

TC TrustCenter

TC Replication Client Administrator Manual

TC Replication Client
Version 3.2d

Hamburg, Germany
September 2010

Geschäftsführung
Dr. Sabine Kockskämper
Robert Steinkrauss

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

Bankverbindung
Commerzbank AG
BLZ 200 400 00
Kto.-Nr. 619 37 00 00
IBAN DE43 2004 0000 0619 3700 00
BIC COBADEFFXXX



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 © 2009 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 © 2009 TC TrustCenter GmbH
All rights reserved.



Table of Contents

| | |
|--|-----------|
| TC Replication Client Administrator Manual | 4 |
| 1 Introduction | 4 |
| 2 Installation Preparation | 4 |
| 3 TC Replication Client Installation | 4 |
| 3.1 Software Installation | 4 |
| 3.2 Configuring and Starting the TC Replication Client | 7 |
| 4 Configuration Reference | 10 |
| 4.1 log4j.properties | 10 |
| 4.2 jndi.properties | 10 |
| 4.3 ReplicationClientConfig.xml | 12 |
| 4.3.1 Core Configuration Settings | 12 |
| 4.3.2 Configuration of CRL Replication into Active Directory | 14 |
| 4.3.2.1 Active Directory Preparation for CRL Publication | 14 |
| 4.3.2.2 Configuring CRL Replication in ReplicationClientConfig.xml | 18 |
| 4.3.3 Configuring TC Replication Client to use a Web Proxy | 19 |
| 4.4 Certificate Replication Policy (plugin_ad.bsh) | 19 |
| 5 Installation Checklist | 22 |
| 6 Frequently Asked Questions | 23 |
| 6.1 Illegal key size | 23 |
| 6.2 Service does not start | 23 |
| 7 List of Figures | 25 |

TC Replication Client Administrator Manual

1 Introduction

The TC Replication Client publishes certificates and/or CRLs into a target LDAP. It is compatible with TC ID Store, TC Enterprise ID QuickStart, and TC Enterprise ID. It is configured to publish the most recent valid certificate per user, it will overwrite older valid certificates as well as certificates that have been revoked, and thus there will be no more than one valid certificate per user in the target LDAP.

A more detailed description of this behaviour can be found in section 4.4.

2 Installation Preparation

TC Replication Client requires a working Microsoft Active Directory Server, no older than 2003, as the target LDAP. It can be installed on Windows Server 2003 or Windows Server 2008.

Additionally the following software modules must be installed:

- Microsoft .Net Framework 3.5
- Java Runtime 1.6 or newer.
- The “Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6” are required (view the readme.txt file of the JCE). They can be downloaded from the Sun Website: <http://java.sun.com/javase/downloads/index.jsp>

TC Replication Client uses HTTPs with SSL client authentication to access the TC ID Store, TC EID QuickStart or TC Enterprise ID API.

- A working TC ID Store, TC EID QuickStart or TC EnterpriseID account is required. An “apiUser” must exist (See section 6.1 of the TC ID Store, TC EID QuickStart or TC EnterpriseID Administrator Manual)
- The *PKCS#12 PSE* file used for authenticating the TC Replication Client to the API must be available together with the associated PIN. See section 6.1 of the TC ID Store, TC EID QuickStart or TC EnterpriseID Administrator Manual.
- TC Replication Client publishes certificates and CRLs to an LDAP target. A username and password with appropriate LDAP publication permission is required (“LDAP Publication User”).

3 TC Replication Client Installation

If the installation has been prepared according to section 2, the TC Replication Client can be installed.

3.1 Software Installation

TC Replication Client is shipped as a MSI package and a separate license file. It can be installed on any Windows server connected to the targeted Windows domain.

Login to the appropriate Windows server with Administrator privileges and start the installation by double-clicking the .MSI file.

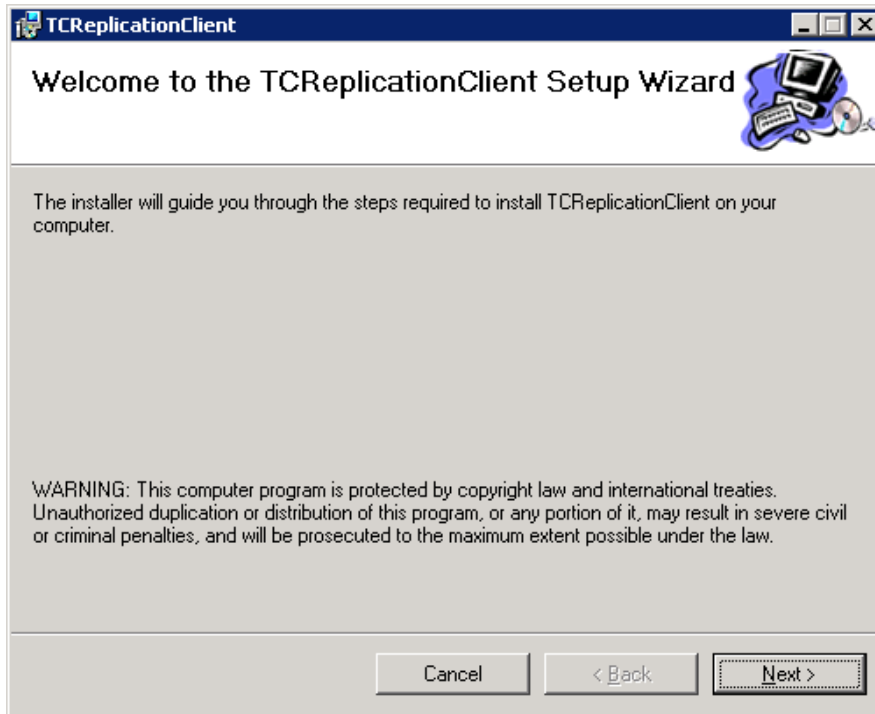


Figure 1: TC Replication Client – Start Installation

Please read and accept the license agreement displayed on the second screen.

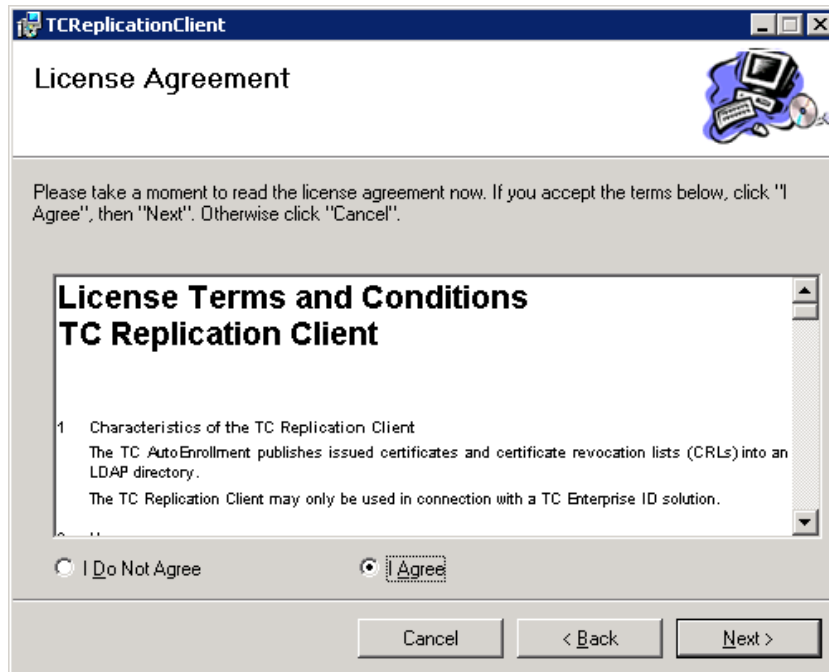


Figure 2: TC Replication Client – Accept Software License

Select “SOAP” as protocol for TC ID Store, TC Enterprise ID QuickStart and TC Enterprise ID 2009.

