We change the shape of the world

Installation / Configuration Manual

TLS and sRTP

Version 3.4.1 of December 16th 2010

Subject to change without notice

We change the shape of the world

Table of contents

Changes

30.07.2010 – New flag “CUCM trunk” see chapter 4.1.

Introduction

Important:
After the activation of TLS the non-protected access to the machines on site is blocked. Any access via V24/USB, ISDN and IP such as HTTP and TELNET will be rejected

How to enable and configure an S3 to establish secured and encrypted SIP/sRTP connections to a CUCM

- Please study chapter 4, if you want to configure a S6. Then proceed here.

- To disable TLS and sRTP for a S3 or S6 continue at chapter 5.

- Version 3.3 contains in chapter 6

    1. Cisco CTL Client Installation, Secure token addition and Secure configuration,

    2. Instructions for CUCM certificates download for S3 addition, and

    3. Instructions to add S3 certifications to the CUCM.

- Version 3.4

Notice: After the TLS-Licence has been loaded and SIP is configured, now some settings will be created automatically. In the past these settings have to be made manually. Please, check these settings (refer to chapter 2.1).

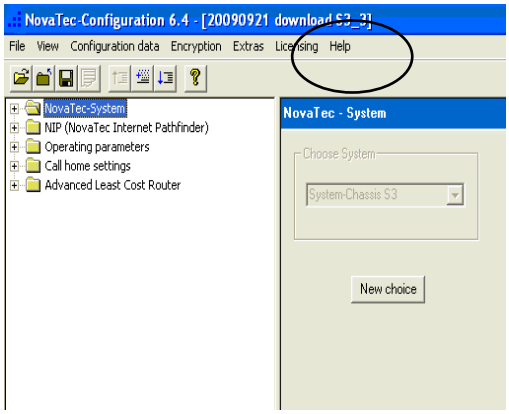
Unlock the Firmware

I) A new licence management to secure the firmware has been introduced. The licence unlocks the firmware. It is generated by Novatec reading a table of MAC addresses. The firmware and configuration will work only on devices which MAC addresses were used to generate the licence file.

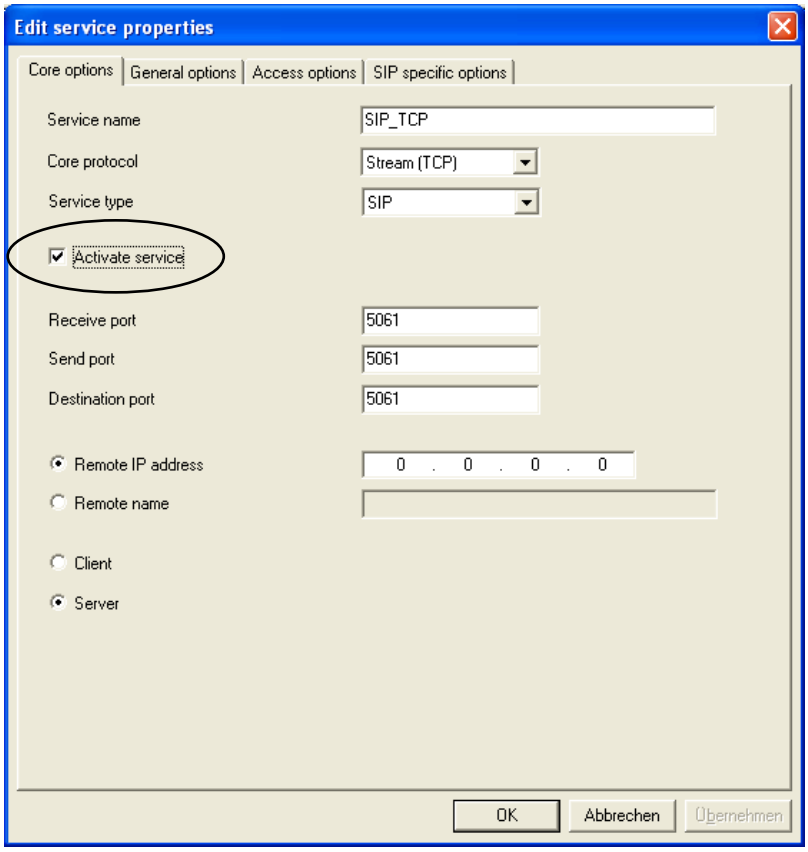
II) Also a new TLS licence has been introduced. It is created like the firmware licence and it unlocks TLS for all devices which MAC addresses were used for building the TLS licence.

III) After you received the “firmware.lic” and optionally the “tls.lic” file from Novatec, open the configuration file by using Ntconfig (version 6.5) and upload the firmware licence. The procedure to load the TLS licence to the system has not been changed (see “2. Enable TLS to secure SIP”). After uploading the new TLS licence, existing certificates should remain in the configuration, but existing ip services like UDP or TCP for SIP will be deactivated! See next page clause IV).

Upload firmware licence:



IV) Under “System IP options” -> “Available IP services” activate the appropriate ip services e.g. UDP or TCP for SIP. The services HTTP and TELNET cannot be activated for security purpose.



1 Enable encryption for RTP

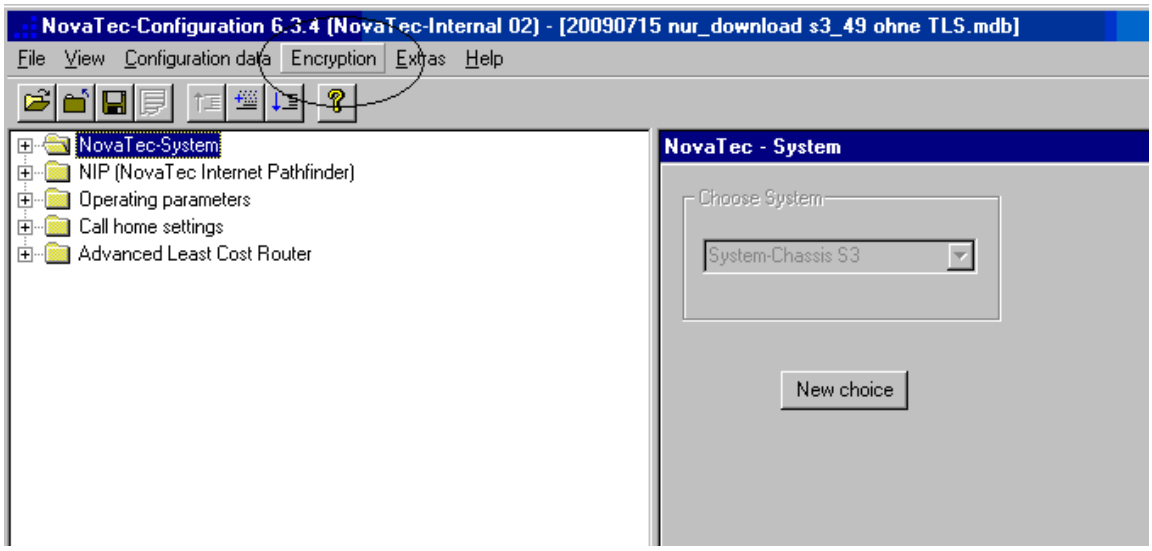
To enable sRTP for a S3 send the Backplane ID of the system to Novatec via email.

The „TraceInfo Client“ displays the Backplane ID under „Device“ -> „System ID“.

A Serial number and a name will be returned.

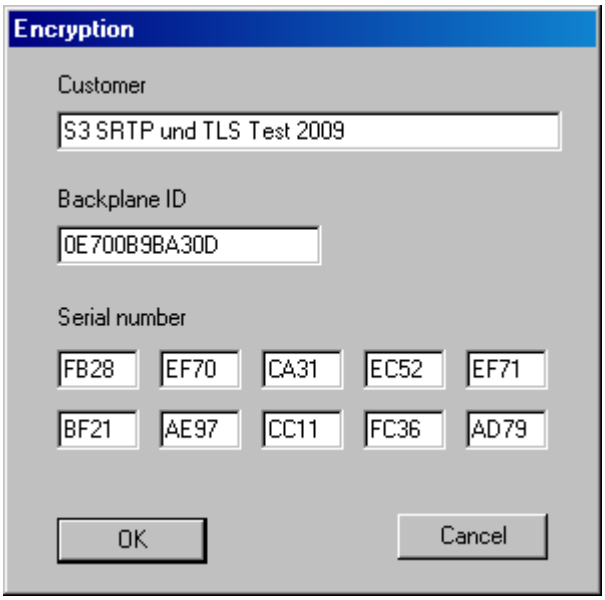
Open the configuration file of the system with „NTConf“.

Select Encryption -> Enter serial number...



Enter the Backplane ID, the received Customer name and the Serial number:

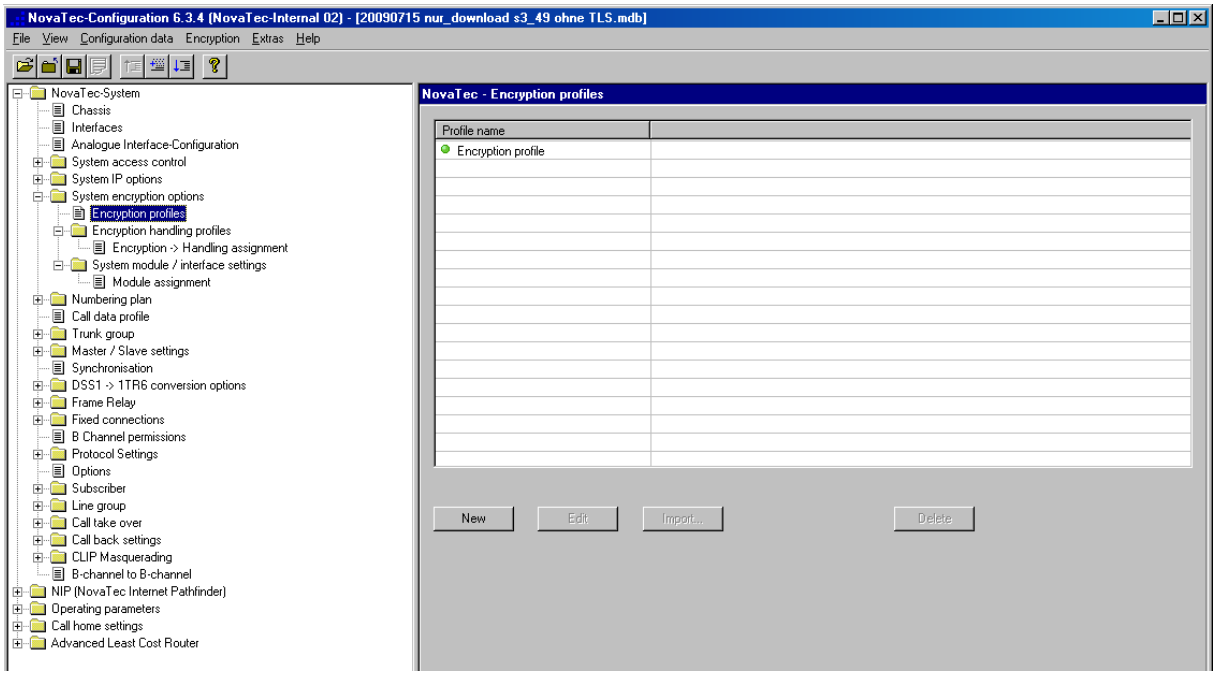
Now this database can be used only to configure the S3/S6, which System ID (also called Backplane ID) was used to generate the „Encryption Serial number“.



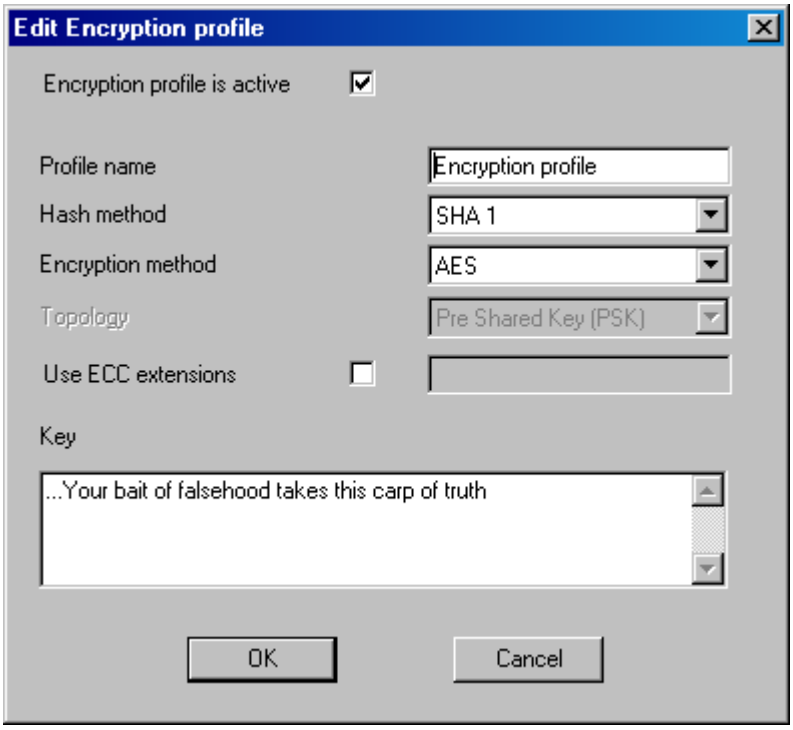
Press OK!

Process the data, close and re-open the database.

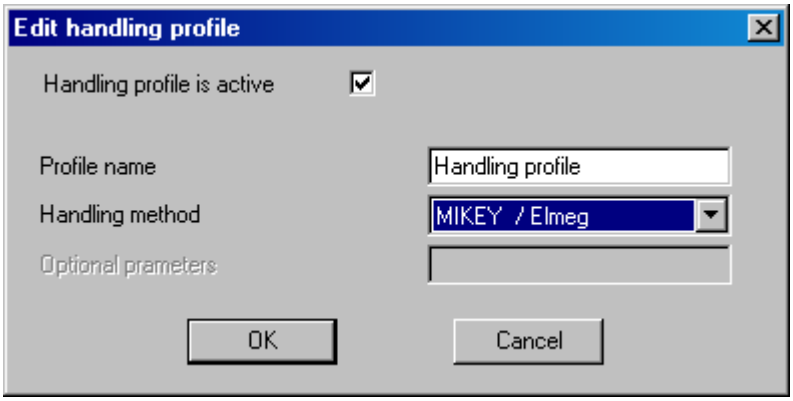
A new item „System encryption options“ will appear at the left hand side.



Leave the Encryption profile unchanged.



Select „Encryption handling profiles“. Set the „Handling method“ to „MIKEY / Elmeg“.



Under „Encryption -> Handling profile“ assign the created „Encryption profile“ to a „Handling method“.

