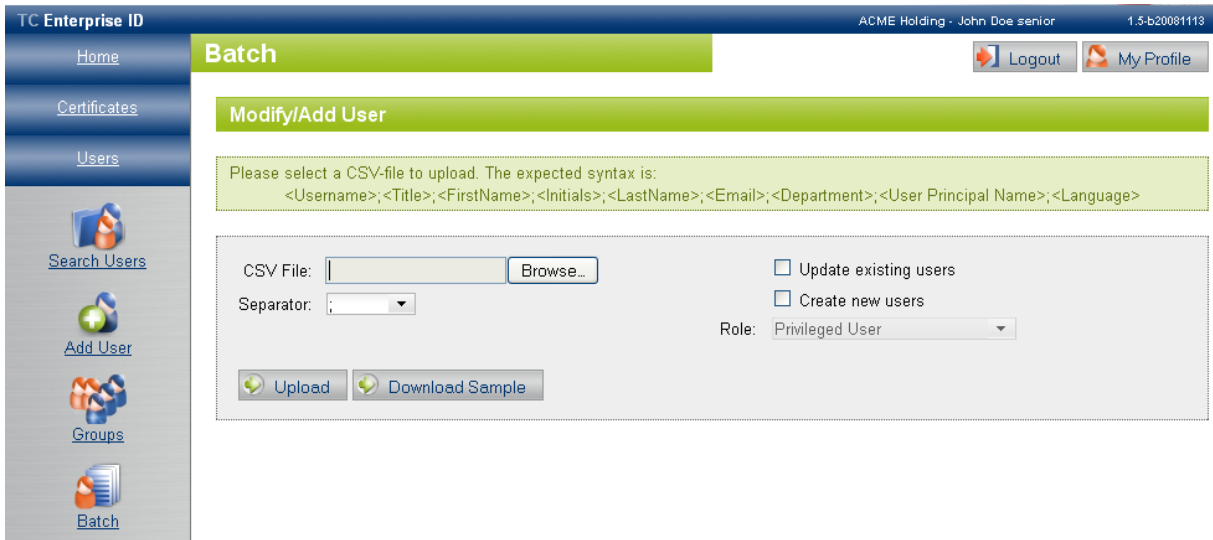


Figure 7 Batch UploadInterface for Adding Users

More details regarding the User management interface can be found in the statement of services.

3 Deploying Client Certificates

The certificate deployment processes will be differentiated between employees and external Users.

3.1 Deploying Client Certificates to Employees

All Users – except those with only the role "External Partner" can actively request certificates once they login to the portal. By default, Users will be given the role "Basic User". This role includes the permission to request certificates for themselves. Certificate requests by "Basic Users" must be approved (or rejected) by an Administrator.

Select "Certificates" | "Request Certificate" to request a certificate. A list of available certificate products will appear¹. Please select the appropriate product, e.g. "TC Business ID, recoverable enc, 1yr". This recoverable certificate will be delivered as download link for a *PKCS#12* file via e-mail.

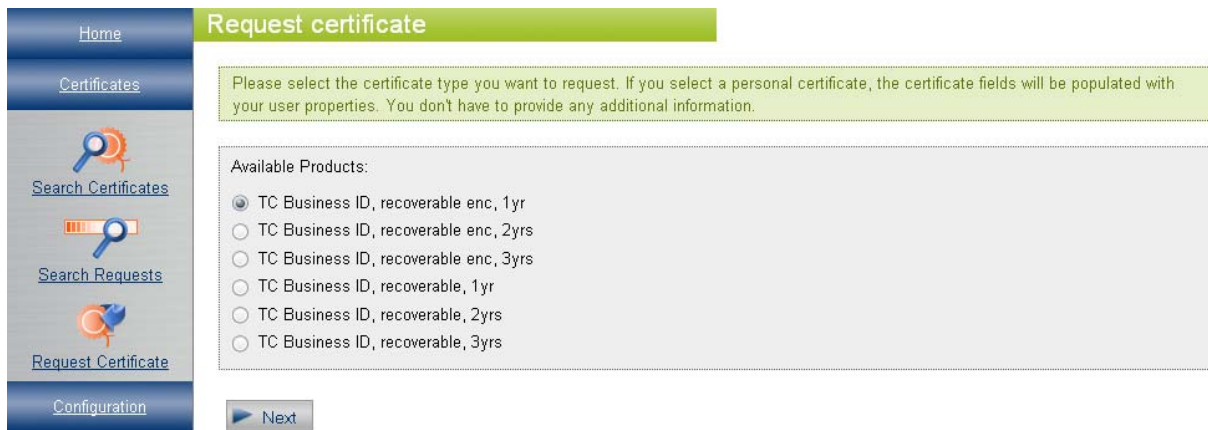


Figure 8 Select Certificate Product

Once the certificate product is defined, the certificate owner has to be selected. This can be the requestor, a new user or an existing user:

Note: Only a "PKI Administrator" or "Enrollment Officer" can trigger certificate requests for other users.

¹ This list only contains „active“ certificate types. You can remove certificate types from this list by deactivating them (see Statement of Service, section „Contracts“).

Request certificate

Request certificate for ...*:

myself

a new user

an existing user

[Back](#) [Next](#) [Cancel](#)

Figure 9 Select Certificate Owner

After selecting the user the data to be contained in the certificate will be displayed. Certain fields may be editable by the User. The request will be completed by pressing "Submit".

Request certificate

Please edit / verify the certificate properties.

Common Name: Jane Doe

Organisation: ACME Europe Ltd.

Organisational Unit:

Locality: London

State Or Province:

Country: GB

Email Address: jane.doe@trustcenter.de

User Principal Name: jado@trustcenter.de

[Back](#) [Submit](#)

Figure 10 Confirmation of Certificate Data

The final message acknowledges the successful submission of a certificate request.

Request certificate

The request was submitted successfully.
The certificate request is now waiting for an Administrator approval.



Figure 11 Acknowledgement of Certificate Request

After this step the certificate request is pending, waiting for approval by the “Enrollment Officer”. All “Enrollment Officers” in the User’s group are notified about pending requests.

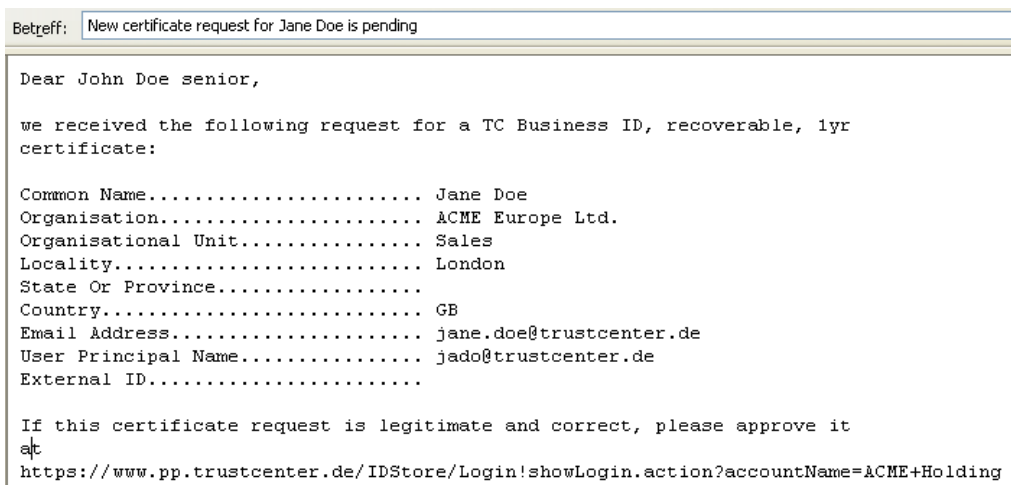


Figure 12 Request Notification

All pending requests are listed on the “Enrollment Officer’s” homepage of the web portal. The request details can be displayed by clicking on the Request-ID. Once the vetting procedure has been completed the request can be approved or rejected by clicking the appropriate action icon.

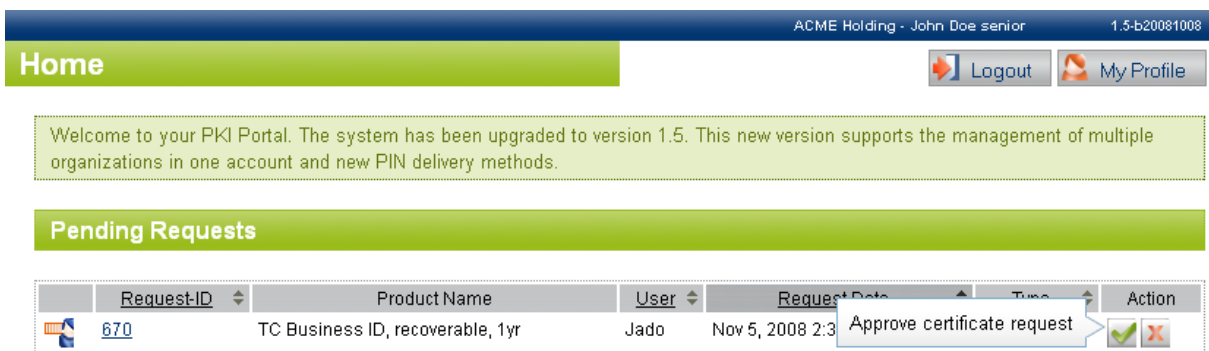


Figure 13 Certificate Request Approval

For certificate types like “TC Business ID, recoverable enc” the CA will generate a key pair and create an encrypted *PKCS#12 PSE* file containing the private key and the certificate. The PIN required to access the *PKCS#12* will be sent to the certificate

owner via e-mail (ePIN method). If “PIN via SMS“ has been selected in the User profile the PIN will be delivered via SMS to the mobile phone number given in the User profile.



Figure 14 PIN E-Mail

The *PKCS#12 PSE* is accessible on the TC TrustCenter web-site. The personalized download link will be sent as separate e-mail to the User.