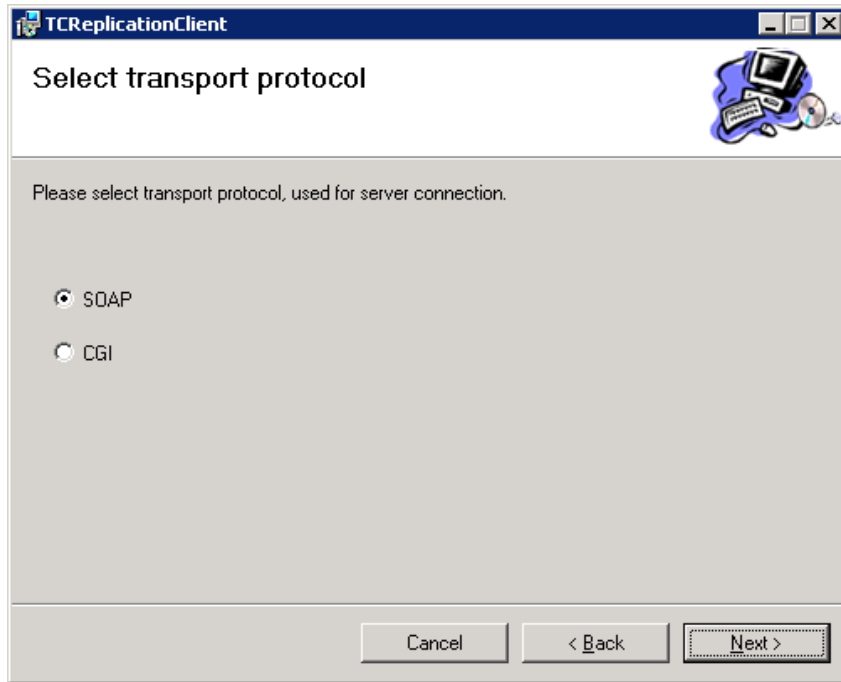


Figure 3: TC Replication Client – Select Protocol

Select the installation folder.

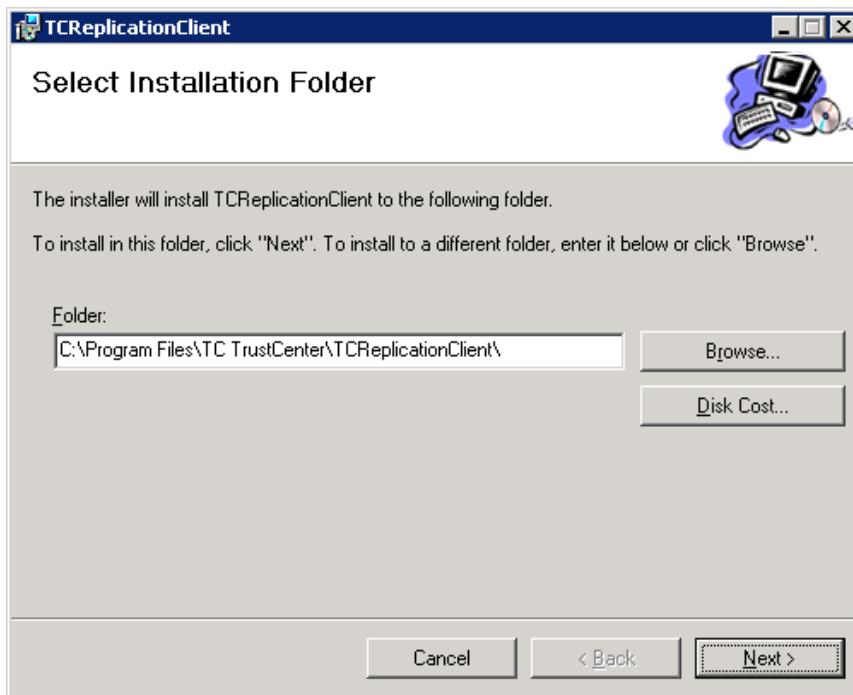


Figure 4: TC Replication Client – Select Installation Folder

Click next to start the copying of the application files.

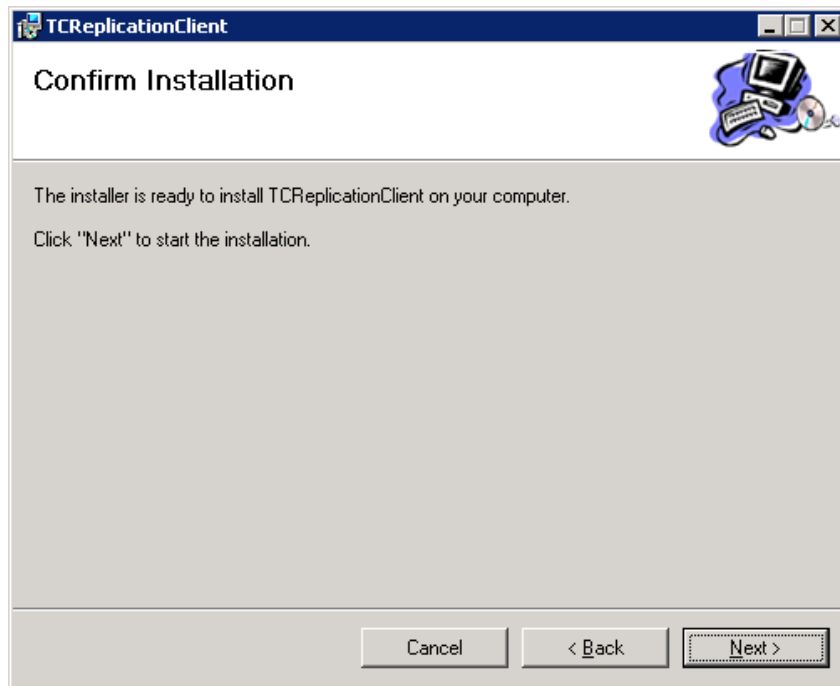


Figure 5: Start Copying Program Files

The TC Replication Client will be added to the Windows services. You must configure the software before starting the service.