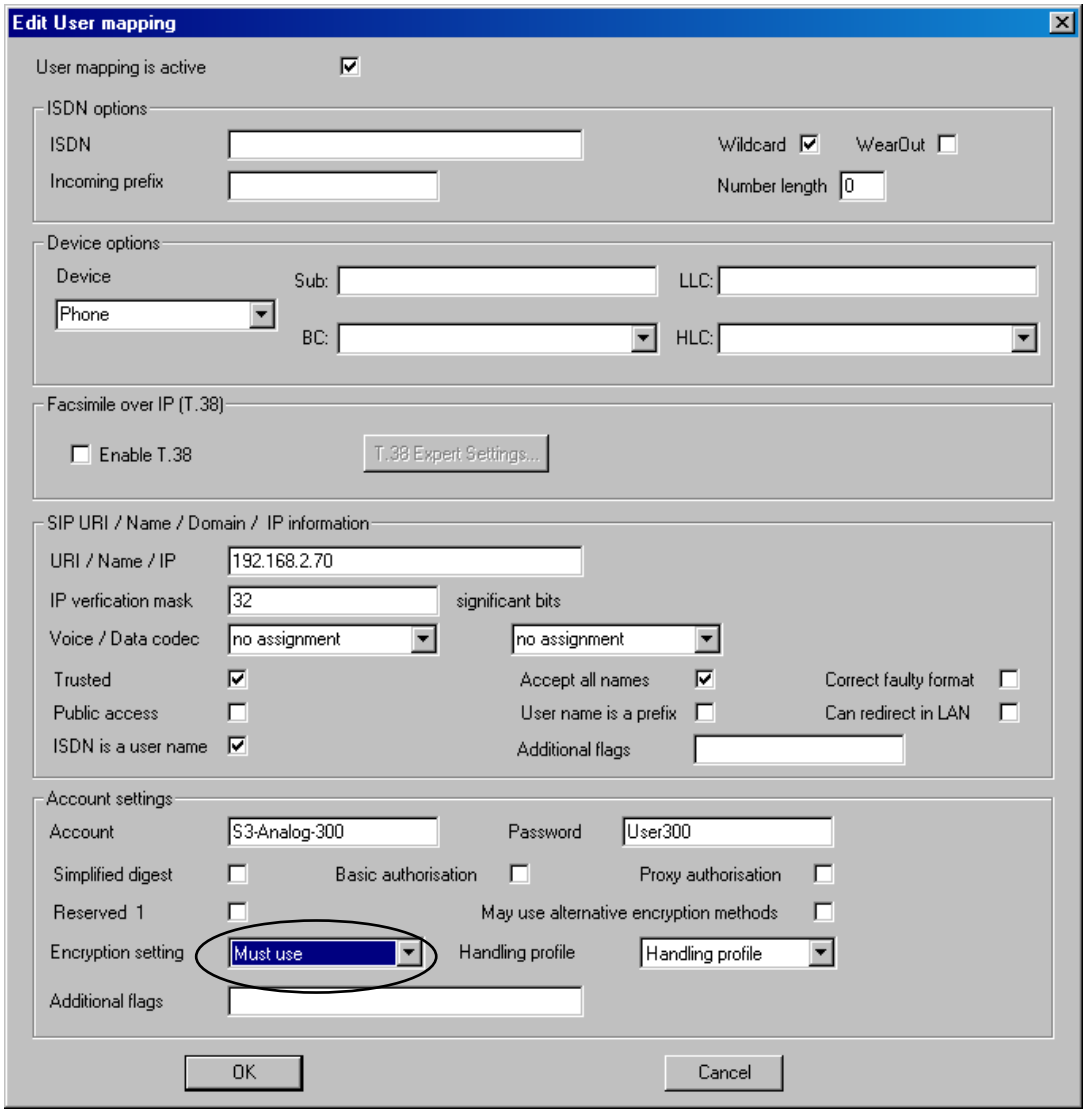
Under „System modul / interface settings“ -> „Modul assignment“ assign the „Handling method“ to a module – today only SIP is possible.

Feel free to change the name/description of the profiles.

Now the created „Handling profile“ can be selected under

„NIP“ -> „SIP“ -> „Mapping lists“ -> „User mapping“.

Then select the appropriate „Handling profile“. If no „Handling profile“ is displayed, process the data and try again!



The setting „Try to use“ instead of „Must use“ for the Encryption setting, activates the sRTP fallback.

Follow the next steps to enable TLS for SIP.

2 Enable TLS to secure SIP

Some parts of the TLS configuration are preliminary and have been changed now (see chapter 2.1 and 3.2).

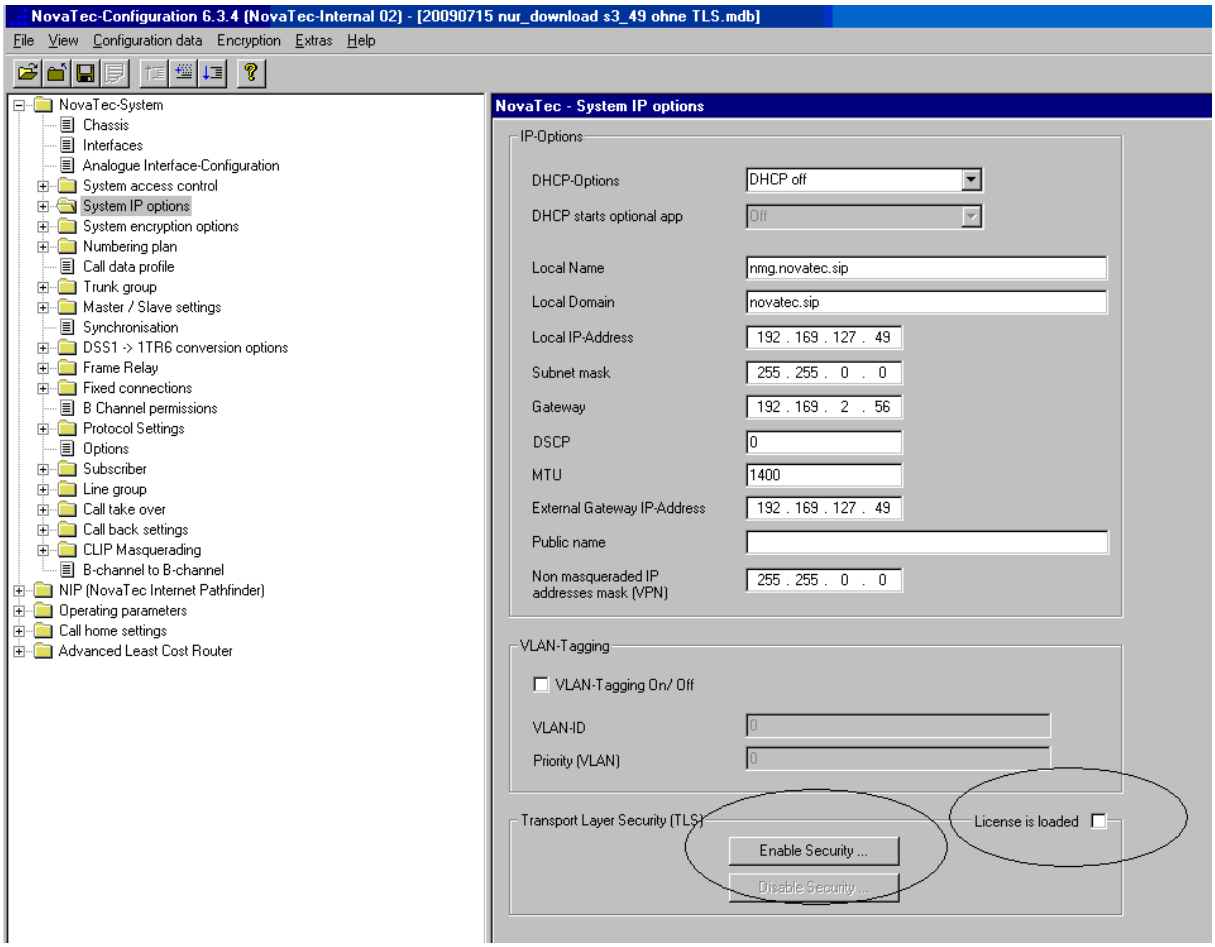
2.1 Enable TLS for S3

Ask Novatec for the licence to enable TLS for this system. Send the MAC address to Novatec and a „tls.lic“ file will be returned.

Then select „System IP options“.

At the bottom of the page select „Enable Security“, enter the path to the saved „tls.lic“ file. Acknowledge the displayed windows.

If the box „Licence is loaded“ is checked, then it is possible to use TLS.



In the tree at the left hand side, under „System IP options“, a new item „TLS Security“ will be displayed.

Notice: After the TLS-Licence has been loaded and SIP is configured, now some settings will be created automatically. In the past these settings have to be made manually. Please, check these settings (refer to chapter 3.2.1):

1. „System IP option" →„Available IP services": A tcp/ip service for SIP via TLS with port 5061 is created.

2. „NIP" → „SIP" → „Mapping lists" -> „User mapping": The port 5061 is added to the user ip address.

3. „NIP" → „SIP" → „Mapping lists" -> „Local mapping": The port 5061 is added to the registrar ip address.

After TLS will be disabled, these settings, created by the system, have to be undone manually for now.

3 TraceInfo CA

3.1 Create a Novatec S3 Root-CA and Key

The „TraceInfo CA“ is used to create a ROOT-CA and to sign the SIP-TLS-Certificate. **To start this program a Novatec dongle is mandatory. Or Novatec can create and sign the certificates online.**

Please make sure only one dongle (e.g. NMS, TI-CA) is connected to the local USB port.

A certificate generated by TI-CA contains a human readable text.

The mandatory part of the certificate starts with a line:

-----BEGIN CERTIFICATE----- and ends with a line:

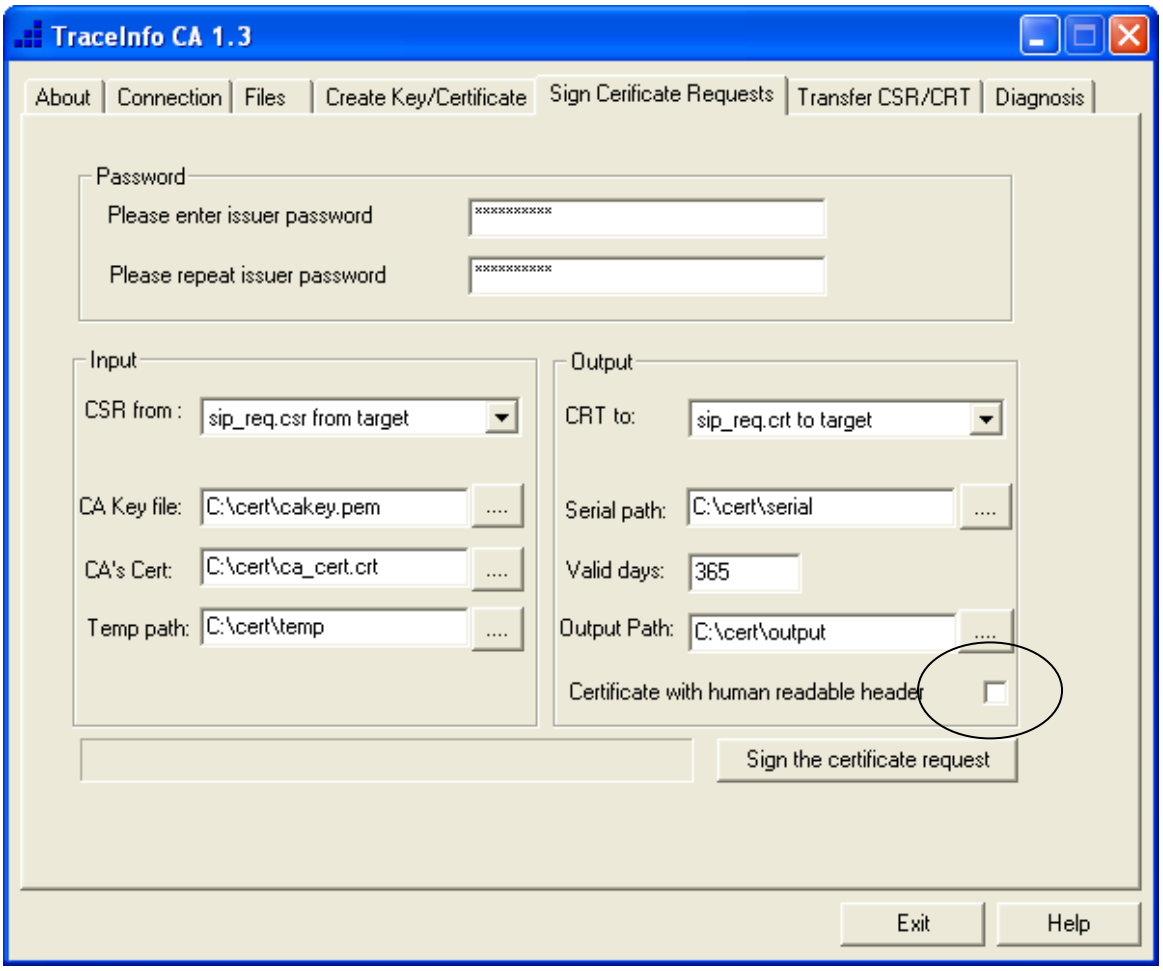
-----END CERTIFICATE-----

Please use an editor, e.g. WordPad, to cut off the human readable text and any blank line, save it. Load the saved file without human readable text to CUCM (see “CUCM Crypto Install Guide”).

TI-CA release 1.3 and above has an option to generate certificate with/without human readable text.

The "Create Key/Certificate" page.

Create a CA private key and a root certificate:



- A connection from the TI-CA application to a target system is not compulsory.

- Select "Root key (2048b) + Certificate" in the combo-box.
- Enter a CA password, which has a minimal length of 4 characters and maximal length of 20 characters.
- Repeat the CA password. If this step fails, an error message will appear on the bottom line and the button "Generate key and certificate" will be disabled.
- Next is to enter country, state, city, organization, organization unit, common name and email address of the CA. Length of the country entry must be 2 characters and the rest of the entries are limited to 64 characters.
- Enter validity of the root certificate in number of days.
- Enter a path, where the serial number of the certificate is stored.(1)
- Enter a path for the CA private key and CA-certificate. The created key and certificate will be stored in this directory. They will have a .pem format with default names, cakey.pem and ca_cert.crt.
- After entering the above information, just press the button "Generate key and certificate". It takes a few seconds to generate the private key. Messages will appear to inform the user.
- Please accept the messages by pressing the OK button.