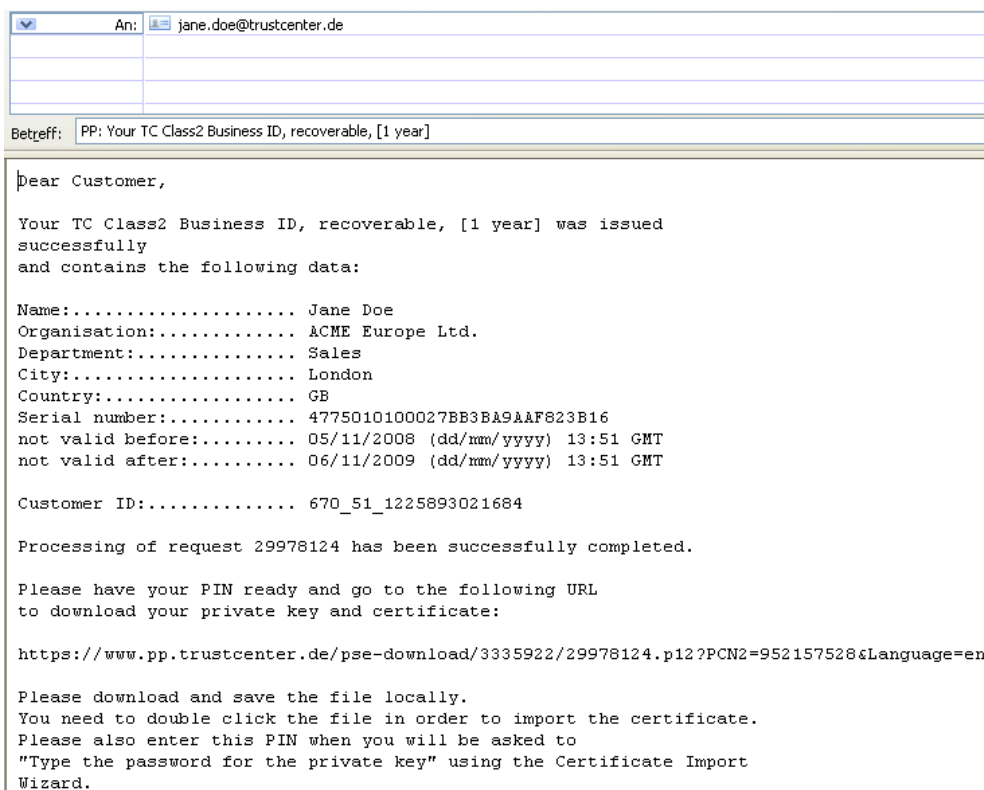



Figure 15 Download Link E-Mail

The download procedure will be initiated by clicking on the link contained in the e-mail.

Download

PIN submission

Please enter your PIN below and click "Start Download". Your encryption certificate along with the private key will be either installed automatically in your certificate store, or you can download a PKCS12 file and install it manually.

Your PIN 

© TC TrustCenter GmbH · E-Mail: info@trustcenter.de · <http://www.trustcenter.de>

Figure 16 PKCS#12 Download Web-Page

The Browser specific download dialog will be opened after entering the PIN for PKCS#12 PSE access. You will need to use the same PIN again for importing the PCKS#12 PSE into your certificate store.

3.2 Deploying Client Certificates to External Partners

With TC ID Store you can deploy certificates to external partners, i.e. to persons who are not members of your organization. Use certificate type "TC Personal ID" for external partners. This certificate type doesn't include an organization name and can be issued without setting up an affiliate.

Note: Please perform the registration according to the certificate policy definitions in all cases.

To issue certificates for external partners please setup the external partner as a User with role "External User" and registration class "Class 1". You have to create an appropriate "affiliate" (approved for registration class "Class 1"), if it doesn't already exist. "External Users" cannot actively request certificates so an Administrator has to trigger the certificate request for him.



Create Certificate Invitation

[Logout](#) [My Profile](#)

Step 1: Please select the product for your certificate invitation. If you select a personal certificate, the certificate fields will be populated using the selected user's properties. The user will be selected on the next page.

Available Products:

- TC Business ID, recoverable enc, 1yr
- TC Business ID, recoverable enc, 2yrs
- TC Business ID, recoverable enc, 3yrs
- TC Business ID, recoverable, 1yr
- TC Business ID, recoverable, 2yrs
- TC Business ID, recoverable, 3yrs
- TC Business ID, sign+auth, 1yr
- TC Business ID, sign+auth, 2yrs
- TC Business ID, sign+auth, 3yrs
- TC DomainController ID, 1yr
- TC DomainController ID, 2yrs
- TC DomainController ID, 3yrs
- TC Personal ID, 1yr
- TC Personal ID, 2yrs
- TC Personal ID, 3yrs

Figure 17 Certificate Invite for an External Partner

All existing Users will be displayed for selection by default. You can either scroll/page through the list or enter appropriate search criteria to find and select the right User.

Request certificate

Request certificate for ...*:

- myself
- a new user
- an existing user

[Back](#) [Next](#) [Cancel](#)

Figure 18 Select Certificate Owner

Once the User is selected, click Next. The request data will be taken from the User profile. Certain data fields can be edited by the Administrator. The field Organization field will remain blank for "TC Personal ID" certificates.

Create Certificate Invitation

[Logout](#) [My Profile](#)

Step 3: Please edit / verify the certificate properties. The invited user will not be able to change the values.

| | |
|----------------------|--|
| Common Name: | Jane Doe |
| Organisation: | |
| Organisational Unit: | <input type="text" value="Finance"/> |
| Locality: | <input type="text" value="Liverpool"/> |
| State Or Province: | <input type="text"/> |
| Country*: | <input type="text" value="GB"/> |
| Email Address: | jane.doe@trustcenter.de |
| User Principal Name: | jado@trustcenter.de |

[Back](#) [Submit](#)

Figure 19 Complete Request Data for Certificate Invite

If the data fields are correct the certificate invite can be submitted.

Create Certificate Invitation

[Logout](#) [My Profile](#)

Success! The Certificate Invitation was submitted successfully. The invited user will be notified to provide any missing information for the certificate request.

[Finish](#)

Figure 20 Certificate Invite Submitted

After submission, a certificate invite e-mail will be sent to the User (Jane Doe in this example).

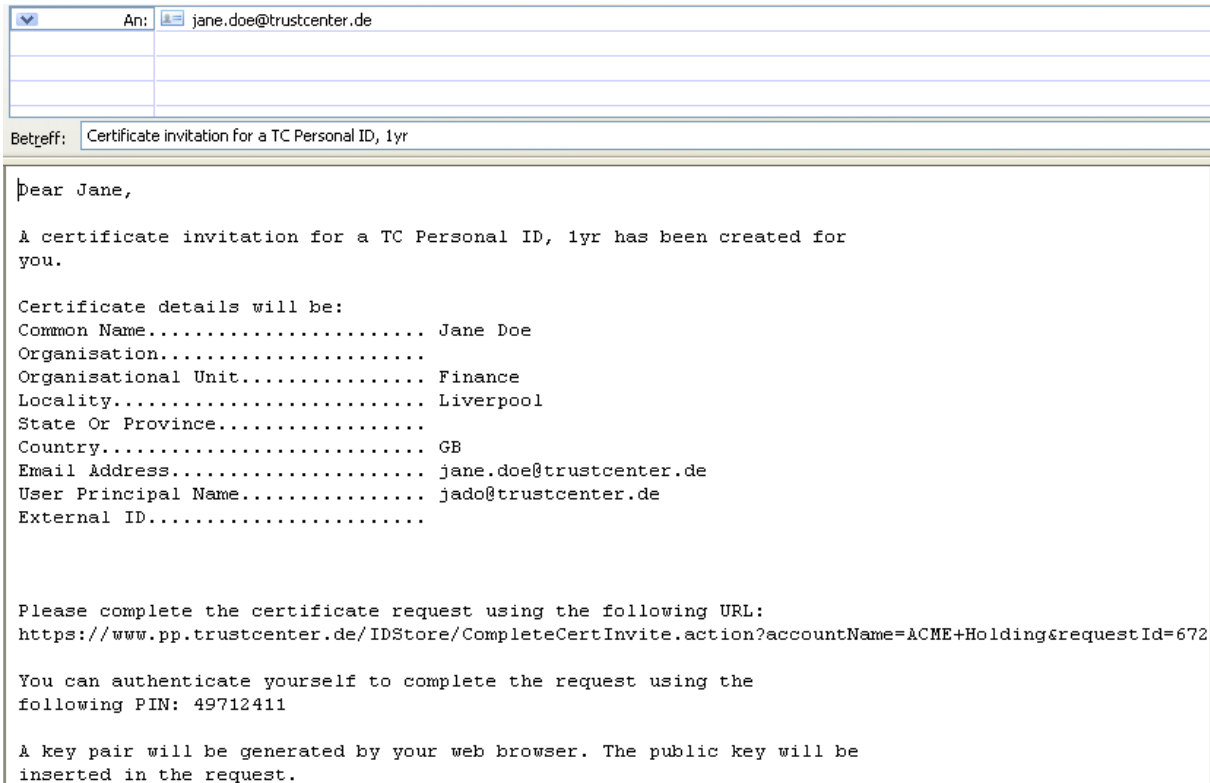


Figure 21 Certificate Invite E-mail

To complete the certificate invite the User needs to click on the URL and login by entering the PIN. The PIN is only valid for this certificate invite.



Figure 22 Login for Key Generation

The key generation process depends on the web browser being used. For Firefox there is a list box with two key lengths: "High Grade" and "Medium Grade". "High Grade" corresponds to 2048 bit RSA keys; "Medium Grade" corresponds to 1024 bit RSA keys.

Complete Certificate Invitation

To complete the certificate invitation, you have to provide a valid key pair. The key pair will be generated by your browser when you submit this form. Please select the required options and continue.

Key Length:

Figure 23 Key Generation with Firefox

In the case of Microsoft Internet Explorer there are 4 parameters to select:

Cryptographic Service Provider

Key Length

Private Key Protection Flag

Private Key Exportable Flag

If you want to use a smart card or USB token based key you must select the Cryptographic Service Provider associated with your smart card or USB token.

The key length of 2048 should be used in most cases. It offers the best level of security and current systems are fast enough to cope with keys of this size.

If you want to backup your key please select "Private Key Exportable". Please note that not all Cryptographic Service Providers for smart cards or USB tokens support this feature.

These parameters can be pre-defined by the "PKI Administrator" using the Key Generation policy for the particular certificate product.

Complete Certificate Invitation

To complete the certificate invitation, you have to provide a valid key pair. The key pair will be generated by your browser when you submit this form. Please select the required options and continue.