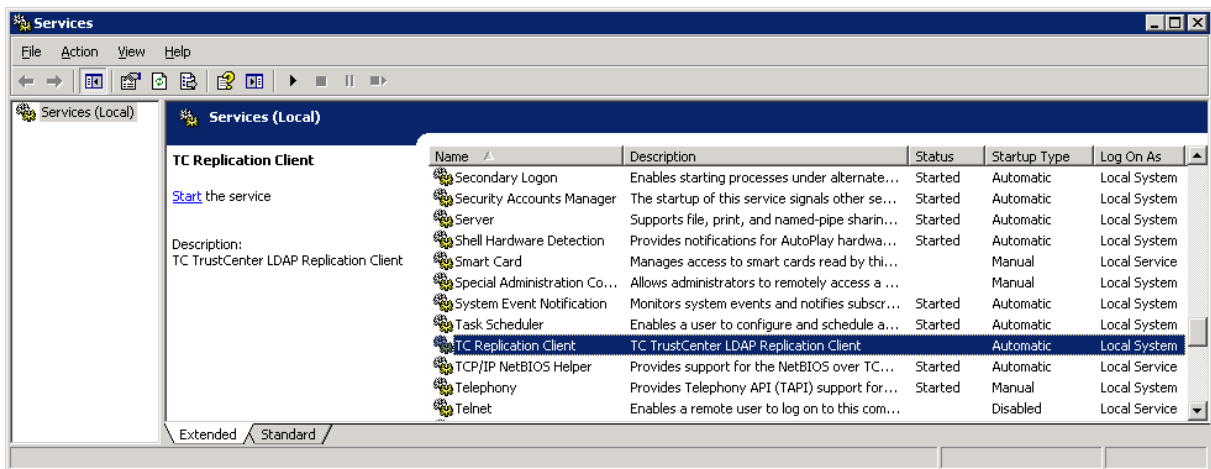


Figure 6: Service Installed but not Started

3.2 Configuring and Starting the TC Replication Client

Please follow these steps:

1. Rename the *PKCS#12 PSE* received for apiUser1 (see TC ID Store, TC EID QuickStart or TC Enterprise ID Administrator Manual section 6.1 for how to get this *PKCS#12 PSE*) to "apiUser1.p12" and copy it to the folder "certs" of TC Replication Client.

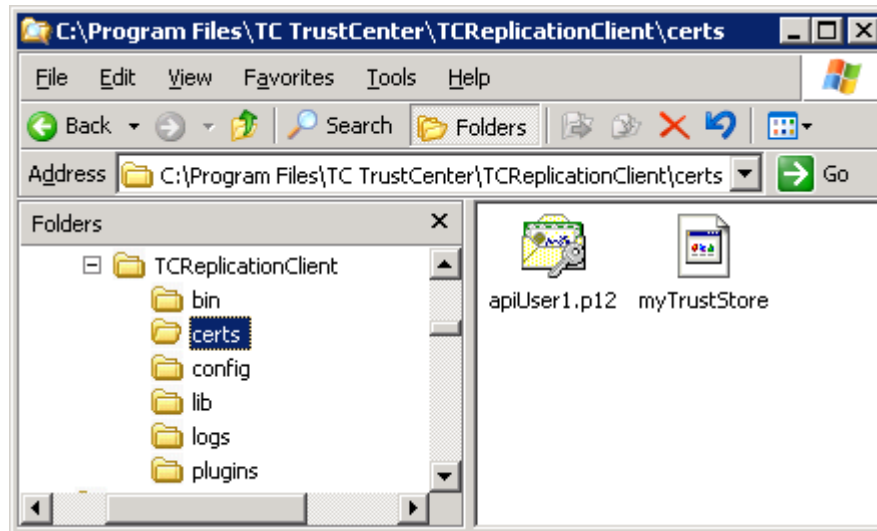


Figure 7: Copy apiUser's PKCS#12 PSE

2. Open a command tool (cmd.exe) and change to folder "bin" of the TC Replication Client. Enter the required passwords/PINs using the following commands:
 - a. `password.cmd -passwordname KeyStore`
(Enter the PIN for the *PKCS#12 PSE* when being prompted to enter the password).
 - b. `password.cmd -passwordname LDAP`
(Enter the password for the "LDAP Publication User" when being prompted to enter the password).
 - c. `password.cmd -passwordname TrustStore`
(Enter the password for the "TrustStore", default value is ("changeit") when being prompted to enter the password).

Note: The passwords will be stored encrypted in the configuration files.

3. Copy the license file into the folder "bin".
4. Open folder "config" of the TC Replication Client.

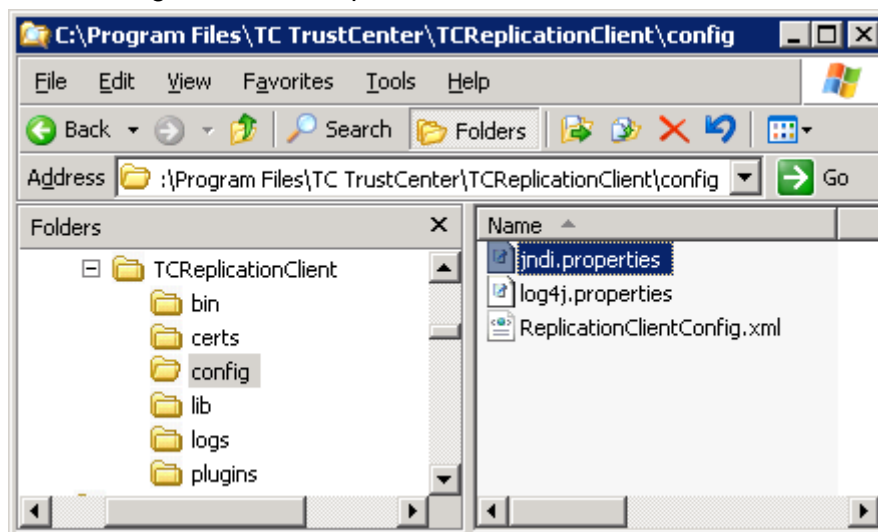


Figure 8: Changing to Folder "config"

Open file `jndi.properties` using a text editor (e.g. notepad) and specify the following parameters

- Servername of the LDAP server in entry “java.naming.provider.url”
 - Name of the “LDAP Publication User“ in entry “java.naming.security.principal”.
4. Open file “ReplicationClientConfig.xml” using a text editor, e.g. notepad and specify the following parameters:
- TC ID Store, TC EID QuickStart or TC Enterprise ID account name in entry “soap_api_accountname”.

Note: It is important to specify the correct account name in the configuration field. The account name can be found in “Configuration | Settings | tab Account Settings | field Account Name” in the web portal.

Account Name *: TC TrustCenter
Description:
Product Name: EnterpriseID QuickStart

Figure 9: Finding the “Account Name” in the GUI

5. Start the service using the Windows „Services“ console.

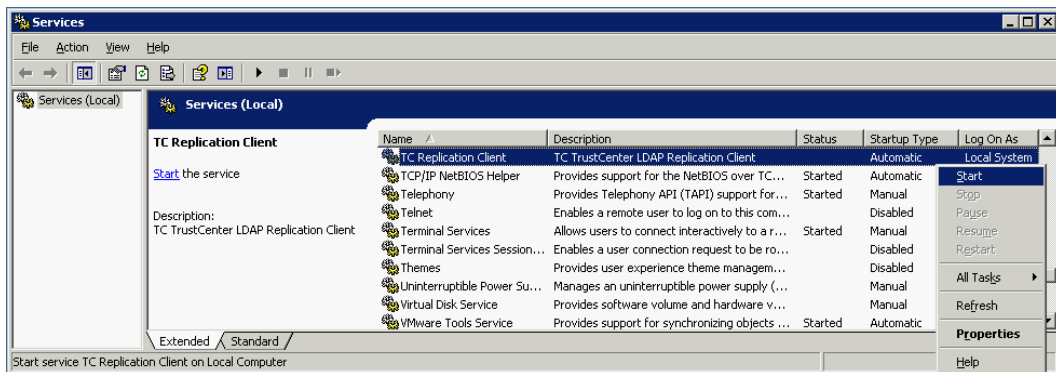


Figure 10: Starting the TC Replication Client Service

Check the service status using the following log files:

- logs/wrapper.log and
- logs/replication_client.log

4 Configuration Reference

TC Replication Client uses 3 configuration files. These configuration files are located in the “config” folder:

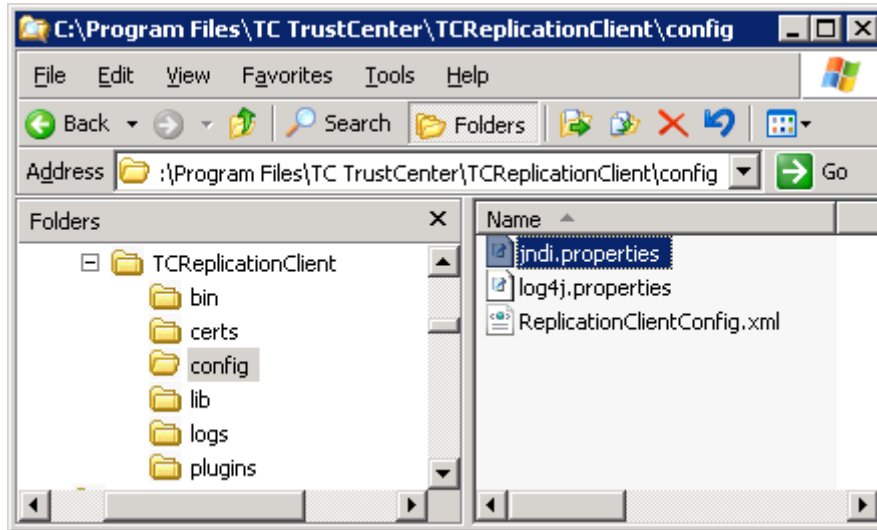


Figure 11: Configuration Files of TC Replication Client

The configurations files and their configuration parameters are described in the following sections.

4.1 log4j.properties

This configuration file defines the log level. The overall log level is defined by the following parameter:

```
log4j.logger.de.trustcenter.replclient = DEBUG
```

The log levels “ERROR”, “INFO”, and “DEBUG” are available. The “INFO” level includes all messages required for auditing purposes. The entry above is not include in the log4j.properties file you received.

The log level can be overwritten on a class level. To enable the “DEBUG” log level for a particular class, please use:

```
log4j.logger.de.trustcenter.replclient.<class> = DEBUG
```

| Supported Classes | Debug Information |
|---------------------------|---|
| ReplicationListProvider | Request-Lists as provided by the backend |
| LDAPReplicator | LDAP-modifications performed by the plugins; Debug-messages from the plugin itself |
| ReplicationClientLauncher | Configuration file parsing |

Table 1: Defining the Log Level by Classes

4.2 jndi.properties

This configuration file contains the entries relevant for LDAP / Active Directory access.

```

# Please insert the name of your Active Directory Server.
#java.naming.provider.url=ldap://servername.local:389
java.naming.provider.url=

# Please specify the LDAP user name
# Please ensure that this user has the rights to publish
# and delete certificates and CRLs, e.g.
#java.naming.security.principal= cn=LDAP Admin,cn=Users,dc=local
java.naming.security.principal=

# Please do not specify the Password of the user above in the clear.
# Use the password.cmd tool instead.
# >Password.cmd -passwordname LDAP
# Therefore please do not change the lines below
#-----
java.naming.security.credentials=
java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory
java.naming.security.authentication=simple
  
```

Figure 12: Default jndi.properties Configuration File

| Parametername | Needs to be changed on installation | Comment |
|-------------------------------------|-------------------------------------|--|
| java.naming.provider.url | Yes | Name of the LDAP server, e.g. ldap://adsservername.local:389 |
| java.naming.security.principal | Yes | Name of the “LDAP Publication User“, i.e. the user used to publish or delete certificates and CRLs. To retrieve the required value, use mmc include Snap-In ADSI Edit Connect to Domain and goto Users. Then open the “LDAP Publication Users“-Properties and click on the entry “distinguishedName“. You can copy the entry into the jndi.properties file. |
| java.naming.security.credentials | Yes | Encrypted password of “LDAP Publication User“. Use password.cmd -passwordname LDAP to set this entry. |
| java.naming.security.authentication | No | Do not change |
| java.naming.factory.initial | No | Do not change |

Table 2 Description of the jndi.properties Configuration Parameters

4.3 ReplicationClientConfig.xml

ReplicationClientConfig.xml contains the general configuration settings of the TC Replication Client. By default CRL replication is disabled since the CRL distribution point included in certificates by default points to a central TC TrustCenter location. CRL replication is only required if the certificates include a custom CRL distribution point.

4.3.1 Core Configuration Settings

The core settings include settings relevant for SSL client authentication. The default configuration is as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<ReplicationClientConfig>
  <de>
    <trustcenter>
      <replclient>
        <url>https://replication.trustcenter.de/rep-sbin/ReqListProvider.cgi</url>
        <itemsPerCall>10</itemsPerCall>
        <counterFile>../logs/last_item_id.properties</counterFile>
        <pluginFile>../plugins/plugin_ad.bsh</pluginFile>
        <execInterval>43200</execInterval>
        <provider>SOAP</provider>
        <soap_api_servername>my-cert.trustcenter.de</soap_api_servername>
        <soap_api_serverport>443</soap_api_serverport>

<!-- It is important to specify the correct Account name here.
The Account name can be found in Configuration | Settings | tab Account
Settings | field Account Name in the web portal.
-->
        <soap_api_accountname></soap_api_accountname>
      </replclient>
    </trustcenter>
  </de>
  <system>
    <javax>
      <net>
        <ssl>
          <keyStore>../certs/apiUser1.p12</keyStore>

<!-- Please do not specify the password manually. Use the command tool Password.cmd
instead.
>Password.cmd -passwordname KeyStore
-->
          <keyStorePassword></keyStorePassword>
          <keyStoreType>pkcs12</keyStoreType>
          <trustStore>../certs/myTrustStore</trustStore>