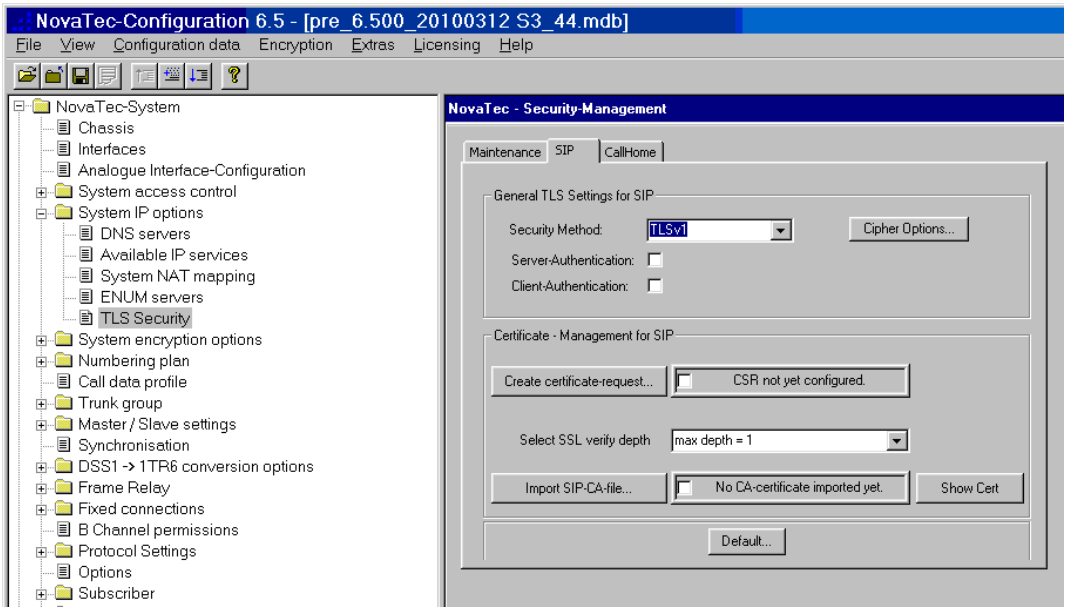
Note (1):
The serial number will be kept in a file called serial.txt. If this file is absent in that given directory, the application will create a new file with a default start number. The user can define his start number by creating a serial.txt file with a 16-digits hex-number himself, e.g. 0123456789ABCDEF. The application will use the current serial number written in the serial.txt file

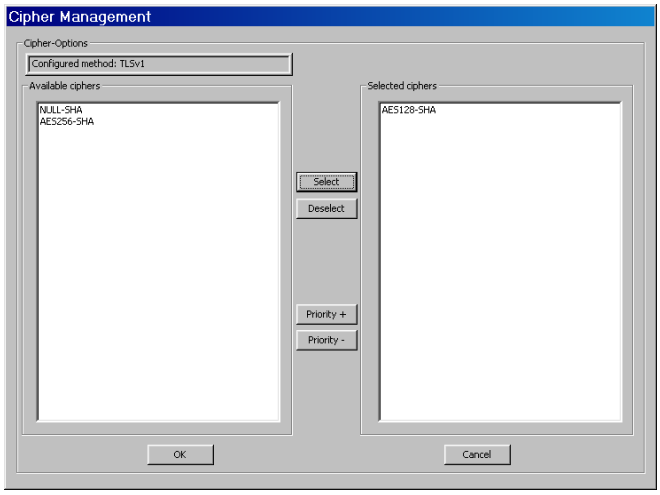
3.2 Configure TLS for SIP

Goto “System IP options” → “TLS Security” → select tab „SIP“

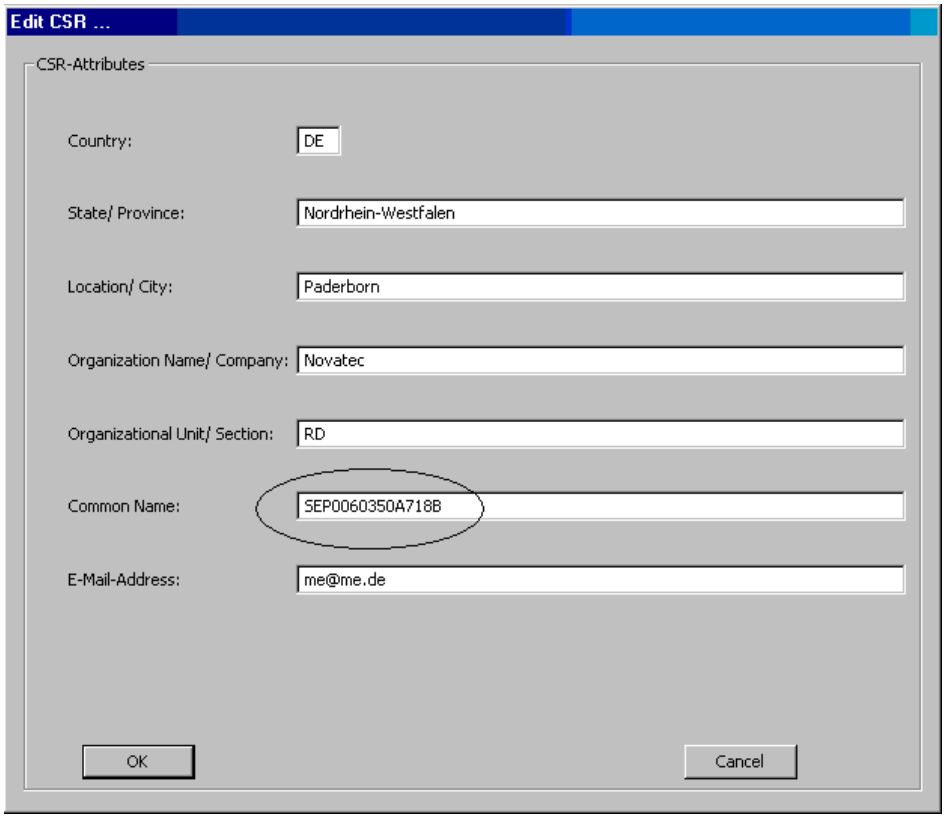
- Set the “Security Method” to TLSv1.
- Set the flag “Server-Authentication” to verify a certificate received from a TLS-server (e.g. S3 and S6 at CUCM).
- Set the flag “Client-Authentication” to request and verify a certificate from a TLS-client (e.g. S6 at trunk of CUCM).
- The SSL “verify depth” is now configurable (values from 1 to 9 – see openSSL documentation). The verify depth is the limit up to which depth certificates in a chain are used during the verification procedure. If the certificate chain is longer than allowed, the certificates above the limit are ignored. Error messages are generated as if these certificates would not be present. E.g. (depth = 0) SIP-CRT → (1) Sub-CRT → (2) Root-CA.
- Click „Cipher Options“ to select the cipher used for TLS encryption (recommended with CUCM AES128-SHA). Select the cipher „NULL SHA“ only for debugging purpose. Do not Select the cipher „NULL SHA“, when sRTP is configured at CUCM.

Note: It is not mandatory to select a cipher here. Not selecting any cipher will enable some cipher by default. Those default values will not harm TLS secured connections.





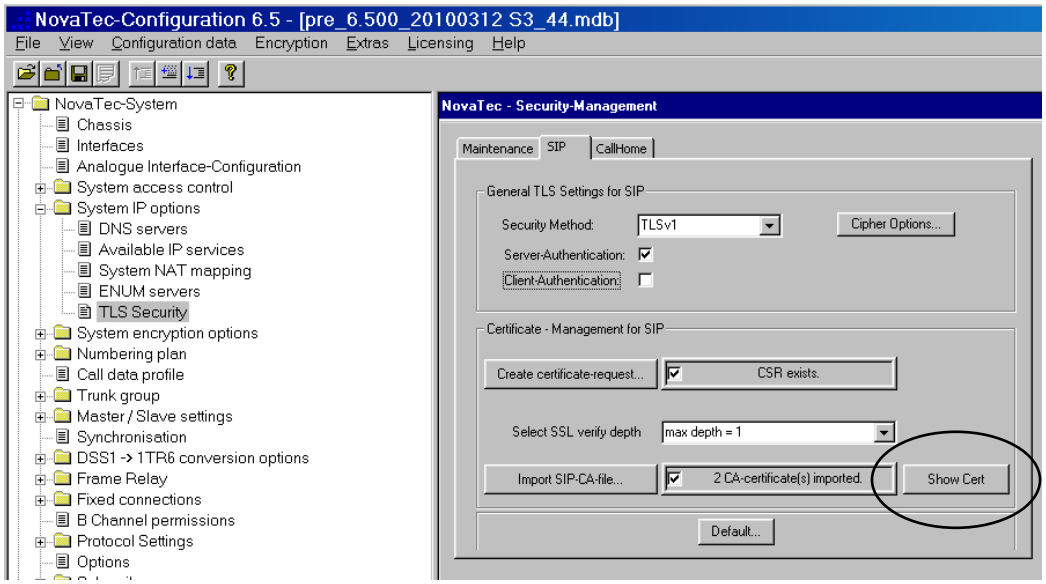
1) Create a certificate-request:



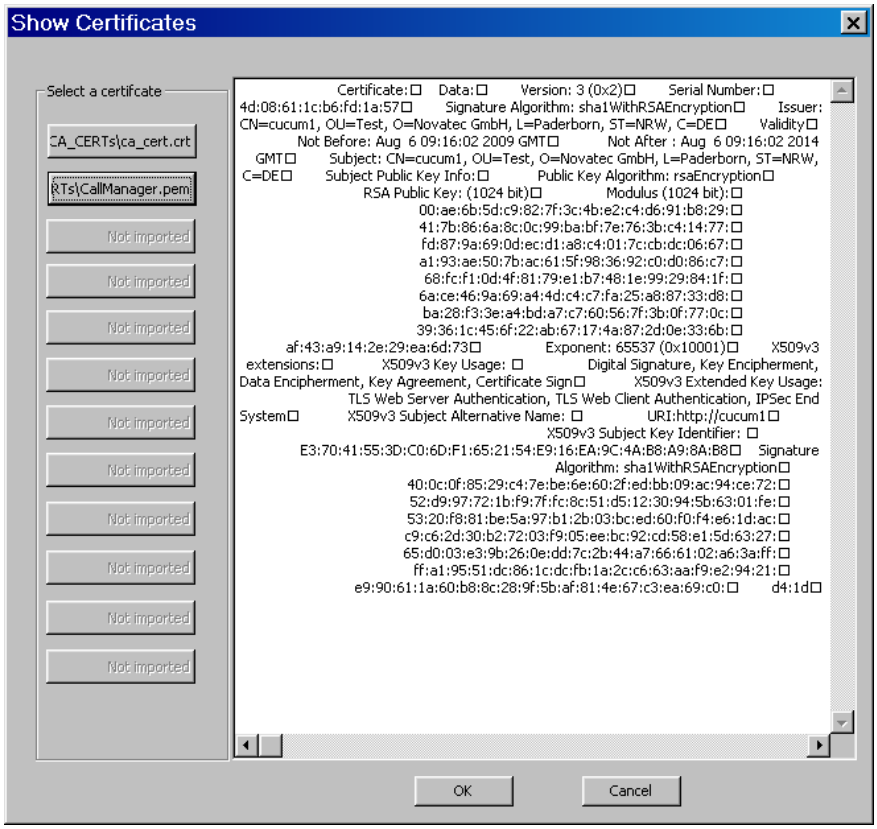
In the Common Name field enter „SEP“ followed by the MAC address of the S3.

2) Import two CAs

Import the CUCM CA certificate (downloaded from CUCM) and the Novatec CA certificate created by the TraceInfo CA.

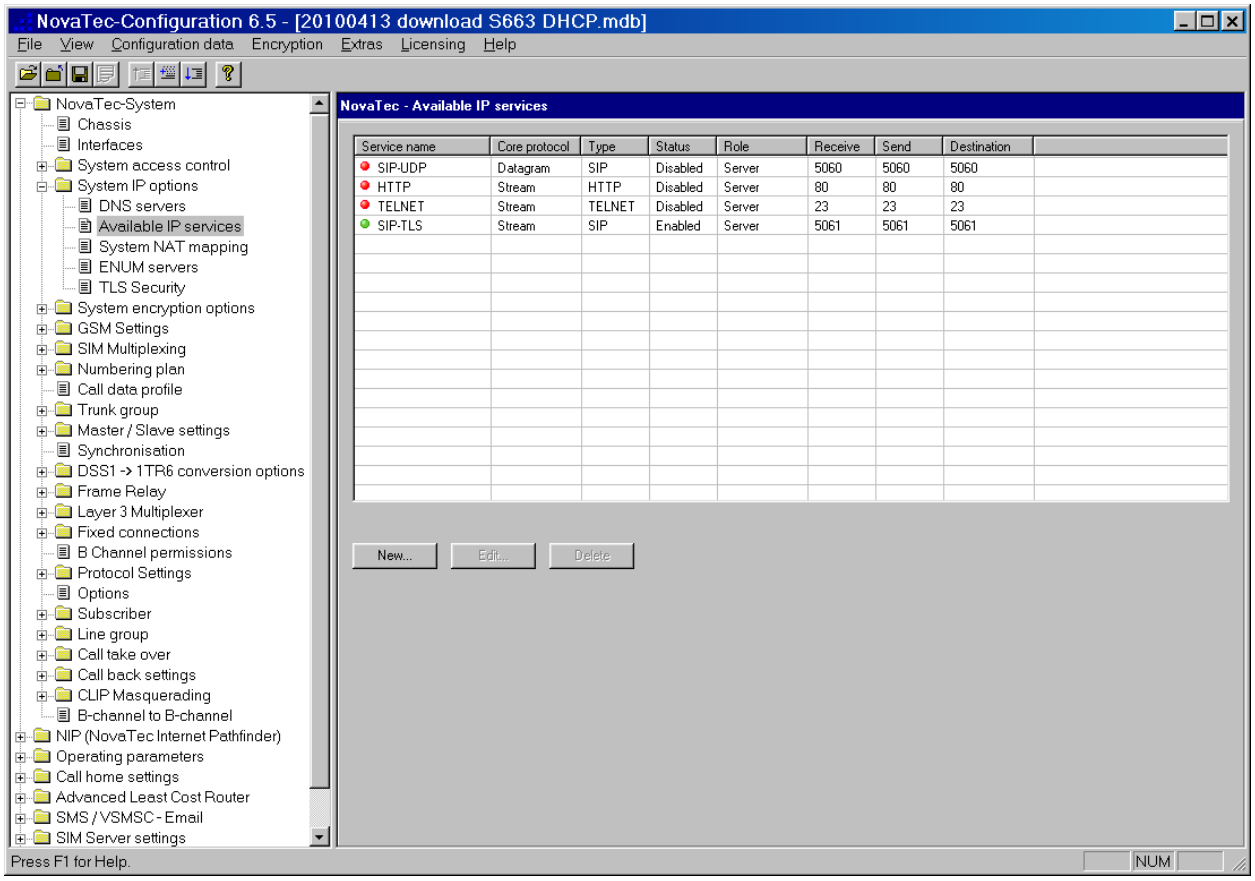


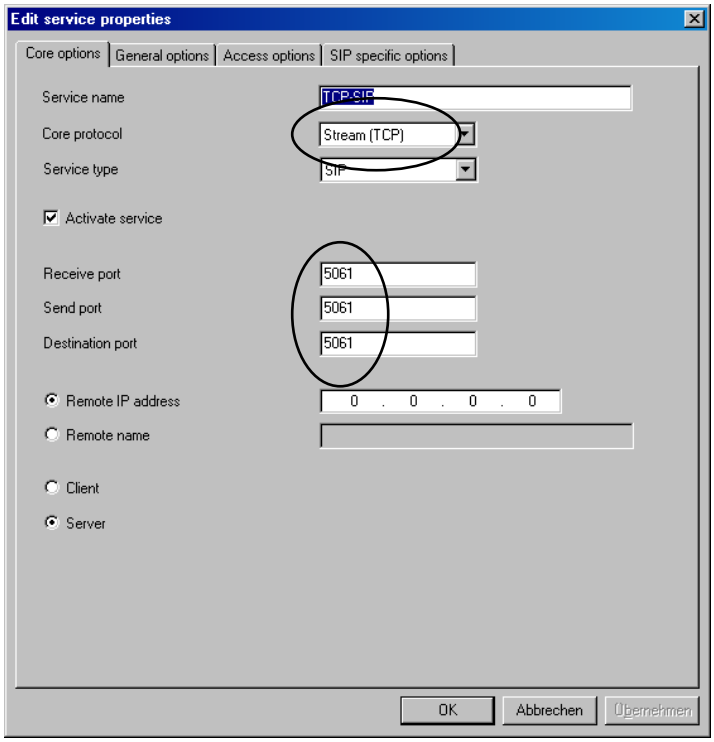
Click the button „Show Cert“ to display the imported certificates.