Cryptographic Service Provider:

Key Length:

Protect Private Key:

Private Key Exportable:

Figure 24 Key Generation with Internet Explorer

The certificate data will be displayed for final confirmation after the key generation process.

Complete Certificate Invitation

Please verify the certificate properties for this certificate invitation.

Common Name: Jane Doe
Organisation:
Organisational Unit: Finance
Locality: Liverpool
State Or Province:
Country: GB
Email Address: jane.doe@trustcenter.de
User Principal Name: jado@trustcenter.de



Figure 25 Certificate Data Confirmation

The certificate invite process is completed by pressing “submit”.

Complete Certificate Invitation

The certificate invitation was completed successfully.



Figure 26 Request Completed

TC TrustCenter will issue the requested TC Personal ID certificate and will send an e-mail containing a link to install the certificate in the web browser.

Note: The certificate can only be installed in the web browser that was used for key generation. Please do not install major browser updates between key generation and certificate installation.

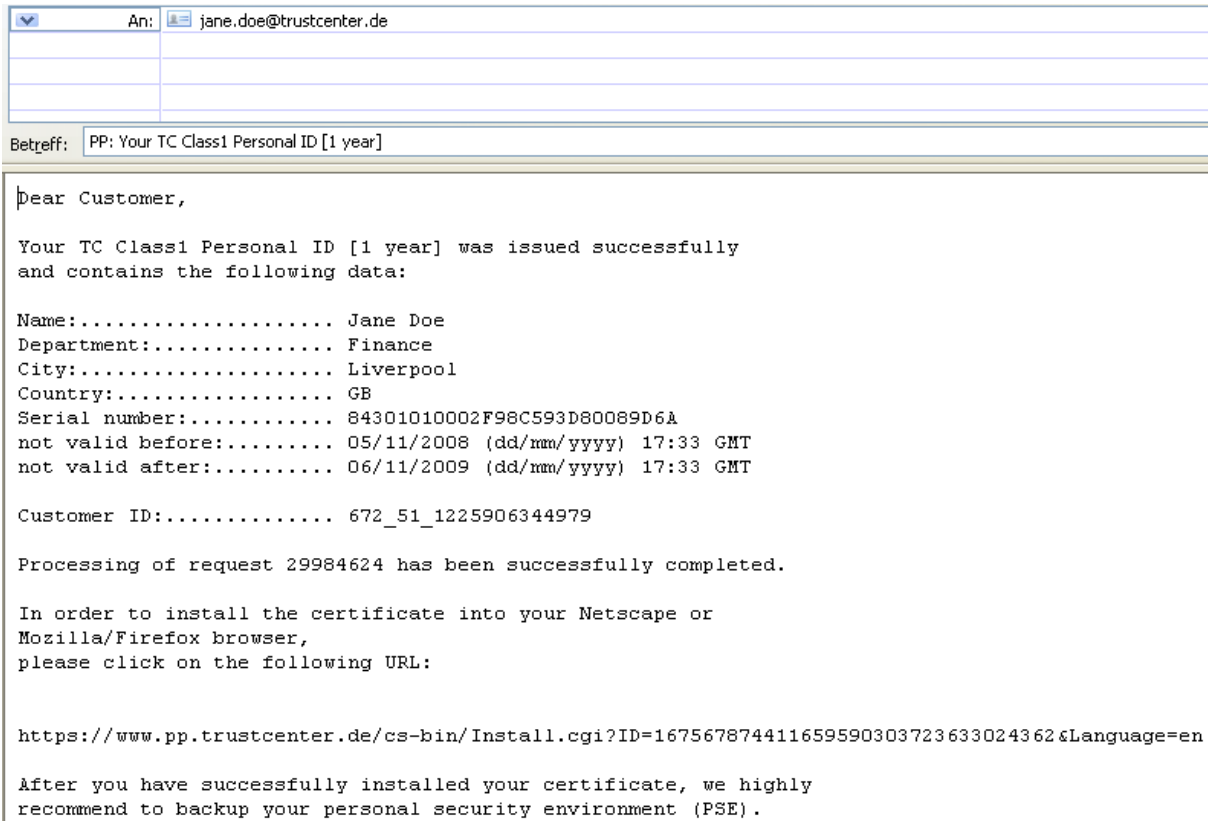


Figure 27 E-Mail containing Certificate Installation Link

The installation link directs the User to a web page displaying the certificate contents and containing the button “install certificate”. Press this button to finally install the certificate into the User’s web browser.

Certificate installation

Your certificate's data

Please check your certificate's data and click on "Install certificate", if you wish to import the certificate into your browser.

| | |
|--------------------------|--|
| Subject (DN): | C=GB, L=Liverpool, OU=Finance, CN=Jane Doe |
| Issuer (DN): | C=DE, O=TC TrustCenter GmbH, OU=Pre-Production TC TrustCenter Class 1 L1 CA, CN=Pre-Production TC TrustCenter Class 1 L1 CA VI |
| Serial number: | 0x84301010002F98C593D80089D6A (167567874411659590303723633024362) |
| Status: | Not revoked |
| Not valid before: | 05.11.2008 |
| Not valid after: | 06.11.2009 |
| Fingerprint: | DD:43:4B:80:98:FD:74:25:28:CA:76:1A:98:21:22:44 |

Install certificate

Figure 28 Certificate Installation Page

You should export and backup your certificate and private key as a *PKCS#12* file. You can then either restore your certificate, or transfer it to other software applications, e.g. e-mail client.

Note: Microsoft Internet Explorer and Microsoft Outlook use the same key store. So you don't have to import the *PKCS#12* file into Outlook if you installed it into Internet Explorer.

4 Requesting Server Certificates

Server certificates can also be requested using menu item *Certificates | Request Certificate*. Please select the appropriate certificate type from the list.



Request certificate

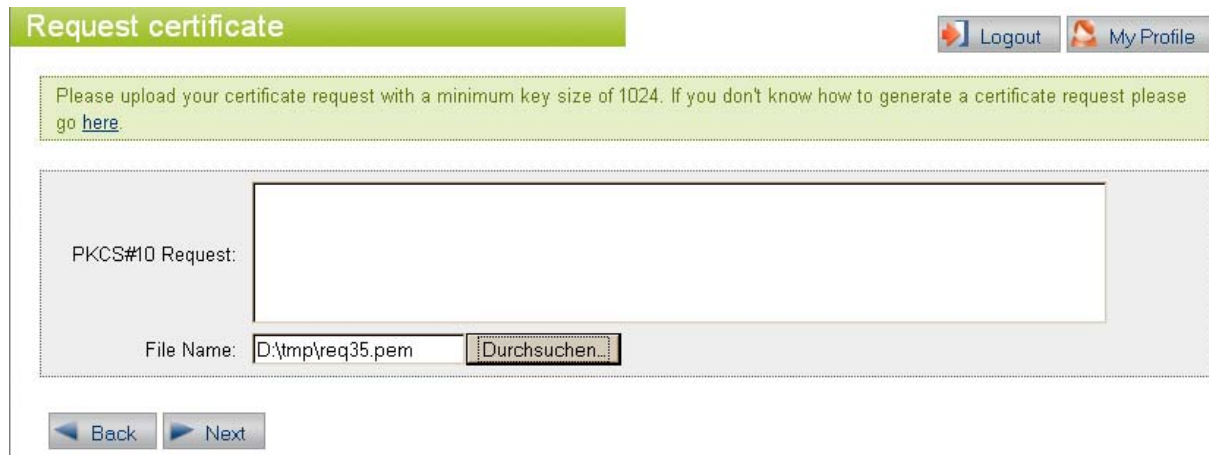
Please select the certificate type you want to request. If you select a personal certificate, you must provide your user properties. You don't have to provide any additional information.

Available Products:

- TC Trust SSL, 1yr
- TC Trust SSL, 2yrs
- TC Trust SSL, 3yrs

Figure 29 Server Certificate Product List

For the next step you need the *PKCS#10* certificate request as generated on the web server. Please either copy&paste it into the text field (base64 encoded) or select the file name and the encoding of the request file (base64 or binary).



Request certificate [Logout](#) [My Profile](#)

Please upload your certificate request with a minimum key size of 1024. If you don't know how to generate a certificate request please go [here](#).

PKCS#10 Request:

File Name:

Figure 30 PKCS#10 Upload

The request data will be displayed for confirmation in the next step.

Request certificate Logout My Profile

Please edit / verify the certificate properties for TC Trust SSL, 1yr.

Server Name*:
 Organisation: ACME Holding
 Organisational Unit:
 Locality: Berlin
 State Or Province:
 Country: DE
 Email Address:
 Additional Server Name:
 Additional Server Name:

Back Submit

Figure 31 Certificate Data Confirmation

Please select the appropriate product options as explained on the web page. Pressing “submit“ will .complete the certificate request.

Request certificate

The request was submitted successfully.
 The certificate request is now waiting for an Administrator approval.

Finish

Figure 32 Acknowledgement of Certificate Request

If a certificate request has not been generated by a “Privileged User” or a “PKI Administrator”, an “Enrollment Officer” has to approve it. The list of pending requests for their group is displayed on the web portal home page for all “Enrollment Officers”.

Pending Requests

| Request-ID | Product Name | User | Request Date | Type | Action |
|---|-------------------|------|------------------------|-------------|---|
|  13871 | TC Trust SSL, 1yr | Jado | Dec 4, 2009 2:31:44 PM | Certificate |   |

Figure 33 Approval of Server Certificate Request

After request approval by the “Enrollment Officer” and approval of the required domain (if no appropriate pre-vetted domain exists) the certificate will be issued and delivered via e-mail.

5 Deploying Certificates via SCEP

The simple certificate enrolment protocol (*SCEP*) is mainly being used by network devices, (e.g. VPN routers) and Apple mobile devices (e.g. iPad and iPhone).

5.1 Overview

TC ID Store offers two different methods to initiate *SCEP* enrollment:

Certificate Requests pre-authorized by an Administrator

Anonymous *SCEP* requests

The certificate request method is best suited when the certificate applicant should have a passive role. This is typically the case when deploying certificates to VPN clients, e.g. iPad. The “PKI Administrator” or “Enrollment Officer” can trigger the Certificate Request.

The Anonymous *SCEP* request method is best suited when the certificate applicant is in an active role. This is typically the case when deploying certificates to VPN servers, e.g. Cisco routers. Using this method a *SCEP* enrollment URL will be generated by the system. This URL can then be published or distributed by the “PKI Administrator”.