<!-- Please change and insert the Standard Password (changeit) of
the myTrustStore file with the command tool Password.cmd
>Password.cmd -passwordname TrustStore
-->
          <trustStorePassword></trustStorePassword>
        </ssl>
      </net>
    </javax>
  </system>
</ReplicationClientConfig>
```

Figure 13: Default ReplicationClientConfig.xml Configuration File



| Parent Node | Element Name | Needs to be changed on installation | Comment |
|-------------------------------|----------------------|-------------------------------------|---|
| de / trustcenter / replclient | url | No | ReplicationListProviders URL. This entry is only required if the „CGI“ protocol has been selected. Please leave this entry unchanged. |
| | itemsPerCall | No | Maximum number of items to be transmitted per call via the API. |
| | counterFile | No | Name of the file to persistently store the last transactionID. |
| | pluginFile | No | Path and name of the Bean Shell script to be used. This script is specific to the target LDAP. |
| | execInterval | No | Number of seconds between two attempts to read replication item via the API. |
| | provider | No | Name of the API protocol, must be „SOAP“. |
| | soap_api_servername | No | Name of SOAP API server. Should be “my-cert.trustcenter.de”. |
| | soap_api_serverport | No | Port of the SOAP API. Should be 443. |
| | soap_api_accountname | Yes | TC ID Store, TC EID QuickStart or TC Enterprise ID account name. The account name can be found in “Configuration Settings tab Account Settings field Account Name” in the web portal. |
| | keyStore | No | Name and path of the PKCS#12 PSE used for SSL client authentication to the API. |
| | keyStorePassword | Yes | Encrypted password required to access the private key contained in the PKCS#12 PSE specified in keyStore. Do not manually specify a password here! Use password.cmd -passwordname KeyStore to change this entry. |
| | keyStoreType | No | Type of keyStore. Must be „pkcs12“ |
| system / javax / net / ssl | trustStore | No | Name and path of the trusted root certificates used for the SSL connection to the API. This so called trustStore must contain the TC TrustCenter Class 3 Root certificates. |

| | | | |
|--|--------------------|----|--|
| | trustStorePassword | No | <p>Encrypted password used to protect the trustStore.</p> <p>Do not manually specify a password here!</p> <p>Use</p> <pre>password.cmd -passwordname TrustStore</pre> <p>to change this entry.</p> |
|--|--------------------|----|--|

Table 3: Description of the ReplicationClientConfig.xml Configuration Parameters

4.3.2 Configuration of CRL Replication into Active Directory

Microsoft Active Directory is capable of storing CRLs.