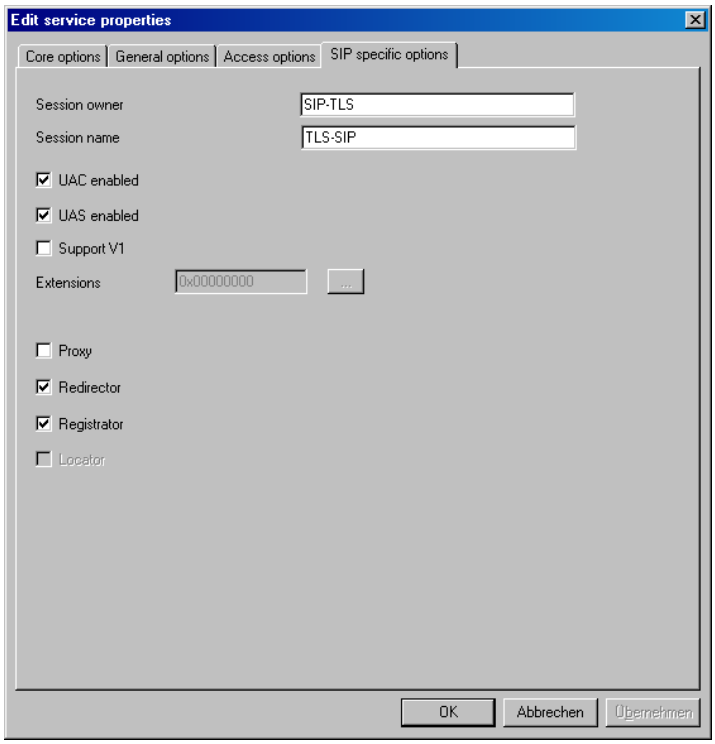


3.2.1 Special SIP via TLS settings

Goto „System IP options“ -> „Available IP services“ to verify that a TCP/IP service (with Port 5061) for SIP via TLS has been automatically created. And check that other services like UDP or TCP of type SIP have been disabled.

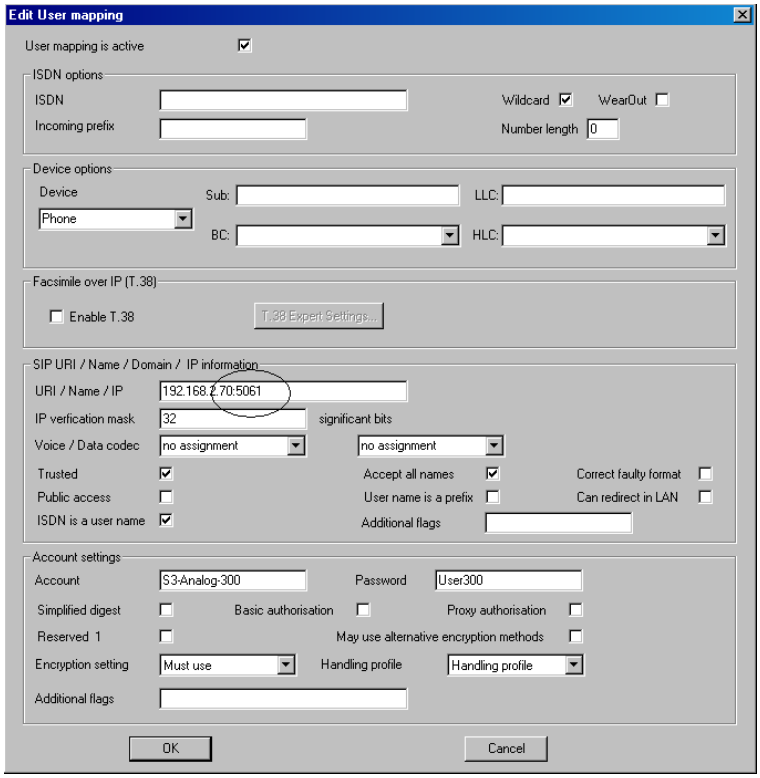






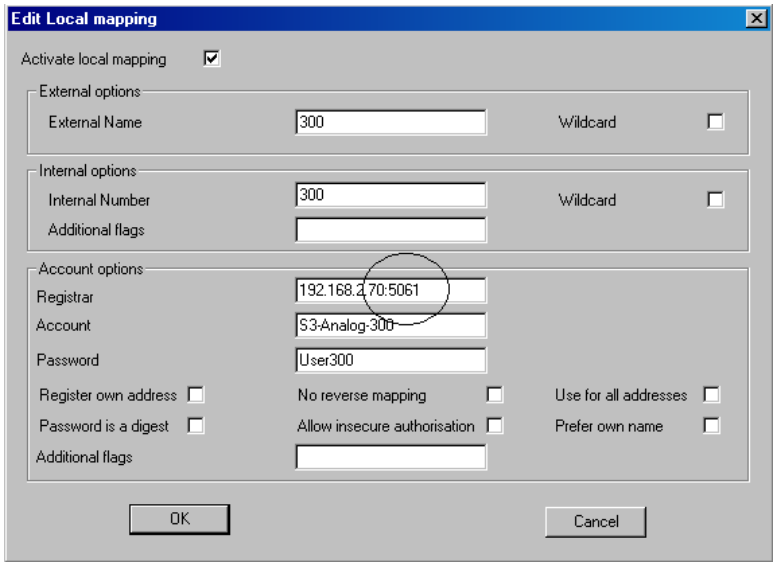
Now go to „NIP“ -> „SIP“ -> „Mapping lists“ -> „User mapping“.

In the „URI/Name/IP“ field the TLS port „5061“ should be existing.

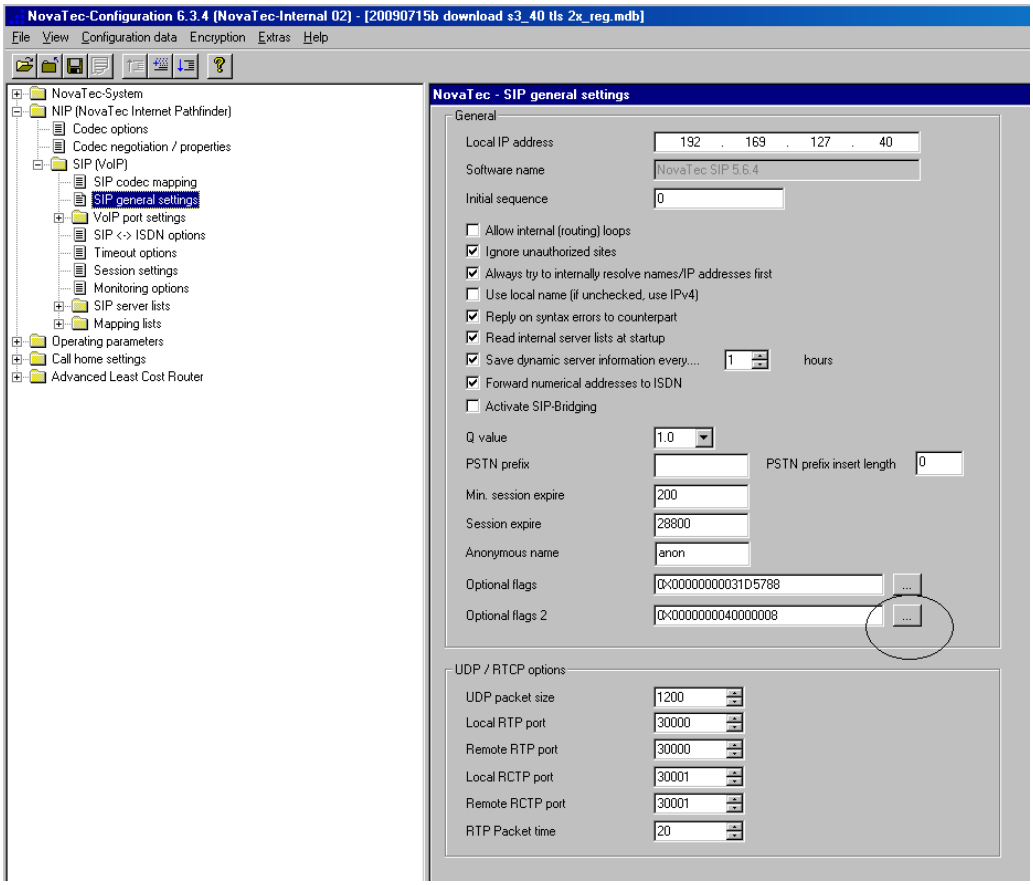


Now go to „NIP“ -> „SIP“ -> „Mapping lists“ -> „Local mapping“.

In the „Registrar“ field the TLS port „5061” should be configured.

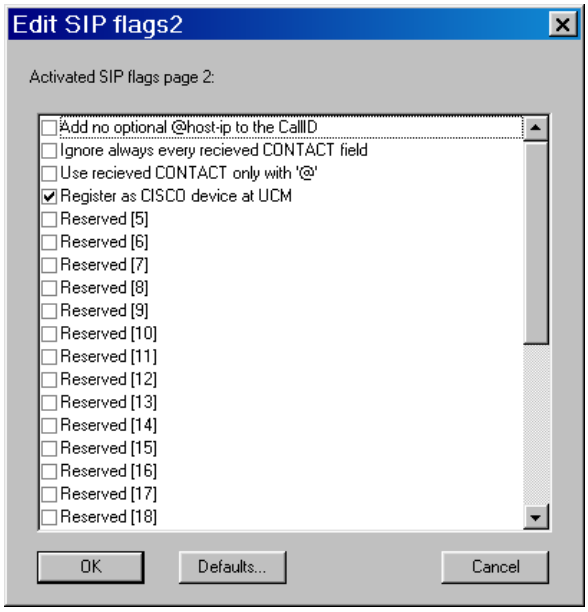


Go to „SIP general settings“, select „Optional flags 2“.



To use a S3 at a device/phone line of a CUCM check the flag “Register as Cisco device at UCM”.

Do not set this flag when using a S3/S6 at a SIP trunk of a CUCM.

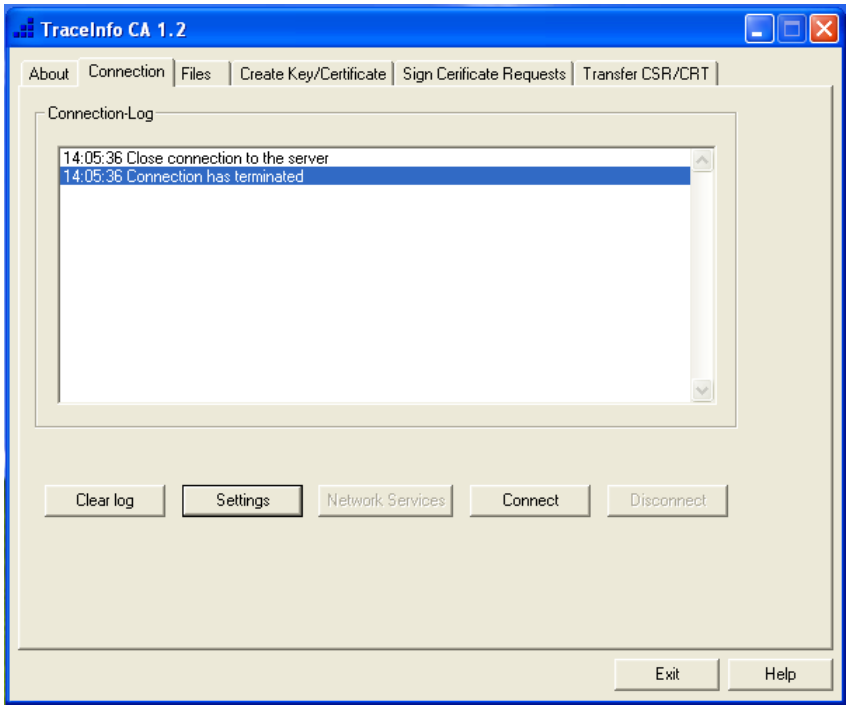


Process and transfer the data to the S3.

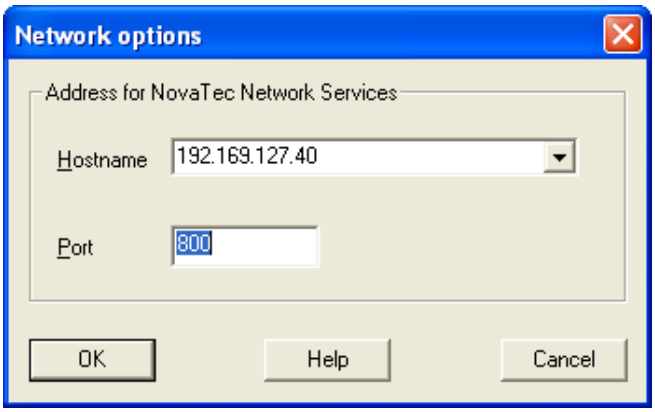
After the S3 has been rebooted, sign the SIP-request with the TraceInfo CA to get a SIP-certificate.

3.3 Sign a SIP-TLS-Certificate

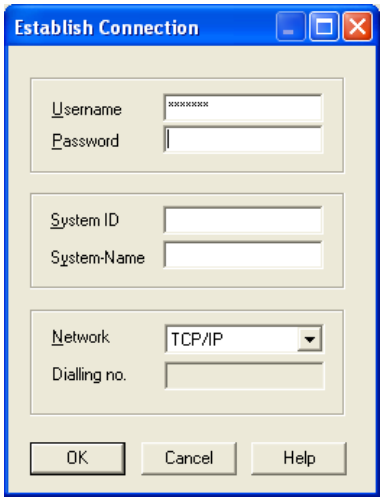
Open the TraceInfo CA.



Under „Settings“ enter the IP address of the S3.



Then connect to the S3. Enter the „Username“ „technics“.

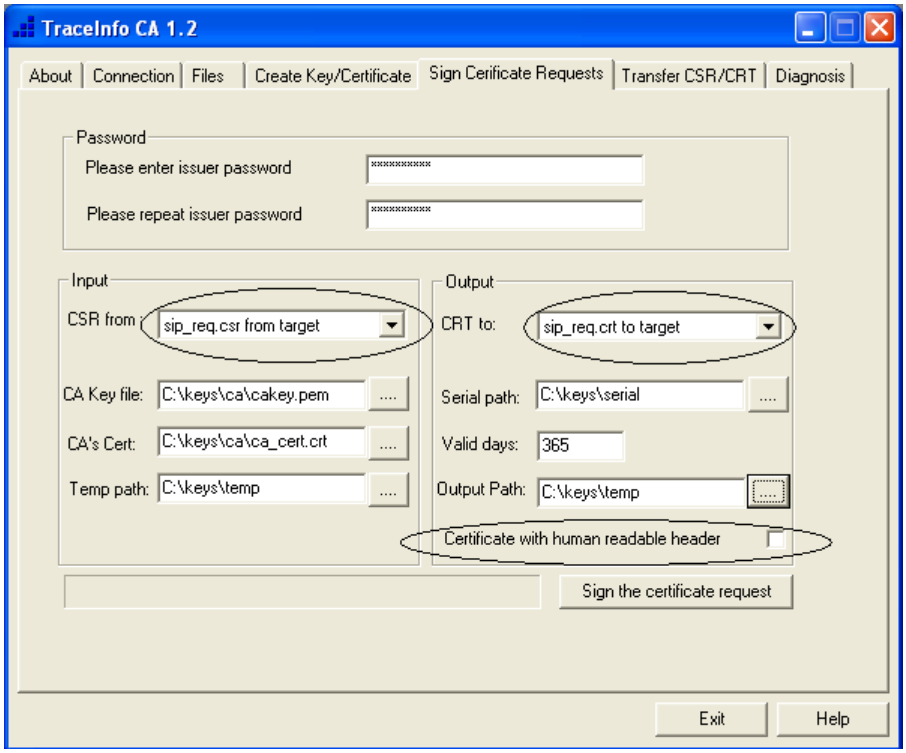


After the connection has been established select the register „Sign Certificate Requests“.