5.1.1 Pre-Authorized Certificate Requests for SCEP

The Administrator can trigger *SCEP* certificate requests with menu “Certificates” | “Request Certificate”. A *SCEP* enabled product has to be selected. Product names for *SCEP* enabled products start with “SCEP”. Click “Next” after selecting the appropriate *SCEP* enabled product. Then select the appropriate user and click “Next” again.

The user will then receive the certificate invite e-mail including the PIN and the *SCEP* enrollment URL.

5.1.2 Anonymous SCEP Requests

Before anonymous *SCEP* requests can be used the following steps are required:

Enable “Anonymous Requests” in Configuration | Settings.

Create a “SCEP User”, i.e. a user with the sole role “SCEP user”.

If anonymous requests are being used, the *SCEP* device needs to download or poll the certificate after the „PKI Administrator“ has approved the request.

The *SCEP* Enrollment URL for anonymous requests can be created using the menu “Configuration” | “Edit Contracts”, then open the active contract and select the appropriate *SCEP* enabled certificate product. Then select “Enrollment URL (*SCEP*)”.

To request a certificate for VPN Server select “SCEP TC VPN ID“, for a VPN Client like the iPhone select the “SCEP TC Business ID”.

Edit Product Configuration

Inactive products cannot be requested by users. They can be re-activated at any point in time.
Only visible products can be requested via the graphical user interface.

| Details | Key Generation Policy |
|--|--|
| Product-No.: 1.2.276.0.44.6.1.17.3.0 | Key Generation Method: PKCS10_UPLOAD |
| Profil-ID: 167602 | Key Provider: USER |
| Product Name: SCEP TC VPN ID Demo, 30 days | PIN Type: ePIN |
| Duration: 1.00 | Price: 0.00 |
| Enrollment URL (SCEP) | Currency: USD |
| | Visible: <input checked="" type="checkbox"/> |
| | Active: <input checked="" type="checkbox"/> |

Figure 34 – Edit Product Configuration

Select the Link “Enrollment URL (SCEP)” as depicted above.

Anonymous Request Link for SCEP TC VPN ID Demo, 30 days

Please select an user with the role "SCEP-user" to create a link for anonymous requests through SCEP-supported devices.
Note that anonymous requests can be submitted without authentication using this URL. The Enrollment Officer has to approve anonymous requests.

User Name*:

Request URL:

Figure 35 – Creating “Enrollment URL (SCEP)”

Select the appropriate user and click button “Create Link”. The URL can then be copied from the text box.

5.2 Sample SCEP Configuration

This section describes sample configurations for VPN servers and VPN clients. In our scenario we have a Cisco VPN server and an Apple iPad as VPN client using IPsec with certificate based authentication. We'll use “demovpn.trustcenter.de” as the VPN name.

Note: The contract in your TC ID Store account needs to provide the SCEP products. If your contract doesn't include these profiles contact our support.

5.2.1 Configuring the VPN Server (Cisco ASA 55xx)

In our sample scenario we use a Cisco ASA 5505 as the VPN server.

Please refer to the Cisco ASDM (Adaptive Security Device Manager) as well as the asdmug.pdf guide.

As a VPN server the device needs a VPN server certificate, the “SCEP TC VPN ID”.

5.2.1.1 Generating RSA Key

Before starting the certificate enrollment process, the RSA key pair needs to be generated with the `crypto key generate rsa` command. To generate the keys, you must first configure a host name and domain name.

```
ASA(config)# hostname demovpn
demovpn(config)# domain-name trustcenter.de

Demovpn(config)# crypto key generate rsa modulus 2048
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
```

Use the `crypto key zeroize rsa` command if an RSA key pair exists.

```
Demovpn(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All certs issued using these keys will also be
removed.
Do you really want to remove these keys? [yes/no]: yes
```

In order to view the key information use the `show crypto key mypubkey rsa` command.

5.2.1.2 Trust Point

Several CA related settings have to be configured in the VPN server. Use the `crypto ca trustpoint` command to get into ca-trustpoint configuration mode.

```
Demovpn# configure terminal
demovpn(config)# crypto ca trustpoint TCTrustCenter
demovpn(config-ca-trustpoint)# enrollment url <Enter-SCEP-
Enrollment-URL-here>
demovpn(config-ca-trustpoint)# enrollment retry count 12
demovpn(config-ca-trustpoint)# enrollment retry period 60
demovpn(config-ca-trustpoint)# fqdn demovpn.trustcenter.de
demovpn(config-ca-trustpoint)# subject-name cn=<FQDN>
```

Replace <FQDN> with the fully qualified name of your VPN server.

```
demovpn(config-ca-trustpoint)# ip-address 192.168.201.154
```

Replace 192.168.201.154 with the IP address of your VPN server.

```
demovpn(config-ca-trustpoint)# accept-subordinates
demovpn(config-ca-trustpoint)# client-types ipsec2
demovpn(config-ca-trustpoint)# exit
demovpn(config)# exit
```

² `Client-types ipsec` = specifies the client connection types for which this trustpoint can be used and indicates that IPSec client connections can be validated using this trust point.

The VPN server is now configured to retry twelve times in case the certificate is not successfully obtained from the CA. It will wait 60 minutes between each request to the CA. The fully qualified domain name (FQDN) used in the enrollment request is configured to be `demovpn.trustcenter.de`. The `subject-name` needs to set to the FQDN as well. The correct enrollment url needs to be obtained from the web portal (see section 5.1.2).

5.2.1.3 Root CA

For security reasons the root certificate has to be approved manually. Use the command `crypto ca authenticate` to trigger loading the root certificate from the CA.

```
Demovpn(config)# crypto ca authenticate TCTrustCenter
...
INFO: Certificate has the following attributes:
...
Do you accept this certificate? [yes/no]: yes
```

`TCTrustCenter` is the name of the previously configured trustpoint. On executing this command, the VPN server establishes a TCP connection to enrollment URL (via *SCEP*).

5.2.1.4 Requesting a TC VPN ID for the VPN server

After the CA certificate has been configured, the certificate for the VPN server can be requested using the command `crypto ca enroll`.

```
Demovpn(config)# crypto ca enroll TCTrustCenter
```

Now the VPN-Server certificate request is pending.

Note: If you use a anonymous SCEP-request url your "PKI Administrator" needs to approve the certificate request. If you receive the message "The certificate enrollment request failed!" wait until your "PKI Administrator" has approved the request. Your request should now be finished with "The certificate has been granted by CA!".

5.2.1.5 Configuring the IPsec VPN

To allow VPN connection to the VPN server some more steps are required. In our example the intermediate (sub) CA certificate "TC TrustCenter Class 2 L1 CA XI" has to be installed as well.

```
demovpn(config)# crypto ca trustpoint TC_Sub_CA_XI
demovpn(config-ca-trustpoint)# enrollment terminal
demovpn(config-ca-trustpoint)# crypto ca authenticate
TC_Sub_CA_XI
```

<Copy the base 64 encoded CA certificate. End with the word "quit" on a line by itself>

```
...  
-----END CERTIFICATE---
```

```
quit
```

```
INFO: Certificate has the following attributes:
```

```
Fingerprint: <value of the fingerprint>
```

```
Do you accept this certificate? [yes/no]: yes
```

```
Trustpoint 'TC_Sub_CA_XI' is a subordinate CA and holds a non  
self-signed certificate.
```

```
Trustpoint CA certificate accepted.
```

After installing the intermediate CA certificate a group-policy and the tunnel-group ipsec-attributes need to be configured. In our scenario we define a VPN_iPhone group policy as type ipsec-ra (i.e. IPSec Remote Access).

```
Demovpn(config)# tunnel-group VPN_iPhone type ipsec-ra
```

```
demovpn(config)# tunnel-group VPN_iPhone ipsec-attributes
```

```
Demovpn(config-tunnel-ipsec)# chain
```

The command `chain` includes the root certificate and any subordinate CA certificates in the transmission. Specify the name of the trustpoint that identifies the certificate to be sent to the IKE peer.

```
Demovpn(config-tunnel-ipsec)# trust-point TC_Sub_CA_XI
```

5.2.2 Configuring the VPN client (Apple iPad)

The certificate will be contained as payload in a device profile. The profile contains the certificate, the VPN configuration and a Web Clip as payload.

Initiate the profile installation by requesting a certificate for your device as described in section 5.1.1. In our scenario we have web mail access from the iPad and receive the enrollment PIN as SMS on a mobile phone.

5.2.2.1 Certificate request on the iPad

The enrollment URL is included in the certificate invite e-mail. Click on the link to open the enrollment web page.

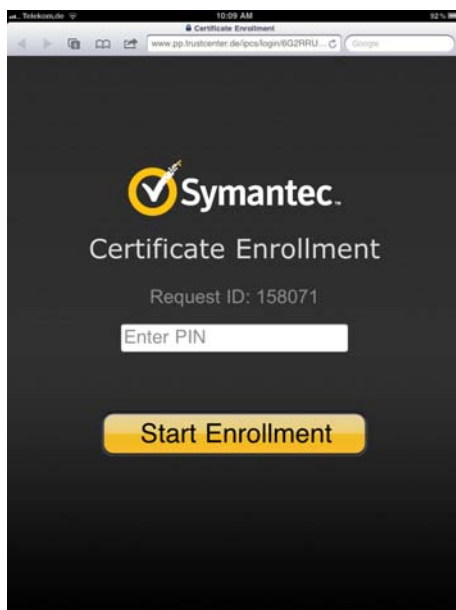


Figure 36 – SCEP Enrollment page

Enter the enrollment PIN and click on button “Start Enrollment”.



Figure 37 – SCEP Profile Overview

Click the “Install” button to proceed with the certificate installation.

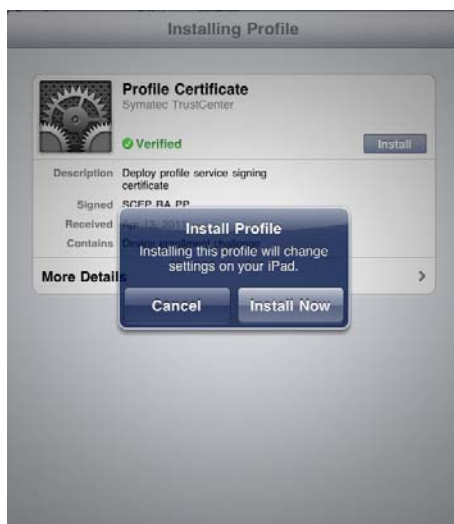


Figure 38 – Install Profile

Click the button “Install Now” in order to accept the profile installation.