When using smart card logon the domain controller has to validate all smart card logon certificates either using a CRL or using OCSP. Sometimes domain controllers don't have permission to open a connection to the internet for downloading the CRL. In this case CRL replication is a solution.

Before publishing CRLs to the Active Directory some initial preparation steps have to be performed.

Note: As the CRL distribution point contained in a certificate is being used to determine the CRL storage location there is no need to store CRLs in Active Directory unless the certificates include a custom CRL distribution point.

4.3.2.1 Active Directory Preparation for CRL Publication

To create the container objects and "crldistributionpoint" objects in the ADS start the "ADSI Edit" Snap-In for the MMC and activate the Connection Point "Configuration". Open "Services | Public Key Services | CDP" and create a new container with your server name in the location labeled "Value":

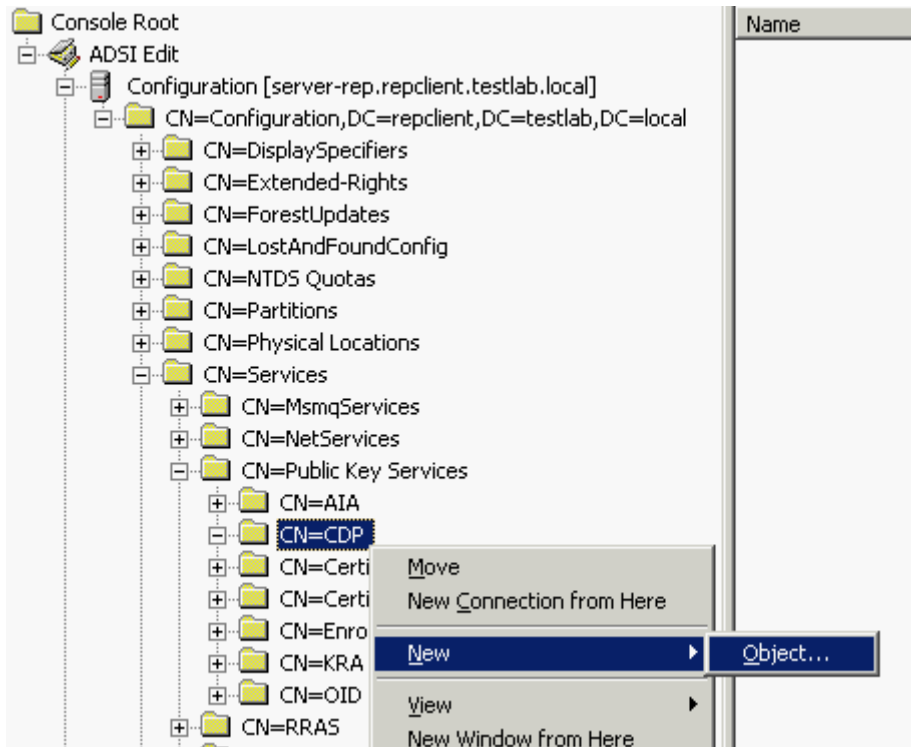


Figure 14: Create New Object

Select class “Container”, and click “Next”.

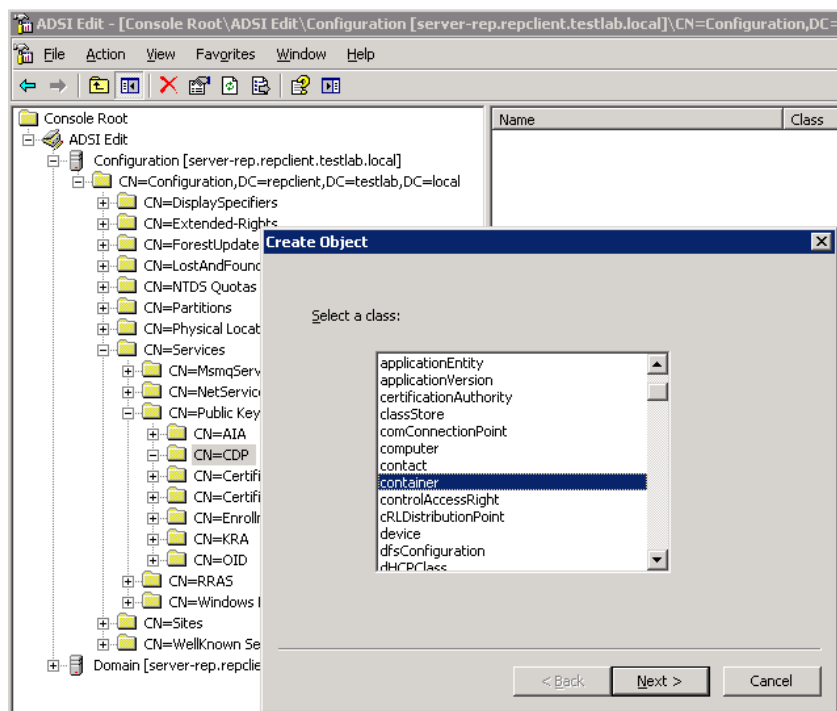


Figure 15: Selecting Class “Container” for the new Object

Specify the name of the Active Directory server as “Value”, and click “Next”.

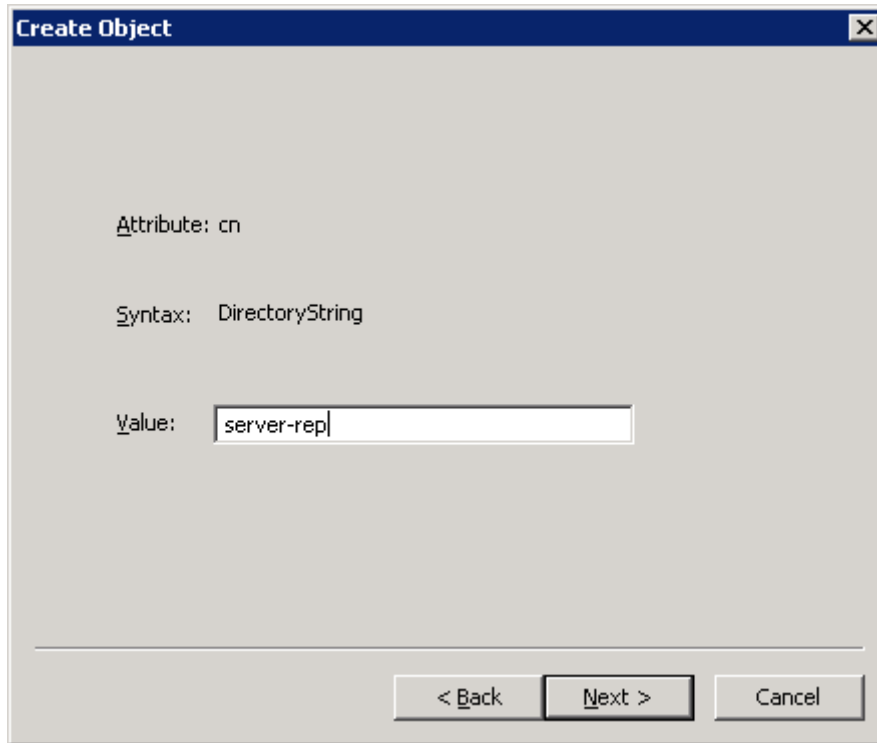


Figure 16: Specifying the Server Name for the new Object

Complete this dialog. Select the new container and create a new "crlDistributionPoint" object for each CRL to be published into the Active Directory (as shown below for the CRL of the TC TrustCenter Class 1 CA).

The LDAP Admin user need write permissions on this container to publish the CRL (right click on the container | Security tab).

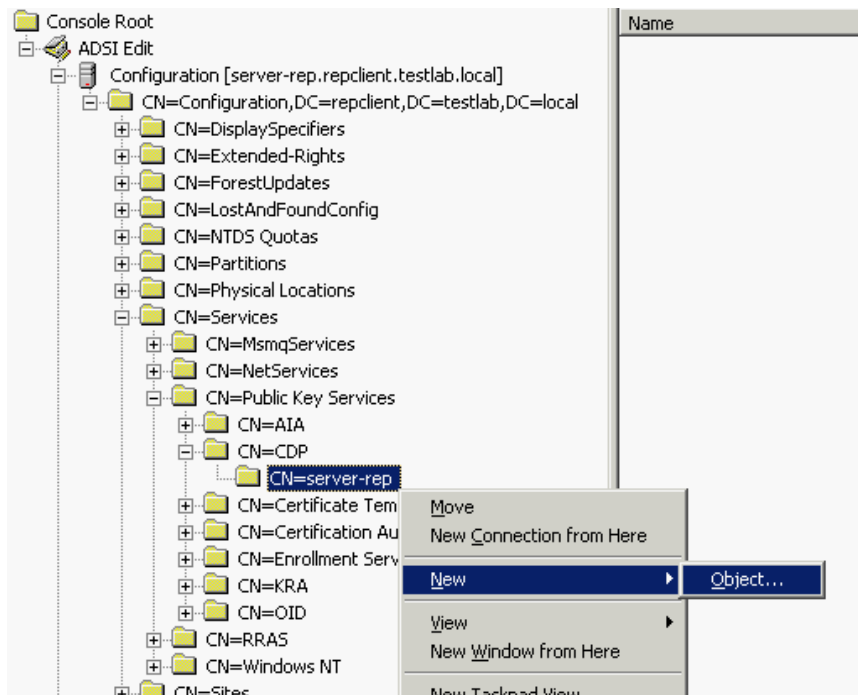


Figure 17: Creating a new Object in the Server Container

Select class "cRLDistributionPoint" for this new object and click "Next".

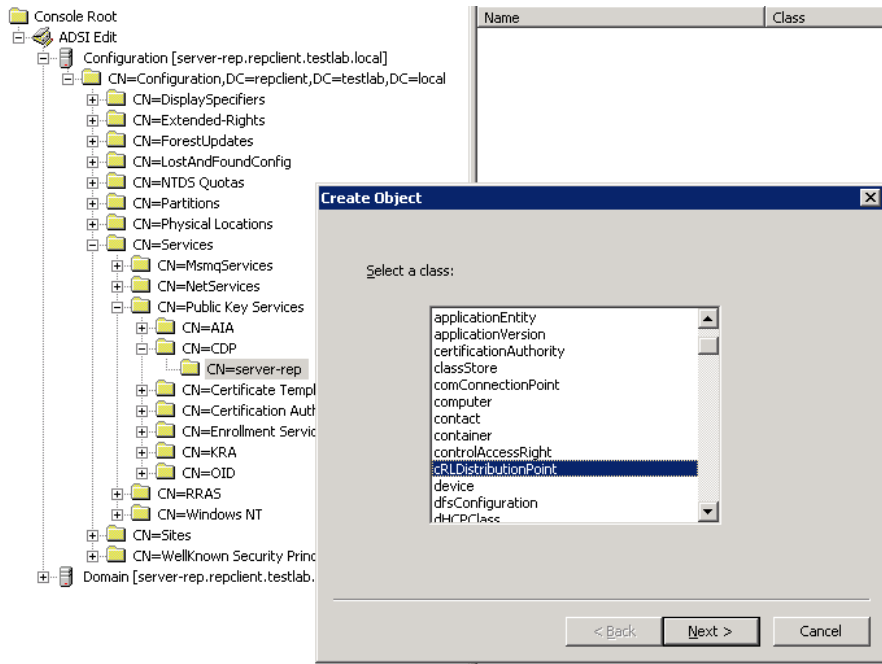


Figure 18: Selecting Class “Container” for the new “cRLDistributionPoint” Object

Specify the CRL issuer’s common name in the location labeled “Value“, and click “Next“.

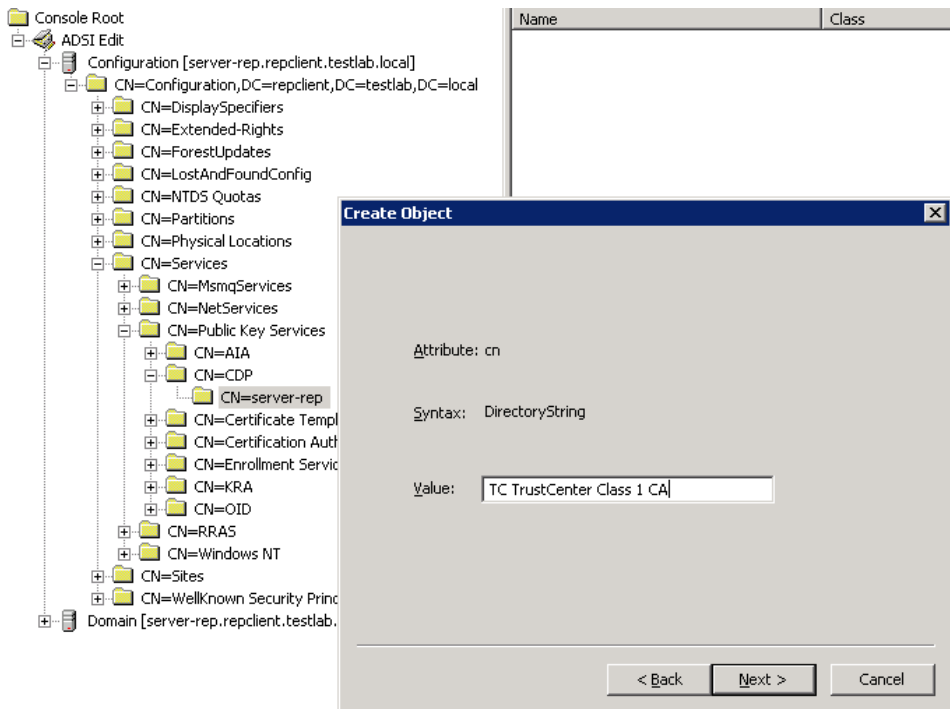


Figure 19: Specifying the CRL Issuer’s Common Name as “Value“

No other attributes are required, click “finish“.

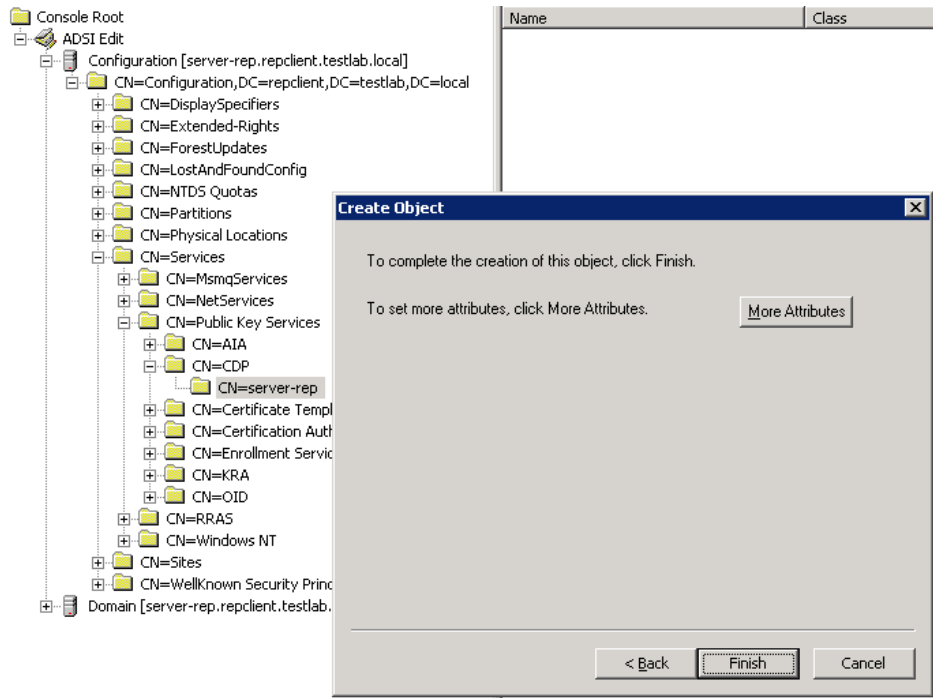


Figure 20: Confirm Creation of “cRLDistributionPoint”

The new “cRLDistributionPoint” object is now shown. Repeat these steps for each additional CRL to be replicated.

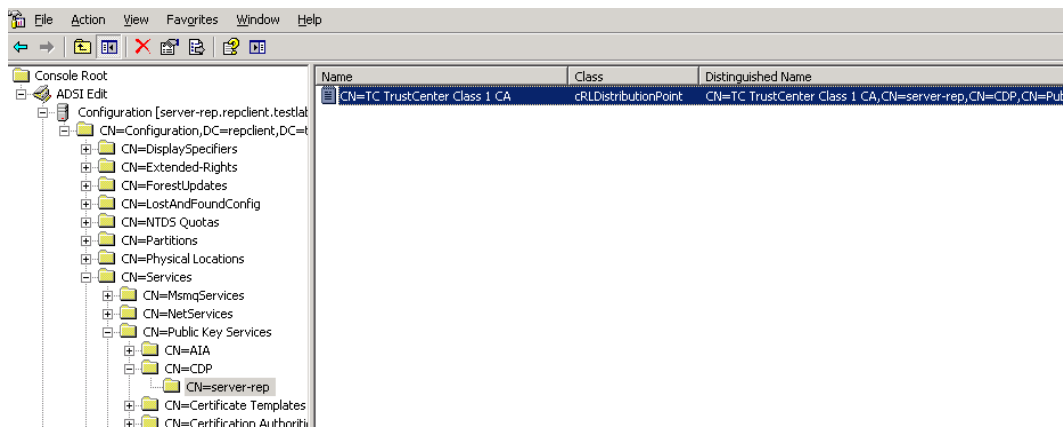


Figure 21: New “crIDistributionPoint“

4.3.2.2 Configuring CRL Replication in ReplicationClientConfig.xml

In order to download the CRLs to be replicated the new node “crls” must be inserted in ReplicationClientConfig.xml between <execInterval> and <provider>.

The following example shows the “crls” node for 2 CRLs:

- TC TrustCenter Class 1 CA and
- TC TrustCenter Class 1 L1 CA VI