3.3.1 Sign Certificate Requests online

With this register, one can sign a certificate request to a certificate. The request can be a file in a PC or in a target system (S3/S6).

Signing a certificate request from a target system and write the signed certificate back to the target system (S3/S6).



- A connection from the TI-CA application to an target system is compulsory in this case.

- Enter a CA password, which was associated with the CA private key, cakey.pem.

- Repeat the CA password. If this step fails, an error message will appear on the bottom line and the button "Sign the certificate request" will be disabled.

- In the Input group box, select the following:

  - Select "certificate request from target" in the Input combo-box.

  - Select the CA private key file.

  - Select the CA certificate.

  - Select a path, where the certificate request file could be stored temporary.

- In the Output group box, select the following:

  - Select "signed certificate to target" in the Output combo-box.

  - Enter a path, where the serial number of the certificate is stored.(1)

  - Enter validity of the root certificate in number of days.

  - Enter a path, where the signed certificate file could be stored temporary.

  - Please disable “Certificate with human human readable header”.

- After entering the above information, just press the button "Sign the certificate request".

Note (1):
The serial number will be kept in a file called serial.txt. If this file is absent in that given directory, the application will create a new file with a default start number. The user can define his start number by creating a serial.txt file with a 16-digits hex-number himself, e.g. 0123456789ABCDEF. The application will use the current serial number written in the serial.txt file. After using the current serial number, the application will increment it in the serial.txt file.

After the request has been signed, reset the S3. The S3 should now establish a TLS connection and register with the call manager. The voice stream should be encrypted by sRTP.

4 Configure S6 secured SIP/sRTP connections to a CUCM trunk

4.1 Differences between S3 and S6 configuration

The differences are minor on the S6 side. You can configure the S6 like a S3 as the manual specifies it above with the following exception.

Under “SIP general settings”, select “Optional flags 2”.

Here don’t check the flag “Register as Cisco device at UCM”. It is only usefull for the S3, not for the S6 at the trunk line.

As a workaround for better performance the S6 tries to register at the CUCM like a S3. The registration will fail, but it will establish the outgoing TLS connection from the S6 to the CUCM prior to a call. The CUCM will establish a second TLS channel in opposite direction. So configure the “Local mapping” (triggers SIP registration at CUCM/registrar) as the manual describes it for the S3. No configuration concerning SIP registration is necessary on CUCM side.

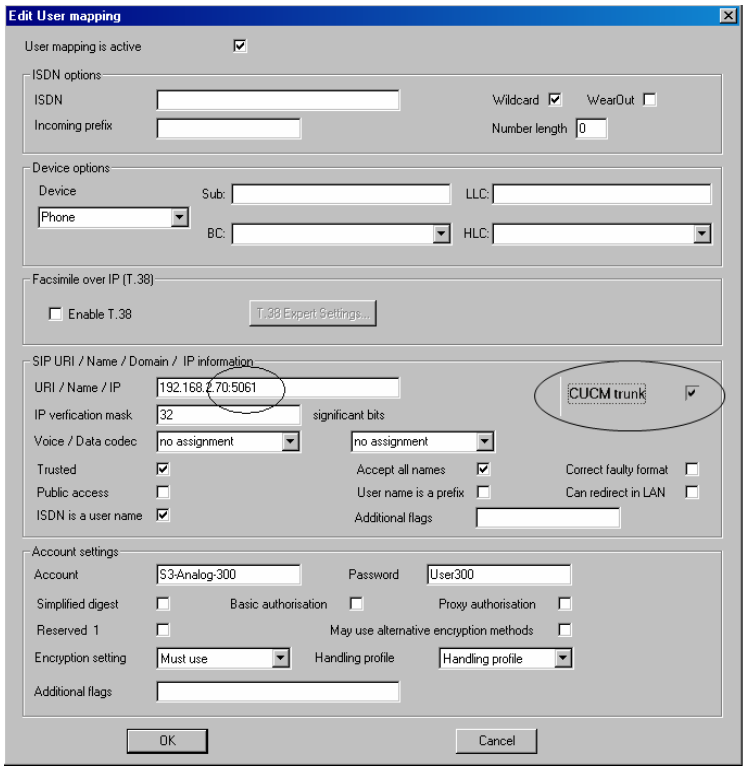
Changes:

30.07.2010

To indicate a IP connection via TLS to a CUCM trunk, set the new flag “CUCM trunk” under user and local mapping. The flags are only available if TLS is activated and the global optional flag “Register as CISCO device at UCM” is not set. Introduced since FW version 00070068.

1. „NIP“ → „SIP“ → „Mapping lists“ -> „User mapping“: Set the new flag “CUCM trunk”.

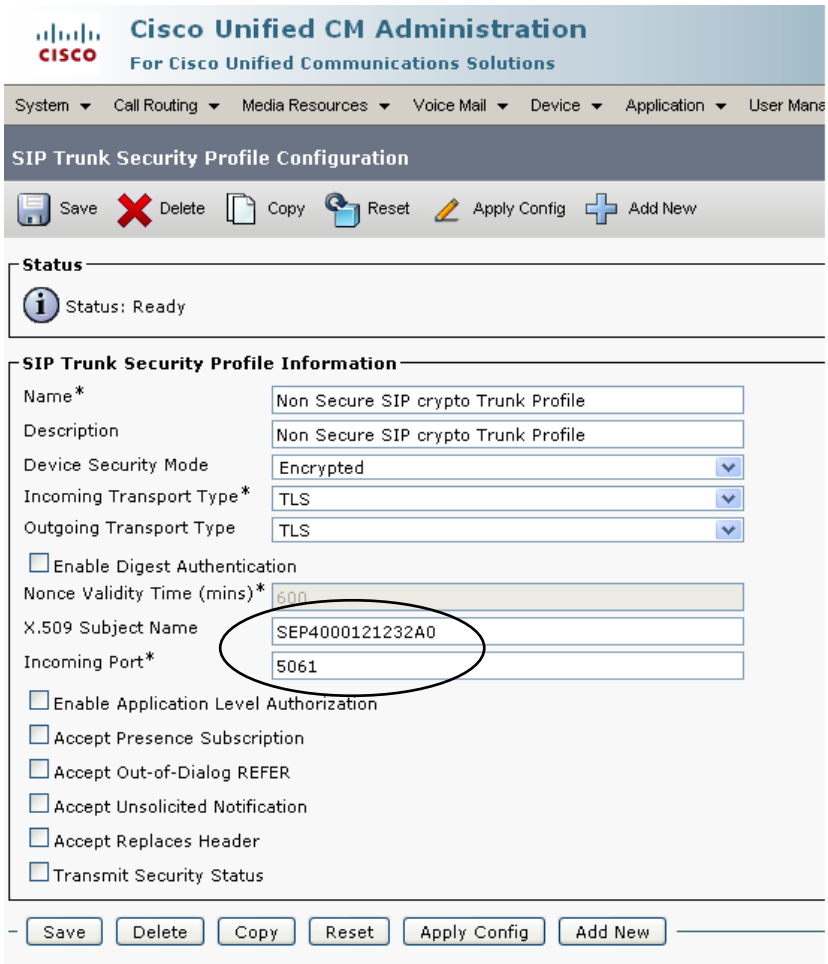
2. „NIP“ → „SIP“ → „Mapping lists“ -> „Local mapping“: Set the new flag “CUCM trunk”.



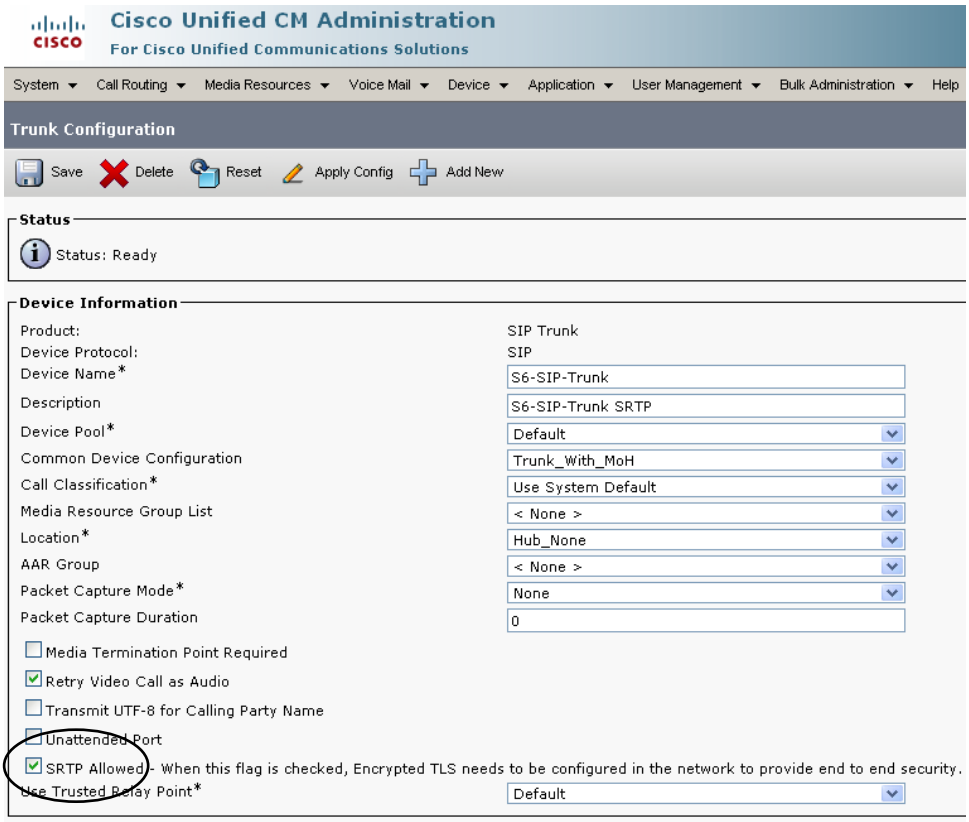
4.2 Configure the S6 trunk at CUCM side

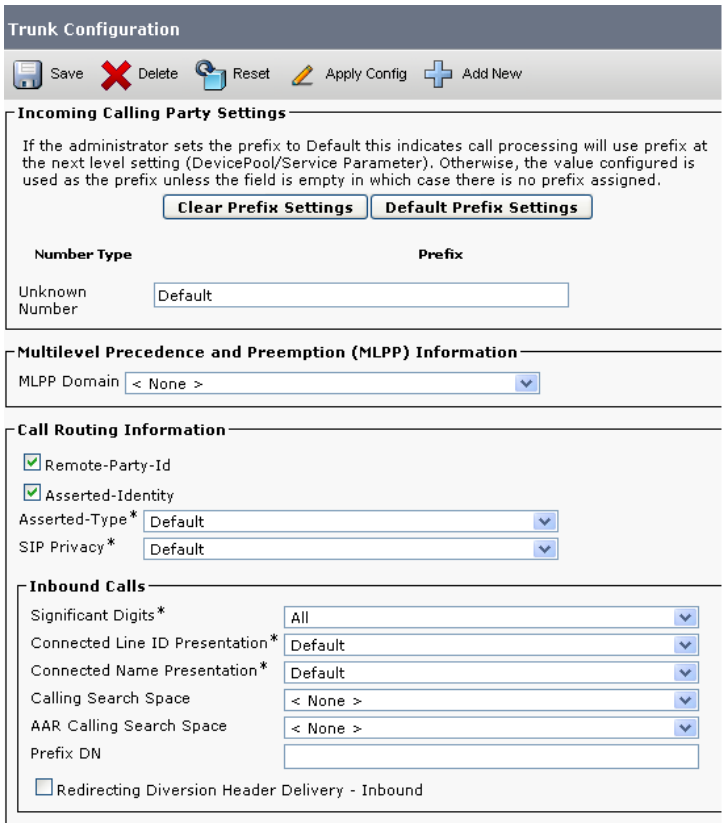
At the trunk security profile enter “SEP” followed by the mac address of the S6/trunk. This implicates a unique secure profile has to be created for every single TLS secured trunk.

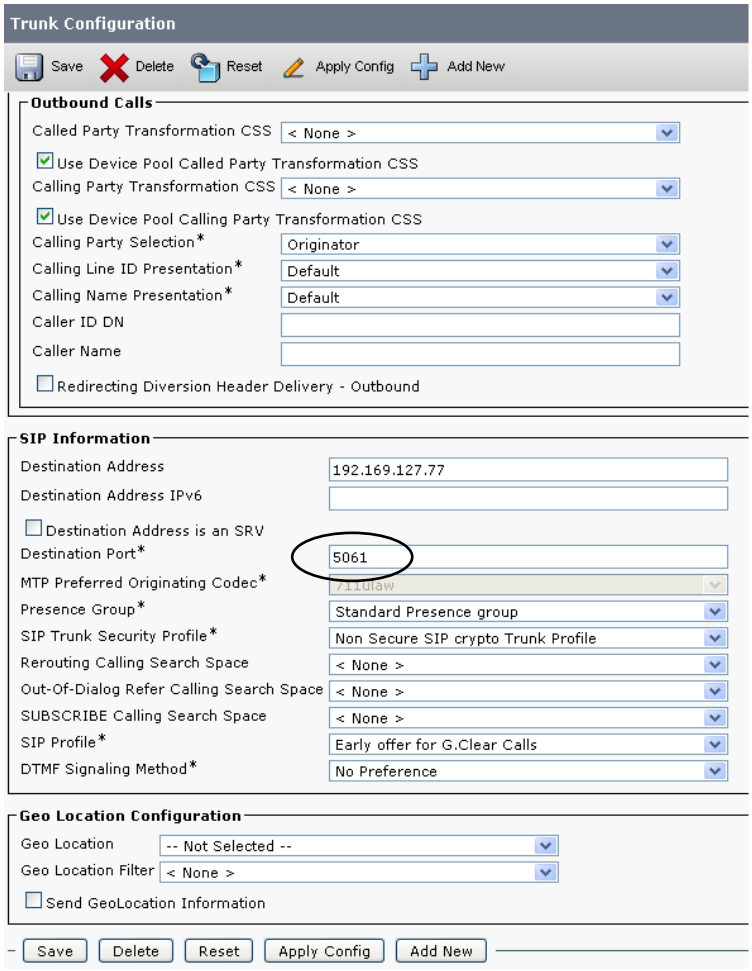
Set “Incoming Port:” 5061.