Figure 39 – Profile installation

The profile installation might take some time as cryptographic keys have to be generated as part of it.



Figure 40 – Installed Profile

When the profile has been installed successfully you can find it on the device in menu “Settings” | “General” | “Profiles”. The profile can be entirely removed by clicking the “Remove” button. Don’t remove the profile now.

5.2.2.2 Establishing the VPN Connection

A VPN configuration is part of the device profile.



Figure 41 – VPN disabled

To enable the VPN connection move the slider to “ON”.



Figure 42 – VPN enabled

The VPN has been established. This is reflected by the VPN icon in the status bar. Our sample intranet page (<http://demovpn.trustcenter.de>) can be opened by clicking on the Web Clip.

5.3 Futher reading

- Cisco ASA 5505 Adaptive Security Appliance Hardware Installation Guide
<http://www.cisco.com/en/US/docs/security/asa/hw/maintenance/5505guide/ASA5505HIG.html>
- Cisco VPN Client User Guide for Windows
http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080930f21.shtml#client
- Configuring Tunnel Groups, Group Policies and Users
<http://www.cisco.com/en/US/docs/security/asa/asa70/configuration/guide/vpnggrp.html>

6 Deploying Certificates on Smart Cards

TC ID Store provides Enrollment Station support, i.e. the possibility to let an “Enrollment Agent” centrally personalize smart cards or cryptographic USB tokens on behalf of a user.

Prerequisites in order to use that feature:

1. User with role “Enrollment Agent” (this role can be granted to a user by the “PKI Administrator“)
2. Administrator with role “PIN Letter Administrator” (see [Administrator authorization form](#))
3. Access to supported smart cards or cryptographic USB tokens. The related PKCS#11 middleware has to be installed on the “Enrollment Agent’s “ computer.
4. A certificate product (e.g. TC Business ID SmartCard) with
 - a. PIN Method set to “PIN Letter” (“PKI Administrator“ can change this setting in menu Configuration | Edit Contract | <select active contract> | <select product> and modify PIN Method setting).
 - b. Key Provider set to “ENROLLMENT_AGENT” (“PKI Administrator“ can change this setting in menu Configuration | Edit Contract | <select active contract> | <select product> and modify Key Provider setting). This is only possible for certain products, e.g. TC Business ID.
 - c. Key Generation Method set to “SMARTCARD”. Please contact our support as this setting can only be modified by TC TrustCenter.

Triggering the certificate request for smart card based certificates is exactly as described in section 3.

Once the certificate request has been approved, the “Enrollment Agent” will see the pending personalization request.

Search Requests

Enter your search criteria below. Use "*" as wildcard character, empty fields are not included in search.


| | |
|-------------------------------------|--------------------------------------|
| Request-ID: <input type="text"/> | After: <input type="text"/> |
| User Name: <input type="text"/> | Before: <input type="text"/> |
| Product Name: <input type="text"/> | Request Type: <input type="text"/> |
| Request No.: <input type="text"/> | Request State: <input type="text"/> |
| Serial Number: <input type="text"/> | Request Origin: <input type="text"/> |
| UPS-ID: <input type="text"/> | |

Search Results

| <input type="checkbox"/> | Request-ID | Request No. | UPS-ID | Product Name | User | Request Date | Status | Type | Action |
|-------------------------------------|------------|-------------|--------|--------------------------------|-------------------------|--------------------------|------------|-------------|--------|
| <input checked="" type="checkbox"/> | 158068 | --- | | TC Business ID Smart Card, 1yr | John.Doe@trustcenter.de | Apr 13, 2011 10:00:20 AM | Incomplete | Certificate | |
| <input checked="" type="checkbox"/> | 158067 | --- | | TC Business ID Smart Card, 1yr | Jane.Doe@trustcenter.de | Apr 13, 2011 9:59:59 AM | Incomplete | Certificate | |

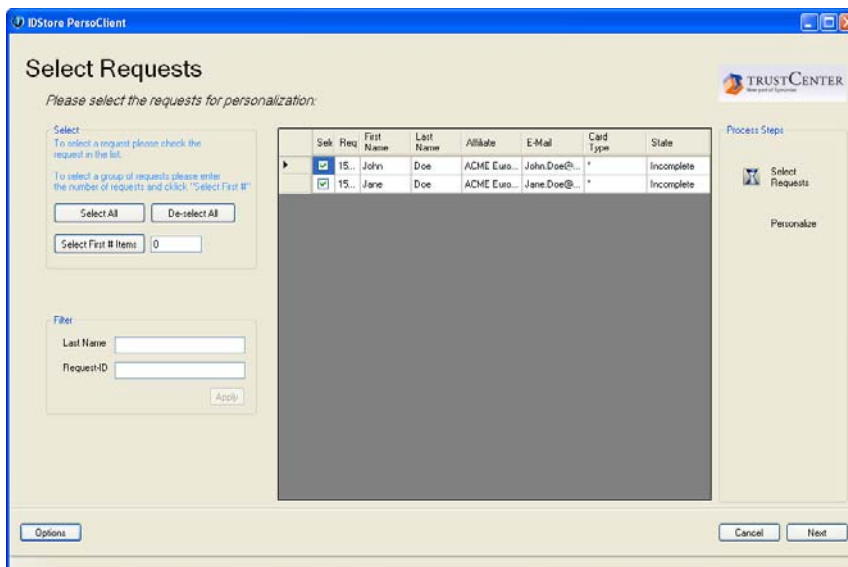
Export options:

Figure 43 – Personalization Requests

The personalization can be started by either clicking the action icon  or by selecting all requests to be personalized within one batch and clicking the button



Note: If more than one certificate has to be personalized to one smart card or cryptographic token, all requests *must* be personalized in one single batch.



The screenshot shows the 'Select Requests' dialog box in the IDStore PersoClient application. It features a table with columns for 'Selk', 'Preq', 'First Name', 'Last Name', 'Affiliate', 'E-Mail', 'Card Type', and 'State'. Two rows are visible, both with 'Incomplete' status. The dialog includes 'Select All', 'De-select All', and 'Select First # Items' buttons, a 'Filter' section with 'Last Name' and 'Request-ID' input fields, and a 'Process Steps' sidebar with 'Select Requests' and 'Personalize' buttons.

Figure 44 – TC PersoClient

The TC PersoClient will be started to personalize the certificates to the smart cards. If the PIN Method PIN Letter has been configured for the product, the “PIN Letter Administrator” will find the list of all PIN letters to be printed in the web portal.

Print PIN Letters

Enter your search criteria below. Use "*" as wildcard character, empty fields are not included in search.


| | |
|-----------------------------------|--------------------------------------|
| User Name: <input type="text"/> | Serial Number: <input type="text"/> |
| Request No.: <input type="text"/> | After: <input type="text"/> |
| Request-ID: <input type="text"/> | Before: <input type="text"/> |
| Printstatus: <input type="text"/> | Printed after: <input type="text"/> |
| | Printed before: <input type="text"/> |

Result

| <input type="checkbox"/> | Request-ID | Request No. | Product Name | User | Request Date | Print date | Printstatus | Action |
|--------------------------|------------|-------------|--------------------------------|-------------------------|--------------------------|------------|-----------------|--------|
| <input type="checkbox"/> | 158067 | 77570924 | TC Business ID Smart Card, 1yr | Jane.Doe@trustcenter.de | Apr 13, 2011 10:40:37 AM | | Not yet printed | |
| <input type="checkbox"/> | 158073 | 77570724 | TC Business ID Smart Card, 1yr | John.Doe@trustcenter.de | Apr 13, 2011 10:35:24 AM | | Not yet printed | |

Export options: [CSV](#) [Excel](#)

Figure 45 – PIN Letter Printing Requests

All PIN Letters to be printed can be selected in menu “Administration” | “Print PIN Letters”. A PDF document containing all PIN Letters will be downloaded automatically by clicking the button . The PDF document has to be printed using the Adobe Reader.

Note: The “PIN Letter Administrator’s” computer should have disc encryption enabled since the PDF document contains the PINs in the clear. The PDF document should be securely erased once it has been printed.

7 Fundamentals

This chapter covers some important principal topics required for setting up a PKI.

7.1 Request Workflow: Certificate Request or Certificate Invite

TC ID Store offers two different workflows for deploying certificates. Both workflows are triggered by menu “Request Certificates”.

7.1.1 Certificate Request

A certificate request is usually initiated by the certificate owner. This gives the certificate owner full control over the time frame of the request. This is usually the best choice in the case of web server administrators requesting a SSL Server certificate since they know best when the certificate is required and what type of certificate is required.

7.1.2 Certificate Invite

For client certificates the Administrator typically wants to have full control over the deployment. He can trigger a certificate request for set of Users, e.g. a department. In the case of a certificate invite the certificate product and all the data about the “Certificate Owner” are pre-defined. The User (= “Certificate Owner”) only has to click a link to complete the certificate invite, usually by having the key generated by the web browser.

Since most of the decisions are made by the “Enrollment Officer” the probability of mistakes by the User is minimal.

7.2 Grouping Users

In some real world scenarios User visibility and officer roles need to be restricted.

In our sample corporation “JohnDCorp. USA LLC” the employees in one company shouldn’t be able to “see” the employees of the other companies. To achieve this goal we create a group “JohnDCorp. USA LLC” and assign all employees of that company to this new group.

If a User belongs to a group he can only “see” other Users if they belong to the same group.

In a second step we want to restrict the permissions of the “Enrollment Officers” of “ACME Europe Ltd.” to that subsidiary. To achieve this, we create the group “ACME Europe Ltd.” and all its employees and the „Enrollment Officer“ of that subsidiary are assigned to that group.

Group restrictions do *not* apply to “PKI Administrators” or “PKI Superadministrators”. Both roles can act across all groups – even if they are a member of a group. Note that Users can belong to only one group

7.3 Managing Certificates for “Affiliates”

When issuing certificates to employees of a subsidiary or a Joint-Venture it is necessary to request appropriate “Affiliates” from TC TrustCenter (see Configuration | Affiliates). A shareholder relationship between the TC ID Store Account owner and an „Affiliate“ is not required. You can request an “Affiliate” for large Offices or even customers – if they agree. This concept of “Affiliates” allows for a registration process



that confirms with the certificate policy definition – even in the case of complex corporate hierarchies.