```

<execInterval>43200</execInterval>
<crls>
  <serialNumberFile>../logs/last_serial_numbers.properties</serialNumberFile>
  <crl>
    <issuer>EMAILADDRESS=certificate@trustcenter.de, OU=TC TrustCenter Class 1 CA,
O=TC TrustCenter for Security in Data Networks GmbH, L=Hamburg, ST=Hamburg, C=DE</issuer>
    <dn>CN=TC TrustCenter Class 1 CA,CN=server-
rep,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=local</dn>
  </crl>

```

```

    <cr1>
      <issuer>CN=TC TrustCenter Class 1 L1 CA VI,          OU=TC TrustCenter Class 1 L1 CA,
O=TC TrustCenter GmbH, C=DE</issuer>
      <dn>CN=TC TrustCenter Class 1 L1 CA VI,CN=server-
rep,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=local</dn>
    </cr1>
  </cr1s>
  <provider>SOAP</provider>

```

Figure 22: Sample “cr1s” Node

The meaning of the parameters is as follows:

| Parent Node | Element Name | Needs to be changed on installation | Comment |
|--|------------------|-------------------------------------|--|
| de / trustcenter / replclient / cr1s | serialNumberFile | yes | Contains the cr1Serial number of the current CRL. File will be created if it doesn't already exist. |
| | cr1 (List) | yes | One or more CRL entries, as described in “de / trustcenter / replclient / cr1s / cr1” |
| de / trustcenter / replclient / cr1s / cr1 | issuer | yes | Issuer-DN of the CRL in Java-Format e.g EMAILADDRESS=certificate@trustcenter.de, OU=TC TrustCenter Class 1 CA, O=TC TrustCenter for Security in Data Networks GmbH, L=Hamburg, ST=Hamburg, C=DE (take a look inside the cr1s you need http://cr1.trustcenter.de/cr1/) |
| | dn | yes | Target location of CRL in LDAP e.g. CN=TC TrustCenter Class 1 CA,CN=server-rep,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration, DC=replclient,DC=testlab,DC=local Note: Base-DN will be appended automatically (see variable java.naming.provider.url in jndi.properties) |

Table 4: Description of the <cr1s> Node

You have to stop and restart the TC Replication Client service in order to apply the changes.

Note: If only CRLs should be replicated (and not certificates), edit the file config/plugin_ad.bsh. Modify the method getCertificateDN only return null in every case – remove all other lines in the body.

4.3.3 Configuring TC Replication Client to use a Web Proxy

TC Replication Client can be configured to use a Web Proxy instead of directly connecting to the internet. Add the following parameters at the bottom of the ReplicationClientConfig.xml file.