At the trunk configuration set the “Destination Port” to 5061 and select the appropriate trunk security profile.




Trunk Configuration
Save
Delete
Reset
Apply Config
Add New
Incoming Calling Party Settings
If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.
Clear Prefix Settings
Default Prefix Settings
Number Type
Prefix
Unknown Number
Default
Multilevel Precedence and Preemption (MLPP) Information
MLPP Domain
< None >
Call Routing Information
Remote-Party-Id
Asserted-Identity
Asserted-Type*
Default
SIP Privacy*
Default
Inbound Calls
Significant Digits*
All
Connected Line ID Presentation*
Default
Connected Name Presentation*
Default
Calling Search Space
< None >
AAR Calling Search Space
< None >
Prefix DN
Redirecting Diversion Header Delivery - Inbound

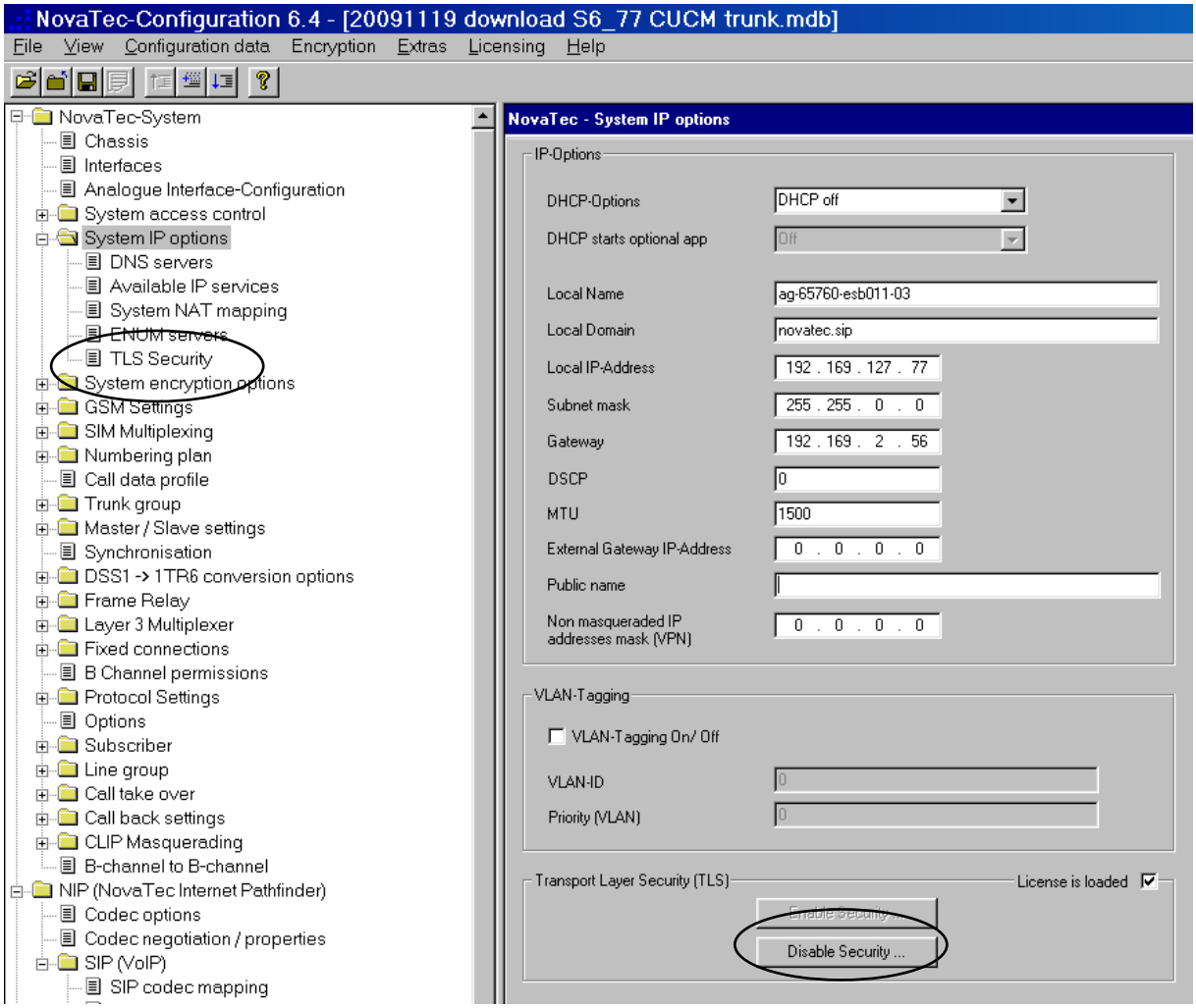

Trunk Configuration
Save
Delete
Reset
Apply Config
Add New
Outbound Calls
Called Party Transformation CSS
< None >
Use Device Pool Called Party Transformation CSS
Calling Party Transformation CSS
< None >
Use Device Pool Calling Party Transformation CSS
Calling Party Selection*
Originator
Calling Line ID Presentation*
Default
Calling Name Presentation*
Default
Caller ID DN
Caller Name
Redirecting Diversion Header Delivery - Outbound
SIP Information
Destination Address
192.169.127.77
Destination Address IPv6
Destination Address is an SRV
Destination Port*
5061
MTP Preferred Originating Codec*
711ulaw
Presence Group*
Standard Presence group
SIP Trunk Security Profile*
Non Secure SIP crypto Trunk Profile
Rerouting Calling Search Space
< None >
Out-Of-Dialog Refer Calling Search Space
< None >
SUBSCRIBE Calling Search Space
< None >
SIP Profile*
Early offer for G.Clear Calls
DTMF Signaling Method*
No Preference
Geo Location Configuration
Geo Location
-- Not Selected --
Geo Location Filter
< None >
Send GeoLocation Information
Save
Delete
Reset
Apply Config
Add New

5 Disable TLS and sRTP for a S3 and S6

5.1 Switch off security for SIP and maintenance

Go to NovaTec-System -> System IP options.

Select “Disable Security …”, acknowledge the displayed windows. In the left hand tree, under “System IP options” the menue “TLS security” will be removed.



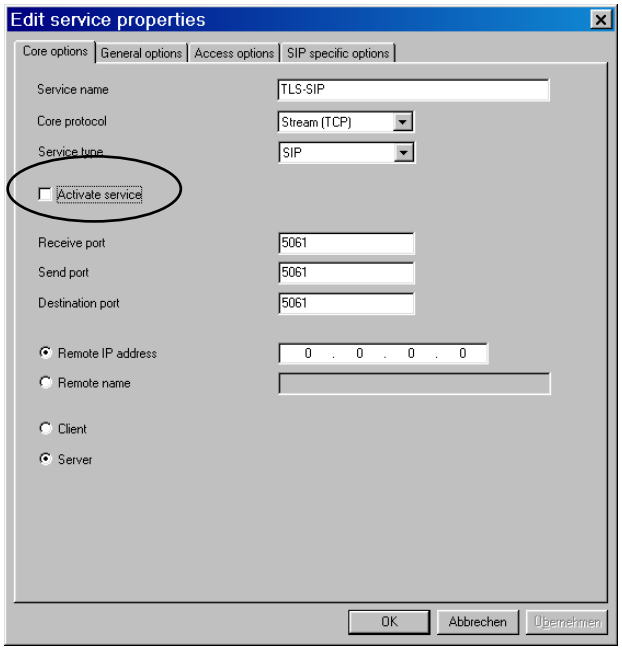
5.2 Change the IP transport service

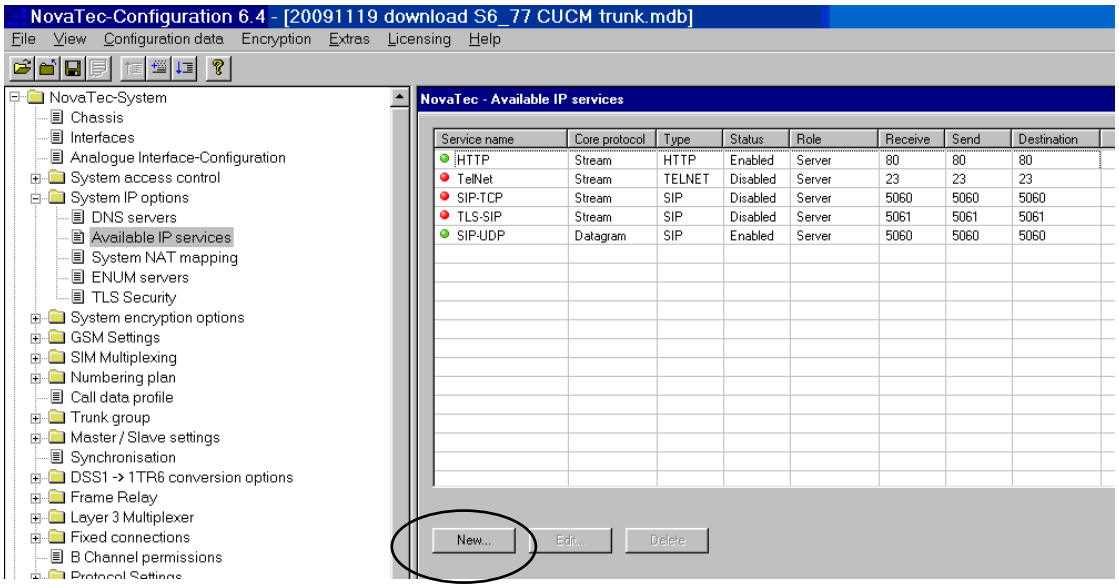
Now the transport protocol TCP for TLS will be switched off and UDP will be used instead.

Goto NovaTec-System -> System IP options -> Available IP services.

Double-click the TLS-SIP service (the name might differ) and uncheck “Activate service”.

Leave with “OK”.

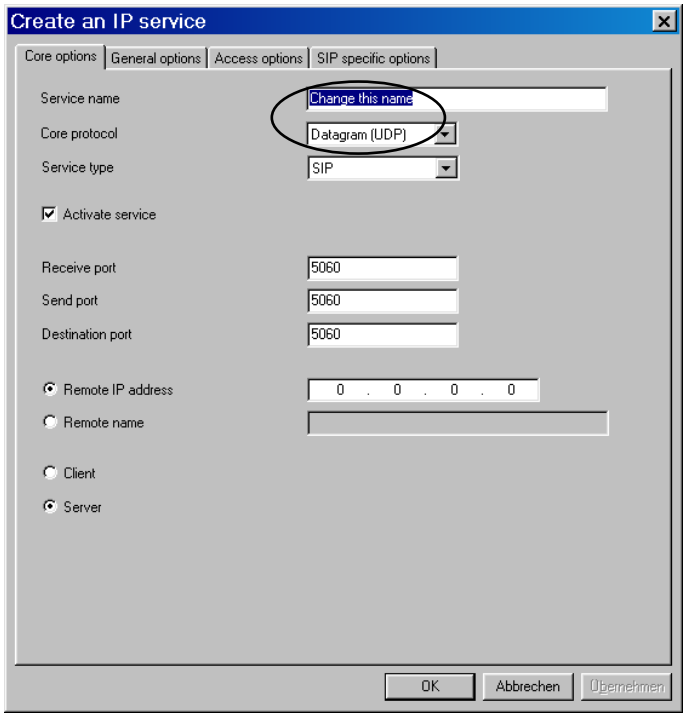




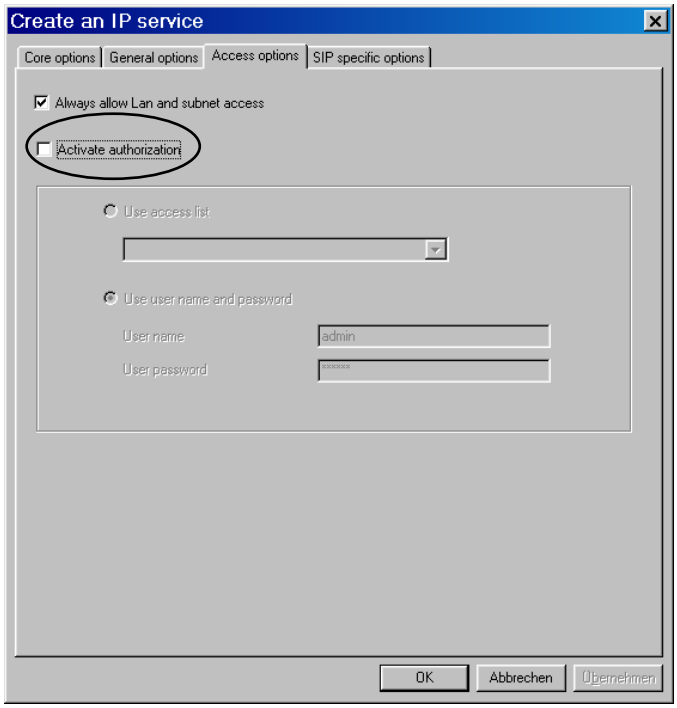
If a UDP service is present but not enabled, double-click this service entry and check “Activate service”.

If no UDP service is available, select the “New…” button to setup this service for SIP.

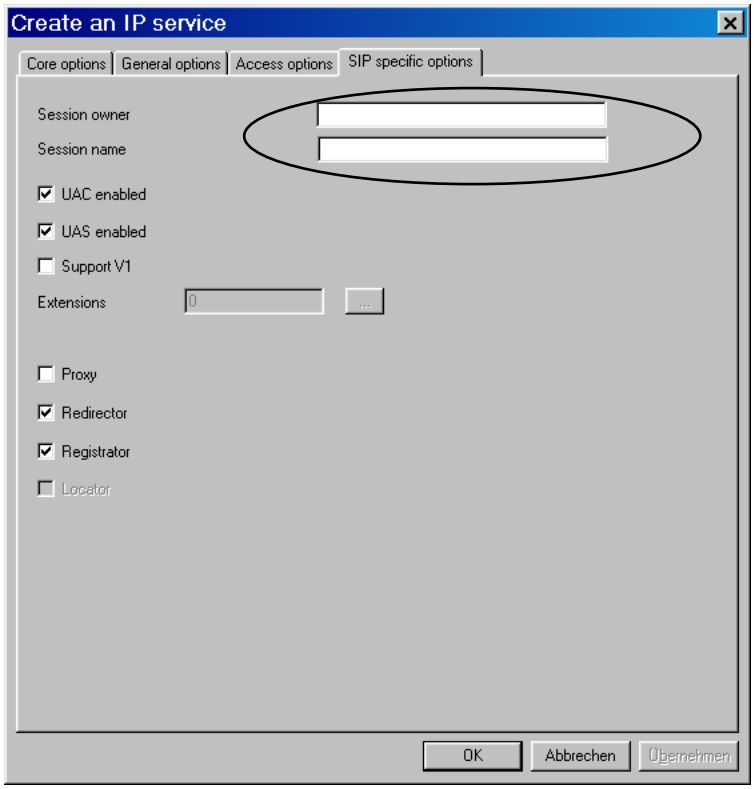
Enter a name for this service and choose “Datagram (UDP)” as the new ip protocol.



At the tab “Access options” uncheck “Activate authorization”.



Enter the session owner and name (free choice) at the tab “SIP specific options”.