The "Affiliate" (object) contains the following data fields: Organization, Location, State or Province Name Country, a display name, data regarding the company registration and the vetting level ("level of trust"). The data fields Organization, Location, State or Province Name and Country will be contained in the associated certificates. If the employees of the Hamburg Office want to have the Country Code "DE" and the city name "Hamburg" in their certificates a separate affiliate is required – even though the Hamburg office is not a separate legal entity.

Users should be assigned to the appropriate "Affiliate" when they are first created.

As already described in section 7.2 Users belonging to a group can only "see" Users belonging to the same group. If the employees of different affiliates shouldn't be able to "see" each other you can use the group concept. We recommend that you create groups with a name similar to the affiliate's display name. For our example with the Hamburg office the group name would be "ACME Europe Ltd. – Hamburg".

7.4 Number of Certificates per User

In principal certificates can be used for three different main purposes:

Signature

Authentication

Encryption

This means that up to three certificates per User can be used.

The recommended number of certificates per User depends on the application environment. There are good reasons to distinguish 3 different certificate usages

7.4.1 Signing

Signing: (non-Repudiation, content commitment). You need to see what you sign before you sign – just as in real life. This can have significant legal impact and PIN entry for every signature is recommended. Key recovery is not recommended for signing keys where non-repudiation is important.

7.4.2 Authentication

Technically this is signing random data without ever seeing it. For practical reasons PIN entry for every authentication is not recommended. PIN caching for a specified time frame is more convenient and usually leads to better (i.e. more secure) PINs.

7.4.3 Encryption

Key recovery is very important if encryption is used, and there can be legal requirements for it. Since key recovery isn't required for authentication or signing keys and its use potentially calls into question the integrity of those keys, the encryption key should be used only for encryption.

7.4.4 Number of Certificates

In real environments the recommended number of certificates per User also depends on the application landscape. There are good reasons to use separate certificates for separate purposes.

Encryption is mainly used in conjunction with e-mail security. Most e-mail applications support different certificates for signing and encryption of messages, e.g.

Outlook Express 6, Outlook 2003 and Thunderbird all support dual certificates. Outlook Express 5 (and earlier) does *not*.

The following table gives an overview over typical combination of certificate purposes and the related certificate products:

| Number of Certificates per User | Certificate purpose | Applications | Suited Certificate Products |
|---------------------------------|---|---|--|
| 3 | Signature Authentication Encryption | Document signing with MS Office, Adobe Acrobat etc. E-mail Signature and E-mail Encryption with Outlook Express 6, Outlook 2003 Thunderbird or e-mail gateways SSL Client authentication for web portals | TC Business ID, sign TC Business ID auth TC Business ID, recoverable enc |
| 2 | Signature + Authentication Encryption | E-mails signature and E-mail encryption with Outlook Express 6, Outlook 2003, Thunderbird or e-mail gateways SSL Client authentication for web portals | TC Business ID, sign+auth TC Business ID, recoverable enc |
| 1 | Signature + Authentication + Encryption | E-mails signature and E-mail encryption with Outlook Express 6, Outlook 2003, Thunderbird SSL Client authentication for web portals | TC Business ID or TC Business ID , recoverable or TC Personal ID |

Table 1 Number of Client Certificates per User

7.5 Login Policy

Two methods of user authentication are supported:

Username + Password and
Certificate based login

All client certificates suitable for authentication issued through the related account can be used for login.

Certificate login is more convenient as the user doesn't have to type in the lengthy username and the secure and thus also lengthy password. Certificate login is also much more secure as it doesn't transmit any secrets over the web (which might be subject to phishing attacks).

The login policy can define certificate login as mandatory for either

all administrative roles or
all users.

7.6 Key Generation Policy

In some PKI environments the key generation policy must be standardized for a certificate product.

In TC ID Store the key generation policy can be defined by the “PKI Administrator” in “Configuration | Contracts | select active Contract | <Product ID> | Tab “Key Generation Policy” “.

Users cannot deviate from these policy settings.



Details | Key Generation Policy

Minimum Key Length: 2048

Private Key Exportable: No

Strong Key Protection: Yes

Only MS IE: Yes

Allowed CSPs: SafeNet RSA CSP

Figure 46 Defining a Key Generation Policy

By defining a set of CSP names the use of a cryptographic token (supported by these CSPs) can be enforced.

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.

7.7 Administrator Hierarchy

In the default configuration the Administrator gets the role “PKI Administrator”. The “PKI Administrator” is setup after appropriate vetting by TC TrustCenter. “PKI Administrators” cannot assign the role “PKI Administrator” to anyone else.

The role “PKI Administrator” contains the following roles:

“Registration Officer”: This role is responsible for User registration.

“Enrollment Officer”: This role is responsible for creating certificate invites, approving certificate requests and selecting the PIN model. Certificate requests from “Privileged Users” do not need to be approved.

“Revocation Officer”: This role is responsible for performing certificate suspension and revocation. Users can suspend or revoke any certificate owned by them.

“Unsuspending Officer”: This role is responsible for unsuspending certificates. This task requires checking that the original User is still in possession of the key and is separate from the role of “Revocation Officer”.

“Key Recovery Officer”: This role can initiate key recovery. Users can initiate key recovery for any certificate owned by them.

The “PKI Administrator” can assign the roles “External User”, “Basic User”, “Privileged User”, “Revocation Officer” and “Key Recovery Officer” to Users. The other roles can only be assigned by TC TrustCenter.

You can realize a 4-eyes-principle by assigning the roles “Registration Officer” and “Enrollment Officer” to different persons. The “Registration Officer” is responsible for identifying the User and to setting up the User in the web-portal. The “Enrollment Officer” is responsible for verifying this data when creating certificate invites or approving certificate requests.

7.8 PIN Methods

TC ID Store supports 4 different PIN methods:

ePIN (e-mail)

ePIN (SMS)

External-PIN

PIN Letters

The *ePIN* (e-mail) method is selected by default. It is appropriate for most environments.

Alternatively the *ePIN* (SMS) method can be selected on a per User basis. The cell phone number (incl. international dialing code) as well as the flag “PIN via SMS” can be entered in the User data.

Sending the PIN via a different communication channel than the request URL significantly increases the overall security. This is especially relevant if the User’s e-mail account can be accessed (even read-only) by other Users.

You can edit the user's data in the following tabs. To save your changes, press the 'Submit' button.

| User Details | User Roles | Authentication Details |
|--|--|---|
| Username*: <input type="text" value="John.Doe@trustcenter.de"/> First Name*: <input type="text" value="John"/> Last Name*: <input type="text" value="Doe"/> Email*: <input type="text" value="John.Doe@trustcenter.de"/> Affiliate*: <input type="text" value="ACME Europe Ltd, - Hamburg"/> Department: <input type="text" value="Test-Lab"/> Language*: <input type="text" value="English (United States)"/> User group: <input type="text" value="Hamburg - TestLab"/> | Title*: <input type="text" value="Herr"/> Middle Initials: <input type="text"/> User Principal Name: <input type="text" value="jodo@trustcenter.de"/> External ID: <input type="text"/> | PIN via SMS: <input checked="" type="checkbox"/> PIN via SMS to Mobile Phone number Mobile Phone: <input type="text" value="+447807522345"/> |
| <input type="button" value="Submit"/> <input type="button" value="Cancel"/> | | |

Figure 47 ePIN (SMS) Activation

As an alternative to the ePIN-Method the PIN method "External PIN" can be selected on a per product basis. This method is especially suited for environments with existing PINs, e.g. in logins for employee portals.

When the External PIN method is used, no PIN will be distributed by the system. The Administrator will provide the PIN for each request. He is also responsible for distributing the PINs to the Users.

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

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.

Note: PIN Methods *ePIN* and *External PIN* cannot be used in conjunction with the "Enrollment Agent" and TC PersoClient.

When selecting PIN Letter, the "PIN Letter Administrator" has to print the automatically generated PIN letters on a secure printer (PDF document).

7.9 Billing Certificates to Cost-Centers

Some organizations want to manage all certificates through a central system but have the need to allocate the certificate costs to different cost centers.

TC ID Store supports this with the following features:

Setup a group for each cost-center and assign the users to the appropriate cost-centers.

Use Certificate Reports to see the certificates issued for the individual cost centers. This report includes the certificate prices, their issuance date and the product name grouped by the respective group.

7.10 Customizing E-Mail-Templates

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

Inform the applicant about the corporate 1st level support

Use a specific wording, e.g. in “Expiry E-mail 3”

Adapt the e-mail template to your Corporate Identity

Disable particular e-mails, e.g. “Revoke Certificate”

7.10.1 Account specific vs. product specific E-Mail Templates

E-mail templates can be defined to be account specific or product specific, see

Configuration | E-mail Templates or

Configuration | Edit Contracts | select Active Contract | select a particular product

When sending an e-mail, the system tries to use the product specific template first. If this doesn't exist the system tries to use the account specific e-mail template. If this doesn't exist the default e-mail template will be used.

Account specific e-mail templates will be used for all products for which no product specific e-mail template is defined.

As a rule of thumb, use account specific e-mail templates rather than product specific e-mail templates if possible. Only if this would need too much scripting (see section 7.10.4) should you use product specific e-mail templates for the relevant products.

Note: The system uses the most specific e-mail template available for a particular purpose.

7.10.2 Customizing E-Mail-Templates

The account specific e-mail templates can be accessed at Configuration | E-mail Templates.

A separate e-mail template is available for each process and supported language.

[Home](#)
[Certificates](#)
[Users](#)
[Configuration](#)

Email Templates

[Logout](#) [My Profile](#)

Edit your Email Templates.