```

...
    </ssl>
  </net>

```

```

</javax>
<https>
  <proxyHost>gate.servername.com</proxyHost>
  <proxyPort>80</proxyPort>
</https>
</system>
</ReplicationClientConfig>

```

Figure 23: Sample Configuration of a Web Proxy

| Parent Node | Element Name | Needs to be changed on installation | Comment |
|---------------------------------------|--------------|-------------------------------------|--|
| de / trustcenter / replclient / https | proxyHost | yes | Name of the web proxy |
| | proxyPort | yes | Web proxy port to be used for https connections. |

Table 5: Configuring TC Replication Client to use a Web Proxy

4.4 Certificate Replication Policy (plugin_ad.bsh)

In the standard configuration, the TC Replication Client searches the user in the LDAP as follows:

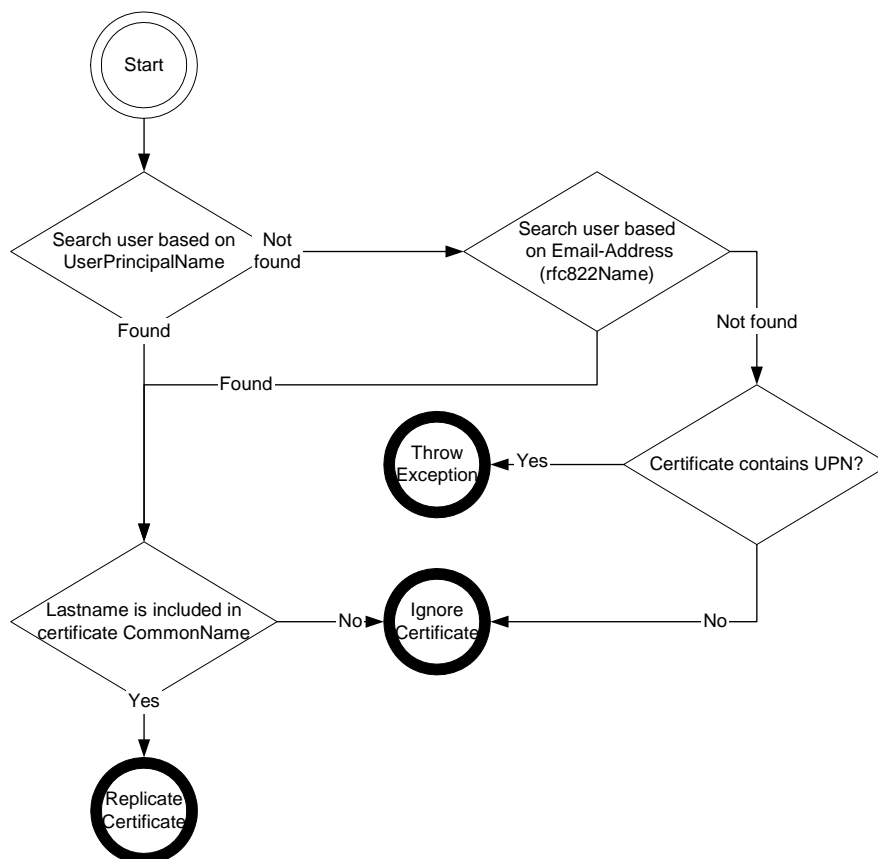


Figure 24: CertificateReplication Policy

If not all certificates suitable for smart card logon should be replicated, the replication policy must be modified.

To modify the replication policy you have to edit the file “config/plugin_ad.bsh”.

In order to ignore certificates which cannot be replicated, the following lines in method getCertificateDN:

```

if ( upn != null )
  throw new NameNotFoundException(message); //must find user if UPN is present in certificate!

```



must be removed.

Note: You should keep a copy of the original file.

Certificates are being replicated using method `updateUserCert(attrs, item)` in “config/plugin_ad.bsh”. This method replaces existing certificates. As a consequence only one certificate per user is available in the LDAP.

Certificates which have already been replicated will be removed from the LDAP once they have been revoked (method `deleteUserCert(attrs, item)` in “config/plugin_ad.bsh”).



5 Installation Checklist

| | |
|--|---|
| | Installation Preparation (see section 2) |
| | Windows Server 2003 or newer |
| | Add User apiUser1 and request SSL authentication certificate for apiUser1 (see section 2) |
| | Setup "LDAP publication" user with permission to publish CRLs and to publish and delete certificates (see section 2). |
| | |
| | TC TrustCenter Components |
| | TC Replication Client Installation (see section 3.1) |
| | TC Replication Client Start (see section 3.2) |
| | If applicable: Setup CRL Replication (see section 4.3.2) |
| | If applicable: Configure Web Proxy to be used (see section 4.3.3) |



6 Frequently Asked Questions

6.1 *Illegal key size*

Error message

When changing the password with the password.cmd tool the following error message appears:

```
>Illegal key size
```

Solution

The "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6" is not present. Please download this Extension from the SUN Website <http://java.sun.com/javase/downloads/index.jsp>. It is required to install it. (Please refer to section 2)

6.2 *Service does not start*

Error message

The TC Replication Client service does not start and the wrapper log-file shows a License Error:

```
A valid license was not found in the Wrapper configuration file.
```

Solution

You need to copy the license file into the "bin" folder (see section 3.2).



Glossary

Administrator

“PKI Superadministrator”, “PKI Administrator” or any delegated role (“Registration Officer”, “Enrollment Officer”, “Unsuspending Officer”, “Revocation Officer”, “Key Recovery Officer”).

LDAP Publication User

User with permission to publish CRLs and to publish or delete certificates into the LDAP.

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.



7 List of Figures

| | |
|--|---|
| Figure 1: TC Replication Client – Start Installation | 5 |
| Figure 2: TC Replication Client – Accept Software License | 5 |
| Figure 3: TC Replication Client – Select Installation Folder | Fehler! Textmarke nicht definiert. |
| Figure 4: TC Replication Client – Select Protocol | 6 |
| Figure 5: Start Copying Program Files | 7 |
| Figure 6: Service Installed but not Started | 7 |
| Figure 7: Copy apiUser’s PKCS#12 PSE | 8 |
| Figure 8: Changing to Folder “config“ | 8 |
| Figure 9: Finding the “Account Name” in the GUI | 9 |
| Figure 10: Starting the TC Replication Client Service | 9 |
| Figure 11: Configuration Files of TC Replication Client | 10 |
| Figure 12: Default jndi.properties Configuration File | 11 |
| Figure 13: Default ReplicationClientConfig.xml Configuration File | 12 |
| Figure 14: Create New Object | 15 |
| Figure 15: Selecting Class “Container“ for the new Object | 15 |
| Figure 16: Specifying the Server Name for the new Object | 16 |
| Figure 17: Creating a new Object in the Server Container | 16 |
| Figure 18: Selecting Class “Container“ for the new “cRLDistributionPoint” Object | 17 |
| Figure 19: Specifying the CRL Issuer’s Common Name as “Value“ | 17 |
| Figure 20: Confirm Creation of “cRLDistributionPoint” | 18 |
| Figure 21: New “crlDistributionPoint“ | 18 |
| Figure 22: Sample “crls“ Node | 19 |
| Figure 23: Sample Configuration of a Web Proxy | 19 |
| Figure 24: CertificateReplication Policy | 19 |