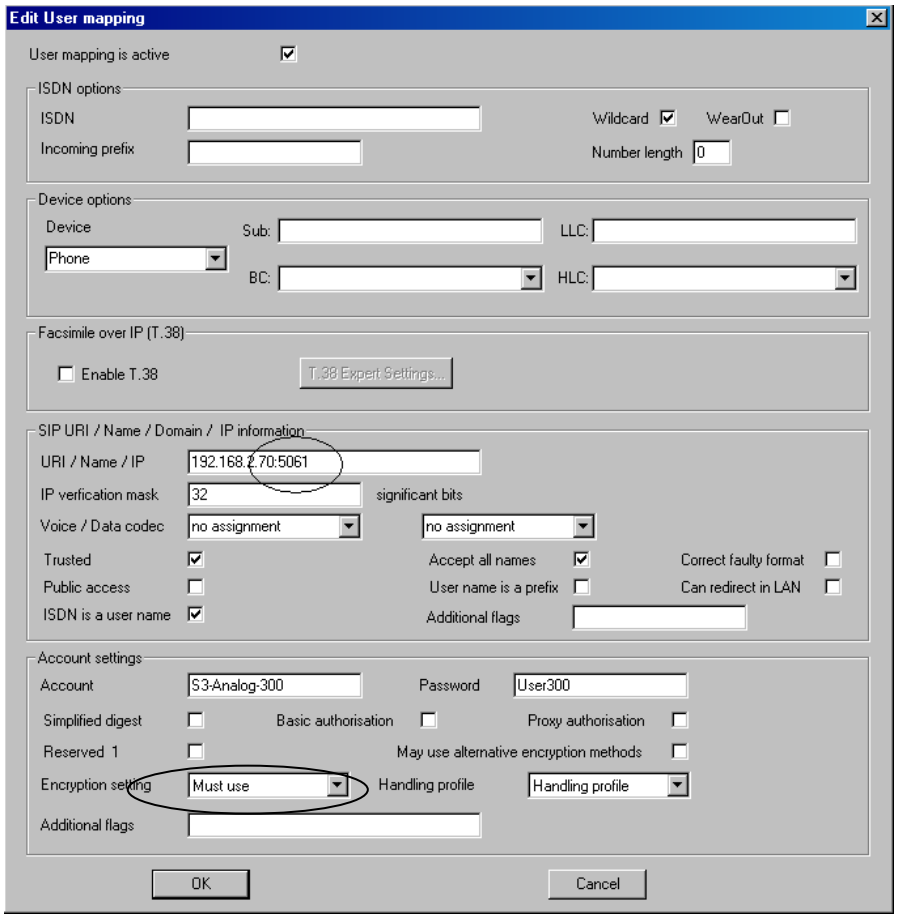
The new transport protocol is now established.

5.3 Remove TLS ports and switch from sRTP to RTP

Now go to „NIP“ -> „SIP“ -> „Mapping lists“ -> „User mapping“.

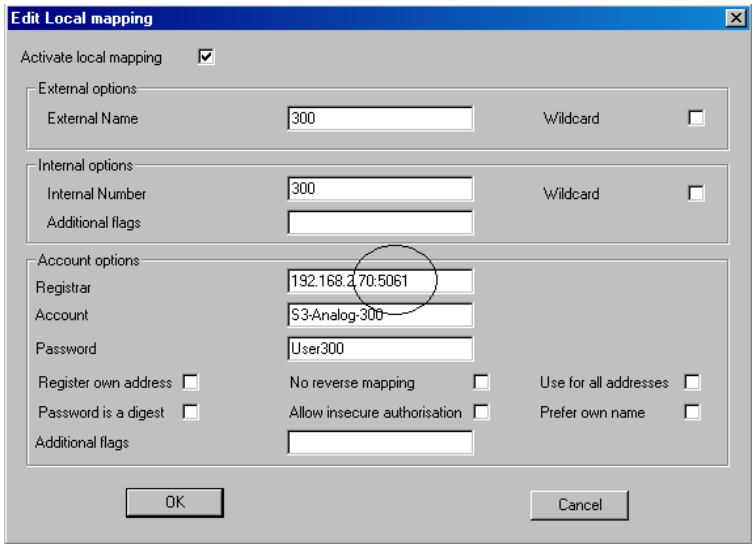
In the „URI/Name/IP“ field delete TLS port „:5061“.

To disable sRTP, select “Do not use” for “Encryption setting”.



Now go to „NIP“ -> „SIP“ -> „Mapping lists“ -> „Local mapping“.

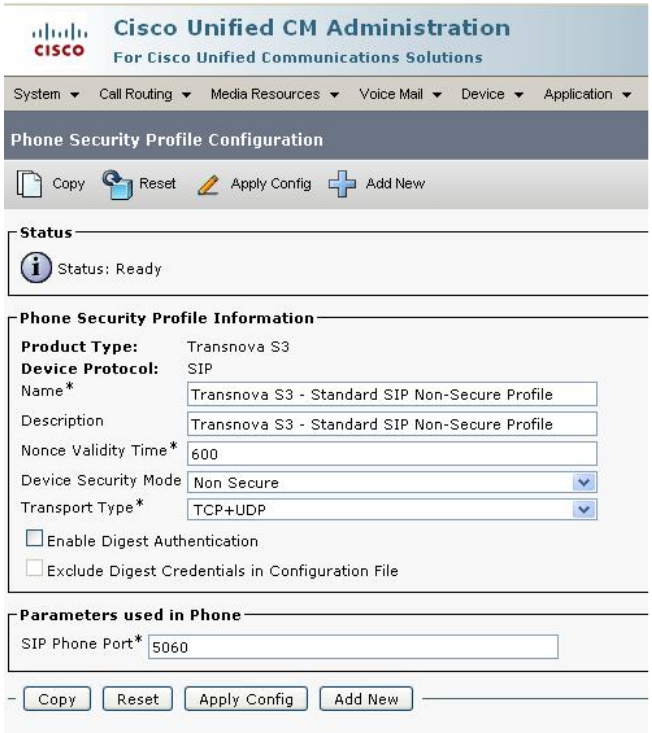
In the „Registrar“ field delete TLS port „:5061”.



5.4 Disable TLS and sRTP for a S3 device in CUCM configuration

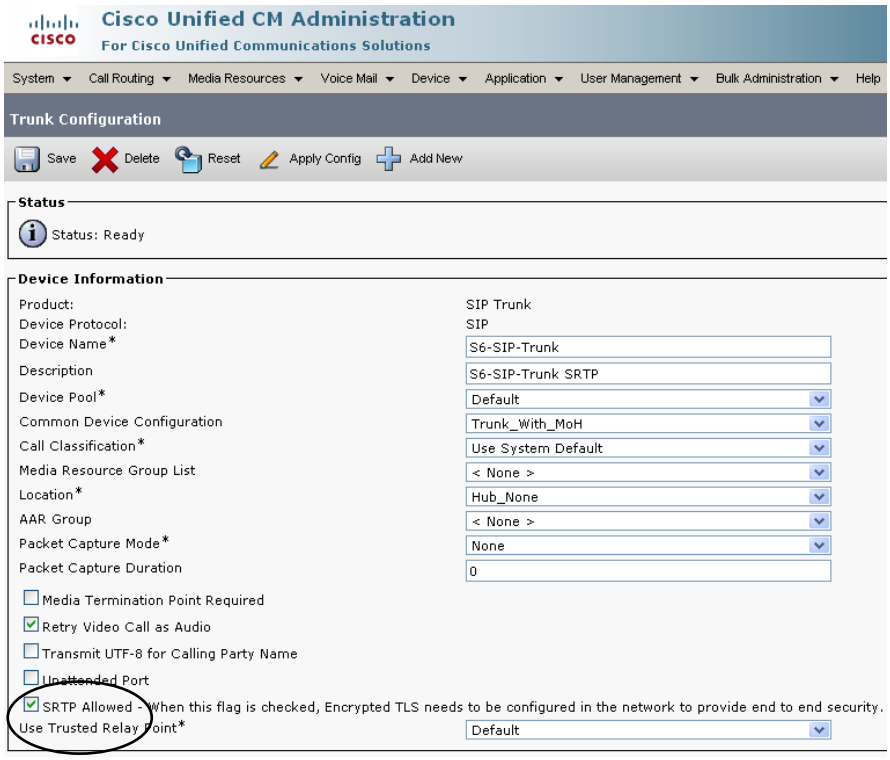
Change from a crypto security profile to a non security phone profile.

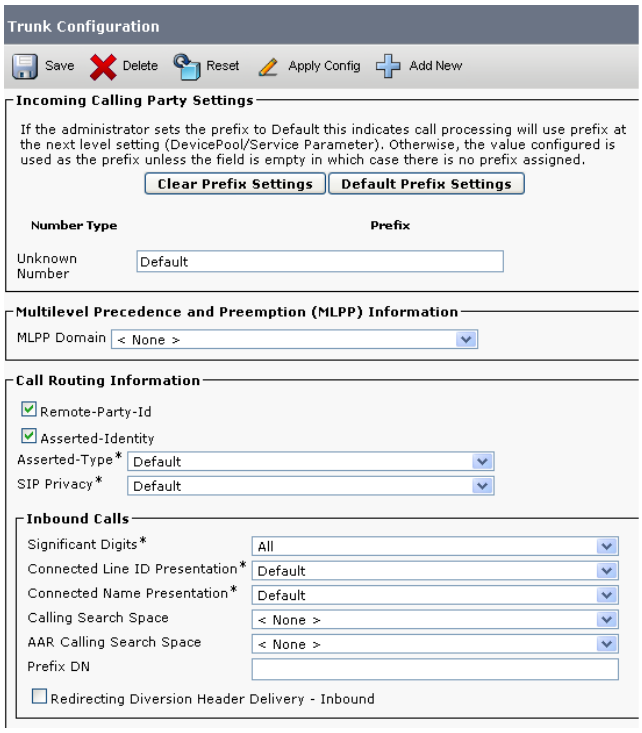
The settings of the phone non security profile should be like this. “Incoming Port:” 5060.

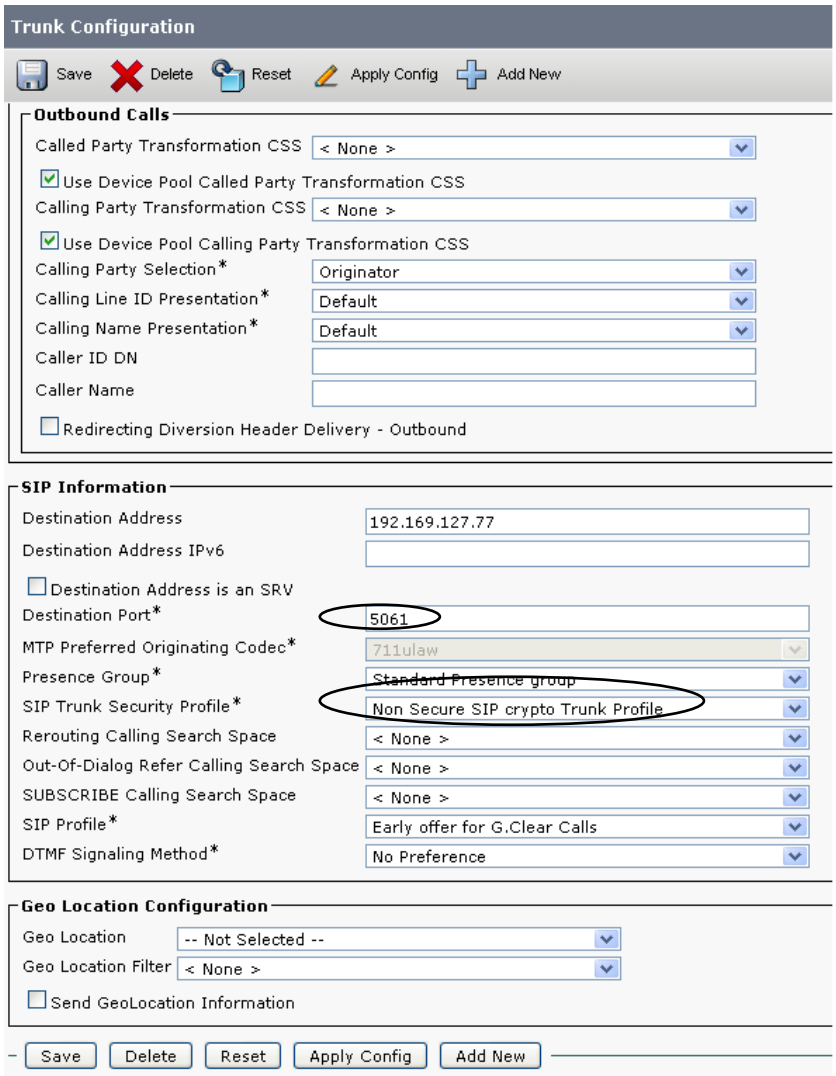


5.5 Disable TLS and sRTP for a S6/trunk in the CUCM configuration

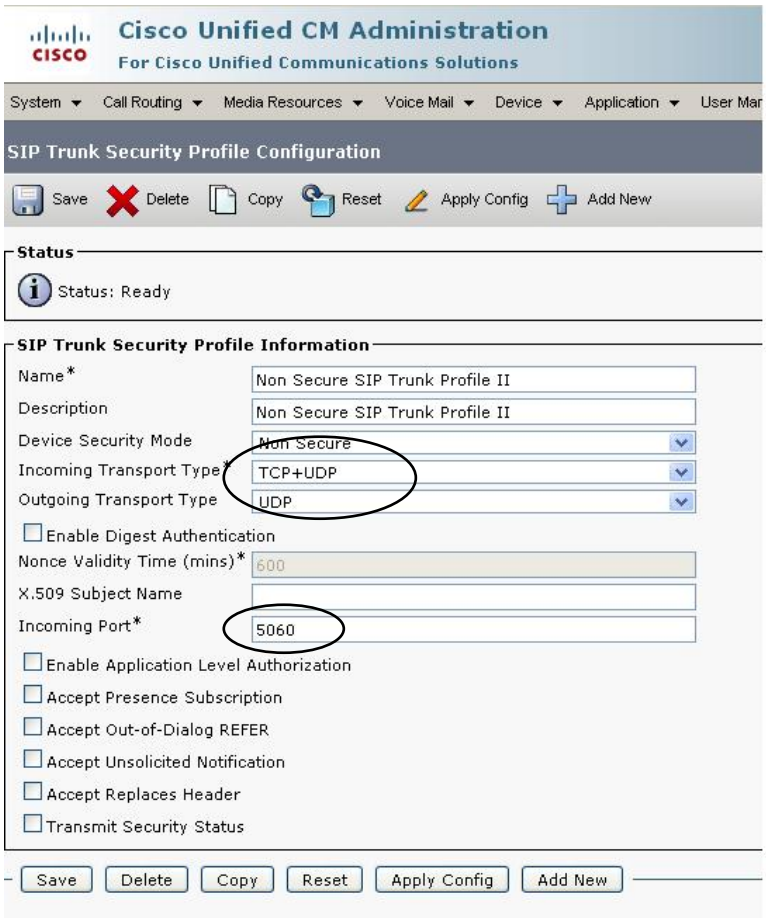
At the trunk configuration window uncheck the “SRTP Allowed..” box, set the “Destination Port” to 5060 and select the appropriate trunk non security profile.