Email template language: English (United States) Refresh

| | Template name | Template type | Active | Actions |
|-------------------------------------|--|-------------------|--------|---------|
| <input type="checkbox"/> | New User | Default | true | |
| <input type="checkbox"/> | Password Lost | Default | true | |
| <input type="checkbox"/> | Certificate Invite | Default | true | |
| <input type="checkbox"/> | Request Approval | Default | true | |
| <input type="checkbox"/> | PIN Delivery Email | Default | true | |
| <input type="checkbox"/> | PIN Delivery SMS | Default | true | |
| <input type="checkbox"/> | Certificate Delivery Email (PKCS10) | Default | true | |
| <input type="checkbox"/> | Certificate Delivery Email (PSE) | Default | true | |
| <input type="checkbox"/> | Certificate Delivery Email (Browser) | Default | true | |
| <input checked="" type="checkbox"/> | Suspend Certificate | Customer Specific | true | |
| <input type="checkbox"/> | Unsuspend Certificate | Default | true | |
| <input type="checkbox"/> | Recover Certificate | Default | true | |
| <input type="checkbox"/> | Key-Escrow (Admin) | Default | true | |
| <input type="checkbox"/> | Key-Escrow (PIN) | Default | true | |
| <input type="checkbox"/> | Revoke Certificate | Default | true | |
| <input type="checkbox"/> | Expiry Email 1 | Default | true | |
| <input type="checkbox"/> | Expiry Email 2 | Default | true | |
| <input type="checkbox"/> | Expiry Email 3 | Default | true | |

Figure 48 List of Different E-Mail Templates

Default e-mail templates can be customized by clicking on the “Template name” (see Figure 48). The template text can either be edited directly using the edit box (see Figure 49) or the text can be copied into an external editor, modified there and be copied back.

Note: A User with role “NoLogin User” doesn’t receive the “New User” e-mail (see Figure 48).

Once you have modified and saved an e-mail template using the “Save” button, this modified template will automatically replace the default one.

Modified e-mail templates are clearly marked, see e-mail template for “Suspend Certificate” (see Figure 48).

They can be reverted to the default value by removing the modification, i.e. clicking the action icon.

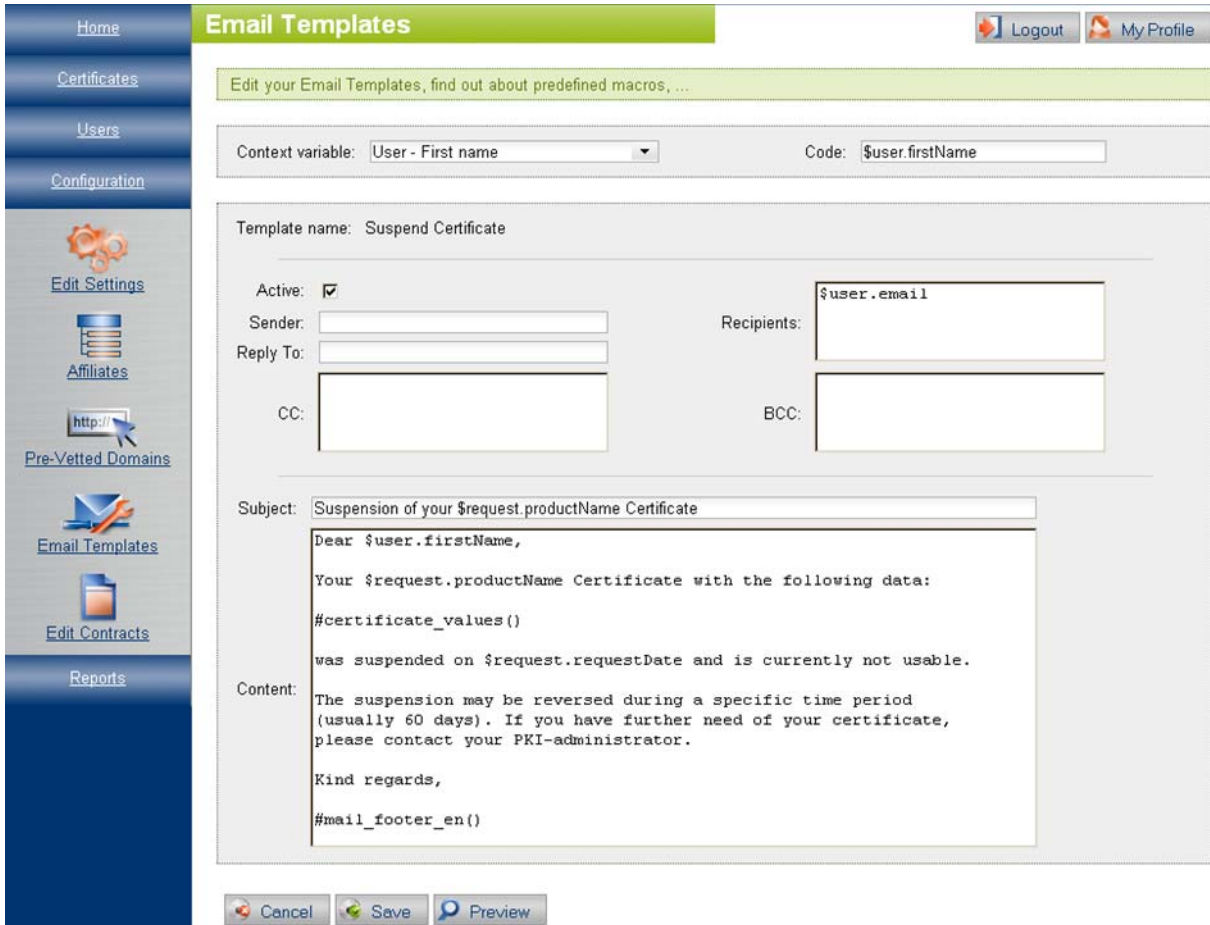
If a particular e-mail should not be sent at all, you can uncheck the checkbox “Active”.

Emails can be sent out as plain text or as HTML emails.

7.10.3 Customizing E-Mail-Templates with Variables

If context variables are required (see section 7.10.4 for details) the appropriate variable can be selected in the list box “Context variable” at the top. The required “code” can be copied from the field labeled “Code” next to it as shown in Figure 49 (`$user.firstName`).

You can use the “Preview” button to see if all context variables are being rendered as expected (see Figure 50).



The screenshot shows the 'Email Templates' management interface. The left sidebar contains navigation links: Home, Certificates, Users, Configuration, Edit Settings, Affiliates, Pre-Vetted Domains, Email Templates (highlighted), Edit Contracts, and Reports. The main content area is titled 'Email Templates' and includes a 'Logout' and 'My Profile' button. Below the title is a subtitle: 'Edit your Email Templates, find out about predefined macros, ...'. The configuration form for the 'Suspend Certificate' template includes the following fields:

- Context variable: User - First name (dropdown)
- Code: \$user.firstName
- Template name: Suspend Certificate
- Active:
- Sender: [text input]
- Reply To: [text input]
- CC: [text input]
- Recipients: \$user.email
- BCC: [text input]
- Subject: Suspension of your \$request.productName Certificate
- Content:


```
Dear $user.firstName,

Your $request.productName Certificate with the following data:

#certificate_value()

was suspended on $request.requestDate and is currently not usable.

The suspension may be reversed during a specific time period
(usually 60 days). If you have further need of your certificate,
please contact your PKI-administrator.

Kind regards,

#mail_footer_en()
```

At the bottom of the form are buttons for 'Cancel', 'Save', and 'Preview'.

Figure 49: Sample E-Mail-Template (Suspend Certificate)

Note: When changing the Sender address to an email address of your domain, you might encounter issues to receive such emails because some email systems consider emails with their own domain coming from outside as invalid and reject them.

Note: When using the batch feature (Batch Modify/Add Users or Batch Certificate Invites), a lot of emails are being sent to your email server within a small period of time. Make sure your email-server does not reject these!

This default e-mail template “Suspend Certificate” uses several “context variables”:

\$user.e-mail

\$user.firstName

\$request.productName

#certificate_value()

#mail_footer_en()

These variables are required to access context information within the e-mail.

The directives “#certificate_value()”, “#mail_footer_en()” and “#mail_footer_de()” cannot be changed. Instead they must be replaced by custom text and Context Variables.

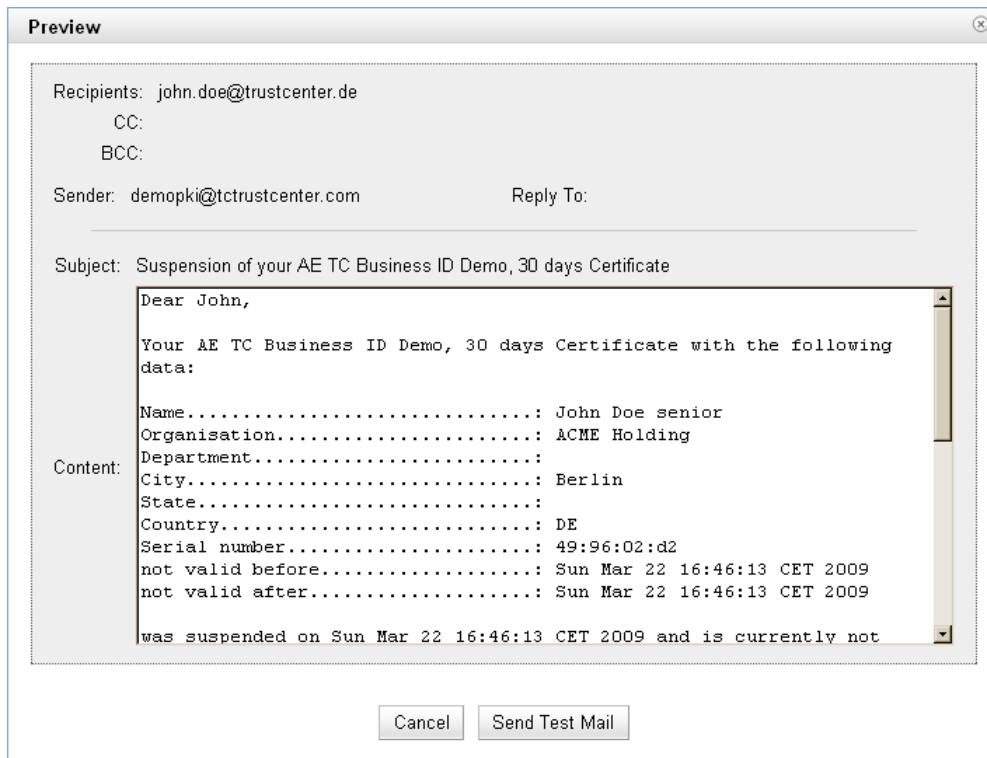


Figure 50 Preview of Sample E-Mail-Template

In the preview all context variables have been replaced by their actual value (based on the current User and some random data).

7.10.4 E-Mail Automation

In most cases the customization methods described in the previous sections should be sufficient. However, if you want to use more advanced feature, you should read this section.

The script language being used is based on Apache Velocity, it supports:

variables, starting with \$

so called directives, e.g. “#if (**condition**) <text1> #else<text2> #end.

The features can be used to conditionally include particular sections of a message.

```
Dear $user.firstName,

#if($admin)
TC $account.customerName has been successfully setup for you. As the
PKI Administrator please review the contact information (see PKI
Portal | Edit Settings). You can setup new users and invite them for
a certificate. If users request certificates you will have to approve
or cancel the request. Privileged users will be able to request
certificates without requiring an approval.
#else
```



```
A TC $account.customerName account has been setup for you. The TC
$account.customerName portal provides you with the ability to
request, revoke or suspend certificates or to update your personal
information.

#end

The TC $account.customerName portal can be accessed via the following
URL:

$idstore_url

Please use the following information to login at the portal and keep
the password confidential:

Username: $user.name
Password: $templateContextNewUserPassword

You can change the password at any time (see My Profile)

Kind regards,

#mail_footer_en()
```

Figure 51 Complex Sample E-Mail Template: New User

The e-mail template for new User notification shows the inclusion of conditional text. It uses the “if”-directive to include more text sections for “PKI Administrators”.

More general programming examples can be found at:

<http://velocity.apache.org/engine/releases/velocity-1.6/user-guide.html>.

Note: For security reasons only a small number of Velocity directives is supported ('#if #else #elseif #end', '#set' and '#foreach').

Since '#' and '\$' are being used for special purposes, the system will try to interpret these as variables or directives. Only if this interpretation fails will the original text appear.

As a consequence, in order to write '#' you can simply use '#' but in order to write existing statements like '#if' the string must be escaped with a backslash '\' to appear properly: \#if

This will be rendered as: “#if”.

There are two special cases.

The string '##' is used to start a single line comment. If you want '##' to appear after the directive

```
#set($l="##"+"##")
```

The variable '\$l' will be rendered as: “##”.

If you want '#' (beginning of a multi-line comment) or '*#' to appear, use the directives

```
#set($ls="#"+"*")
```

```
#set($s1="*"+"#")
```

After that the variables '\$ls' and '\$s1' will be rendered as: "#*" and "*#".

8 The TC ID Store API

TC ID Store provides a Simple Object Access Protocol (SOAP) API. External applications can programmatically use TC ID Store via this API. This section describes the required steps to make use of the API. It covers the configuration of TC ID Store as well as the configuration of the external application.

8.1 Preparations for using the API

Every external application has to authenticate itself using a certificate in order to access the API. The owner of this certificate is the so called apiUser.

Setting up the apiUser can be request by checking the related checkbox in the Administrator Authorization form. This form is available on the product web site.

In order to use the API a client authentication certificate has to be requested. Create a certificate invite for the product “TC Business ID, recoverable, 1yr” for the apiUser.

This certificate will be delivered to the Administrator as a *PKCS#12 PSE* via e-mail. The PIN required to access the *PKCS#12 PSE* will be sent as a separate e-mail. Once downloaded, the *PKCS#12* file should be renamed to “apiUser1.pfx”. The PIN used to download the *PKCS#12* file will also be required by the application to use the *PKCS#12*.

The certificate issued for apiUser1 can automatically be used as the authentication (or login) certificate.

8.2 Using the API in Custom Applications

The SOAP API can be used from custom applications in order to integrate with TC ID Store.

A sample client in Java and the API description can be provided upon request.

The WSDL specification can be retrieved from:

<https://my.trustcenter.de/IDStore/services/api-1.8/api?wsdl>

Most programming environments will automatically generate source code based on the WSDL file.

In some cases the API URL must manually be added. This URL can be found in the WSDL file in Tag „location“:

<https://my-cert.trustcenter.de/IDStore/services/api-1.8/api>

Note: It is important to pass the correct Account name in the SOAP message. The Account name can be found in Configuration | Settings | tab Account Settings | field Account Name in the web portal.

9 Glossary

| | |
|--------------------------|--|
| Administrator | “PKI Superadministrator”, “PKI Administrator” or any delegated role (“Registration Officer”, “Enrollment Officer”, “Unsuspending Officer”, “Revocation Officer”, “Key Recovery Officer”). |
| Application Certificates | <p>In the case of Application Certificates the Certificate Owner and the Certificate Holder 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> |
| Basic User | One of the possible roles for Users. |
| Batch Key Recovery | Performing the Key Recovery process in batch mode, i.e. for multiple Users simultaneously. |
| Certificate Holder | <p>This denotes the entity mentioned in the certificate.</p> <p>It can be a natural person (Client Certificate), a team or an application or a web server (<i>Application Certificate</i>).</p> |
| Certificate Owner | This is the person responsible for the certificate, i.e. <i>Certificate Holder</i> in case of Client Certificates and the server administrator in case of server and other <i>Application Certificates</i> . |
| Client Certificate | In the case of Client Certificates the <i>Certificate Holder</i> is also the <i>Certificate Owner</i> . TC Business ID is a typical example for Client Certificates. |
| Enrollment Officer | One of the possible delegated roles for Users. |
| ePIN | Electronic PIN. A PIN which is being delivered by E-Mail or SMS is denoted as ePIN. |
| External PIN | A PIN which is delivered by the <i>Administrator</i> to the User or to the web portal is denoted as <i>External PIN</i> . <i>External PINs</i> are administrated outside the system. |
| External User | One of the possible roles for Users. |

| | | |
|------------------------|--------|---|
| Key Recovery | | Recovery of the private key and the certificate for the User. |
| Key Recovery Officer | | One of the possible delegated roles for Users. |
| Key nonRepudiation | Usage | This key usage is used for document signing. It means that the User who signed the document cannot deny to know and to have signed the document at a later point in time. |
| NoLogin User | | One of the possible roles for Users. |
| PIN Administrator | Letter | One of the possible roles for Users. This role is responsible for printing 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 <i>PKCS#12 PSEs</i> . All other certificates will be requested using either web browser based key generation or copy&paste of a <i>PKCS#10</i> request. |
| 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 <i>PKCS#12 PSEs</i> . All other certificates will be requested using either web browser based key generation or copy&paste of a <i>PKCS#10</i> request. |
| PKI Administrator | | One of the possible roles for Users. The "PKI Administrator" can assign the following roles: "Revocation Officer", "Key Recovery Officer". |
| PKI Superadministrator | | One of the possible roles for Users. The "PKI Superadministrator" can assign the following roles: "PKI Administrator", "Registration Officer", "Enrollment Officer", "Unsuspendation Officer", "Revocation Officer" and "Key Recovery Officer". |
| Privileged User | | One of the possible roles for Users. |
| Registration Officer | | One of the possible delegated roles for Users. |

| | |
|----------------------|---|
| Revocation Officer | One of the possible delegated roles for Users. |
| SCEP | Simple Certificate Enrollment Protocol. See http://en.wikipedia.org/wiki/Simple_Certificate_Enrollment_Protocol for more details. |
| SCEP User | One of the possible roles for Users. 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. |
| 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. |

10 List of Figures

| | |
|---|----|
| Figure 1: Hierarchy of our Sample-Company | 5 |
| Figure 2 Verifying the Contract History | 6 |
| Figure 3 Contract Details and Status | 7 |
| Figure 4 Adding Groups | 7 |
| Figure 5 Add User | 8 |
| Figure 6 E-mail containing Login Credentials | 8 |
| Figure 7 Batch UploadInterface for Adding Users | 9 |
| Figure 8 Select Certificate Product | 10 |
| Figure 9 Select Certificate Owner | 11 |
| Figure 10 Confirmation of Certificate Data | 11 |
| Figure 11 Acknowledgement of Certificate Request | 12 |
| Figure 12 Request Notification | 12 |
| Figure 13 Certificate Request Approval | 12 |
| Figure 14 PIN E-Mail | 13 |
| Figure 15 Download Link E-Mail | 13 |
| Figure 16 PKCS#12 Download Web-Page | 14 |
| Figure 17 Certificate Invite for an External Partner | 15 |
| Figure 18 Select Certificate Owner | 15 |
| Figure 19 Complete Request Data for Certificate Invite | 16 |
| Figure 20 Certificate Invite Submitted | 16 |
| Figure 21 Certificate Invite E-mail | 17 |
| Figure 22 Login for Key Generation | 17 |
| Figure 23 Key Generation with Firefox | 18 |
| Figure 24 Key Generation with Internet Explorer | 18 |
| Figure 25 Certificate Data Confirmation | 19 |
| Figure 26 Request Completed | 19 |
| Figure 27 E-Mail containing Certificate Installation Link | 20 |
| Figure 28 Certificate Installation Page | 21 |
| Figure 29 Server Certificate Product List | 22 |
| Figure 30 PKCS#10 Upload | 22 |
| Figure 31 Certificate Data Confirmation | 23 |
| Figure 32 Acknowledgement of Certificate Request | 23 |
| Figure 33 Approval of Server Certificate Request | 23 |
| Figure 34 – Edit Product Configuration | 25 |
| Figure 35 – Creating “Enrollment URL (SCEP)” | 25 |
| Figure 36 – SCEP Enrollment page | 29 |
| Figure 37 – SCEP Profile Overview | 29 |
| Figure 38 – Install Profile | 30 |
| Figure 39 – Profile installation | 30 |
| Figure 40 – Installed Profile | 31 |
| Figure 41 – VPN disabled | 31 |
| Figure 42 – VPN enabled | 32 |

| | |
|---|----|
| Figure 43 – Personalization Requests _____ | 34 |
| Figure 44 – TC PersoClient _____ | 34 |
| Figure 45 – PIN Letter Printing Requests _____ | 35 |
| Figure 46 Defining a Key Generation Policy _____ | 39 |
| Figure 47 ePIN (SMS) Activation _____ | 41 |
| Figure 48 List of Different E-Mail Templates _____ | 43 |
| Figure 49: Sample E-Mail-Template (Suspend Certificate) _____ | 44 |
| Figure 50 Preview of Sample E-Mail-Template _____ | 45 |
| Figure 51 Complex Sample E-Mail Template: New User _____ | 46 |