The settings of the trunk non security profile should be look like this example. “Incoming Port:” 5060.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
System
Call Routing
Media Resources
Voice Mail
Device
Application
User Mar
SIP Trunk Security Profile Configuration
Save
Delete
Copy
Reset
Apply Config
Add New
Status
Status: Ready
SIP Trunk Security Profile Information
Name*
Non Secure SIP Trunk Profile II
Description
Non Secure SIP Trunk Profile II
Device Security Mode
Non Secure
Incoming Transport Type*
TCP+UDP
Outgoing Transport Type
UDP
Enable Digest Authentication
Nonce Validity Time (mins)*
600
X.509 Subject Name
Incoming Port*
5060
Enable Application Level Authorization
Accept Presence Subscription
Accept Out-of-Dialog REFER
Accept Unsolicited Notification
Accept Replaces Header
Transmit Security Status
Save
Delete
Copy
Reset
Apply Config
Add New

6 Cisco CTL Client Installation and Secure token addition

For additional information explore CUCM help pages.

In order to support S3 or trunk TLS and sRTP secured SIP calls, the Cisco Unified Communication Manager (CUCM) cluster security mode must be set to mixed mode. See the "Configuring the Cisco CTL Client" section in the CUCM security guide (http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/7_0_1/secugd/sec701-cm.html) to check the steps needed to turned mixed security mode on CUCM.

6.1 Installing the Cisco CTL Client

To install the Cisco CTL Client, perform the following procedure:

1. From the Windows workstation or server where you plan to install the client, browse to Cisco Unified Communications Manager Administration, as described in the Cisco Unified Communications Manager Administration Guide.

2. In Cisco Unified Communications Manager Administration, choose **Application > Plugins**. The Find and List Plugins window displays.

3. From the Plugin Type equals drop-down list box, choose **Installation** and click **Find**.

4. Locate the Cisco CTL Client.

5. To download the file, click Download on the right side of the window, directly opposite the Cisco CTL Client plug-in name.

6. Click **Save** and save the file to a location that you will remember.

7. Make sure security agent on server is off. Eg: No enterprise security agent is running on this server.

8. To begin the installation, double-click **Cisco CTL Client** (icon or executable depending on where you saved the file). **Note**: You can also click **Open** from the Download Complete box.

9. The version of the Cisco CTL Client displays; click **Continue**.

10. The installation wizard displays. Click **Next**.

11. Accept the license agreement and click **Next**.

12. Choose a folder where you want to install the client. If you want to do so, click Browse to change the default location; after you choose the location, click **Next**.

13. To begin the installation, click **Next**.

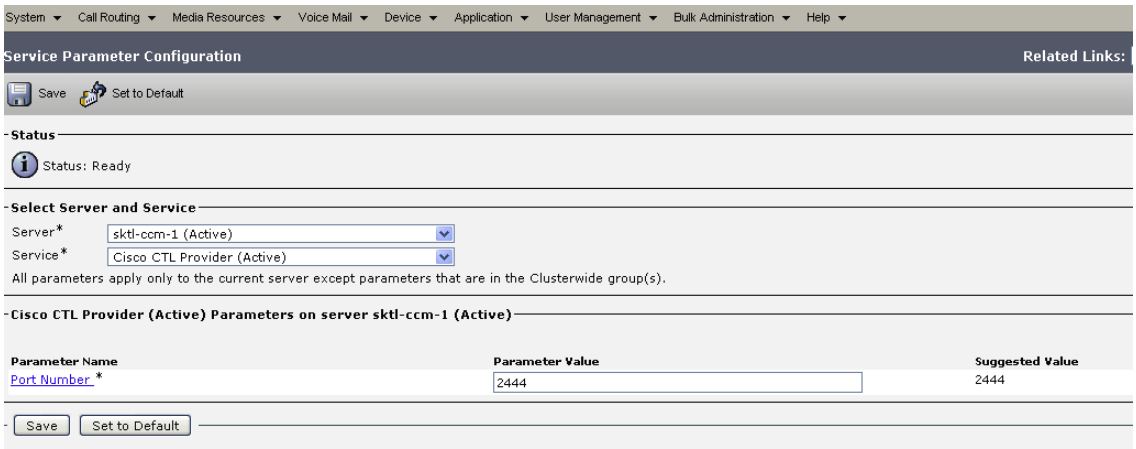
14. After the installation completes, click **Finish**.

Please, check the following before starting CTL Client connect to CUCM:

1. Go to Cisco Unified Serviceability-> Tools-> Service Activation and ensure following two services are active:

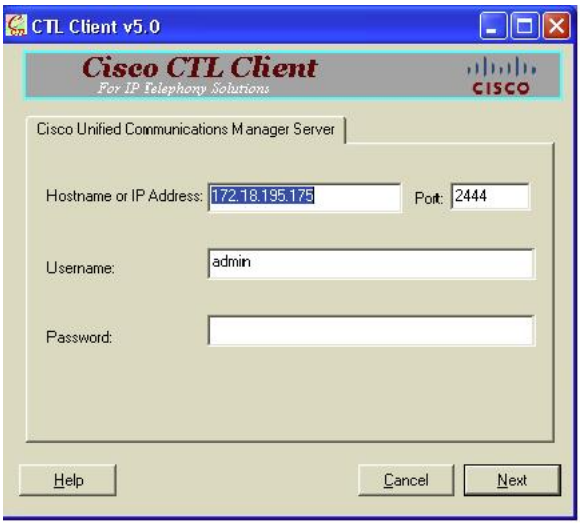
    - Cisco CTL Provider is ACTIVE
    - Cisco Certificate Authority Proxy Function is ACTIVE

2. Go to CUCM Admin page -> System -> Select CUCM server and Cisco CTL Provider service to confirm port number.



Token additions to CUCM and mixed mode secure configuration

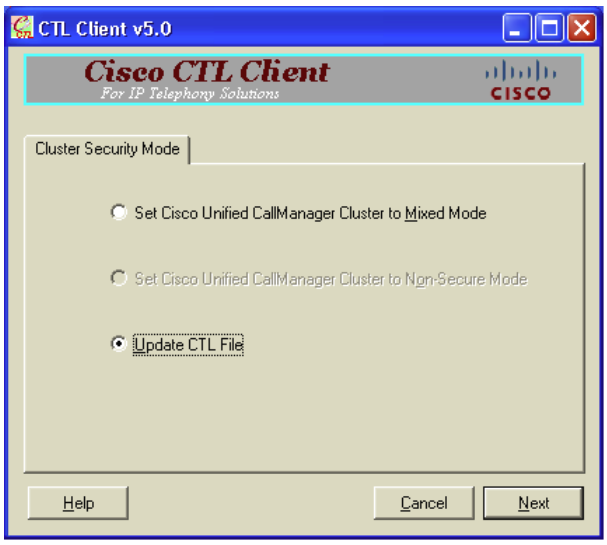
1. Start CTL Client :



- Don’t use CUCM name, use IP address only.
- Port by default should be 2444
- User name and Password are CUCM user names and password.

2. CTL will authenticate user and will connect to CUCM.

3. Following screen will be rendered. At this point, select “Set Cisco Unified CallManger Cluster to Mixed Mode”. Select Next



4. Client will prompt to add secure token. At this time insert token to USB port of CTL client installation server.

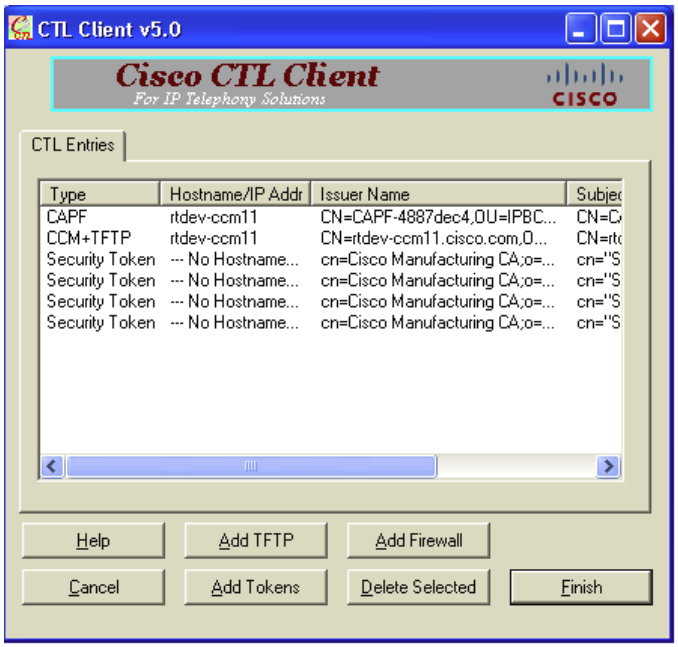
5. CTL client will prompt for token password. Use password e.g. “Cisco_xyz” from the top of stickers.

6. Be very careful with password entry. **Two wrong password entries will make token unusable.**

7. Process will end with FINISH option, and ask to add another token.

8. Follow the same steps as followed earlier and select NEXT/FINISH

9. At the end of this exercise you will see two entries for security token along with CAPF and CCM TFTP line items, as shown below. **Caution: You will see only two security tokens, while picture has four security tokens.**



10. Close CTL Client.

11. Make sure to RESTART CUCM and TFTP services from CUCM serviceability page.

6.2 Exporting CUCM certificates to S3

Download a Certificate or CTL

To download a certificate or CTL from the Cisco Unified Communications Operating

System to your PC, follow this procedure:

1. Navigate to Security>Certificate Management.
   The Certificate List window displays.

2. You can use the Find controls to filter the certificate list.

3. Click the file name of the certificate or CTL.
   The Certificate Configuration window displays.

4. Click Download.

5. In the File Download dialog box, click Save.

6.3 Importing S3 certificates to CUCM

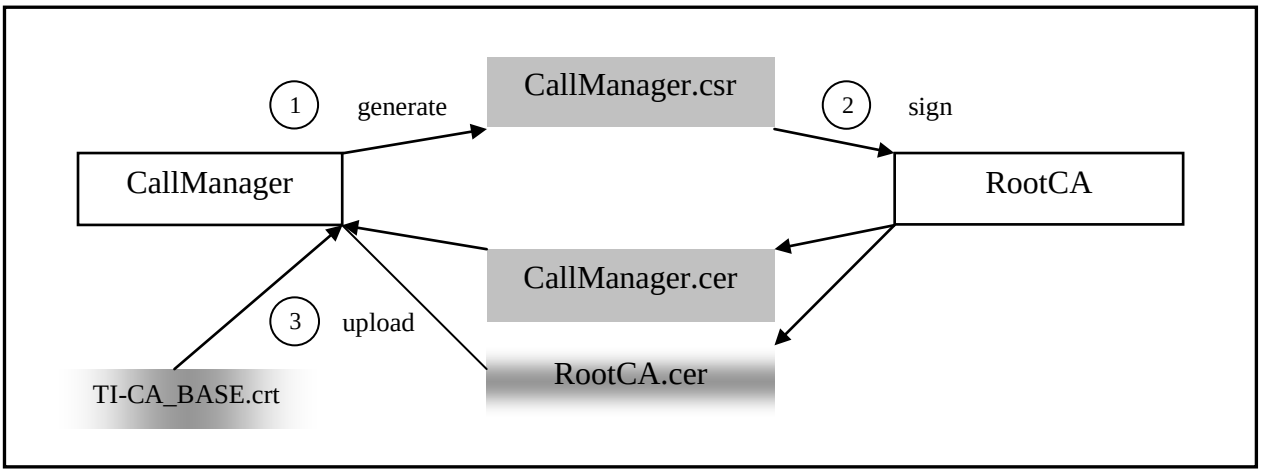
I. The S3 CA that signs the S3 device certificates needs to be imported in the CUCM trust store. Please see the “Security” section in the CUCM OS Admin Guide (http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cucos/7_0_1/cucos/os_701_cm.html) to check how to import a certificate into the CUCM trust store.

II. S3 CA credentials upload on CUCM: The file "xxxxx" should be uploaded to the call-manager and categorized as a "trusted" certificate.
OS Administration; Security; Certificate Management
Upload Certificate
Certificate Name: Callmanager-trust
Root Certificate (can leave blank)
Upload File: <file siptcl_ca_cert.pem>
If multiple call-managers are in a "cluster" configuration, then the "xxxxx" must be applied to all call managers in the cluster.

7 A common third party Certificate Authority for CUCM and S3 or S6

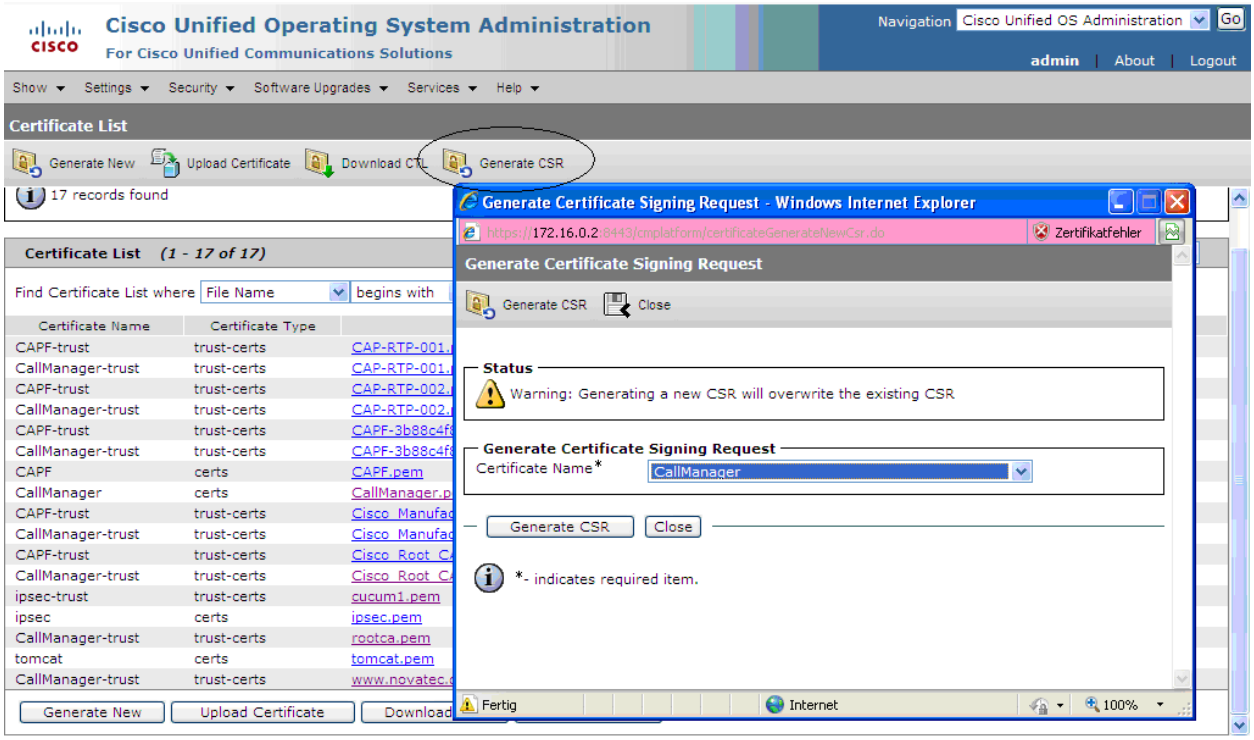
This chapter demonstrates the workflow to establish a common RootCA for a Cisco CallManager and a S3 respectively a S6.

7.1 Replace a self signed CUCM certificate by a third party signed one



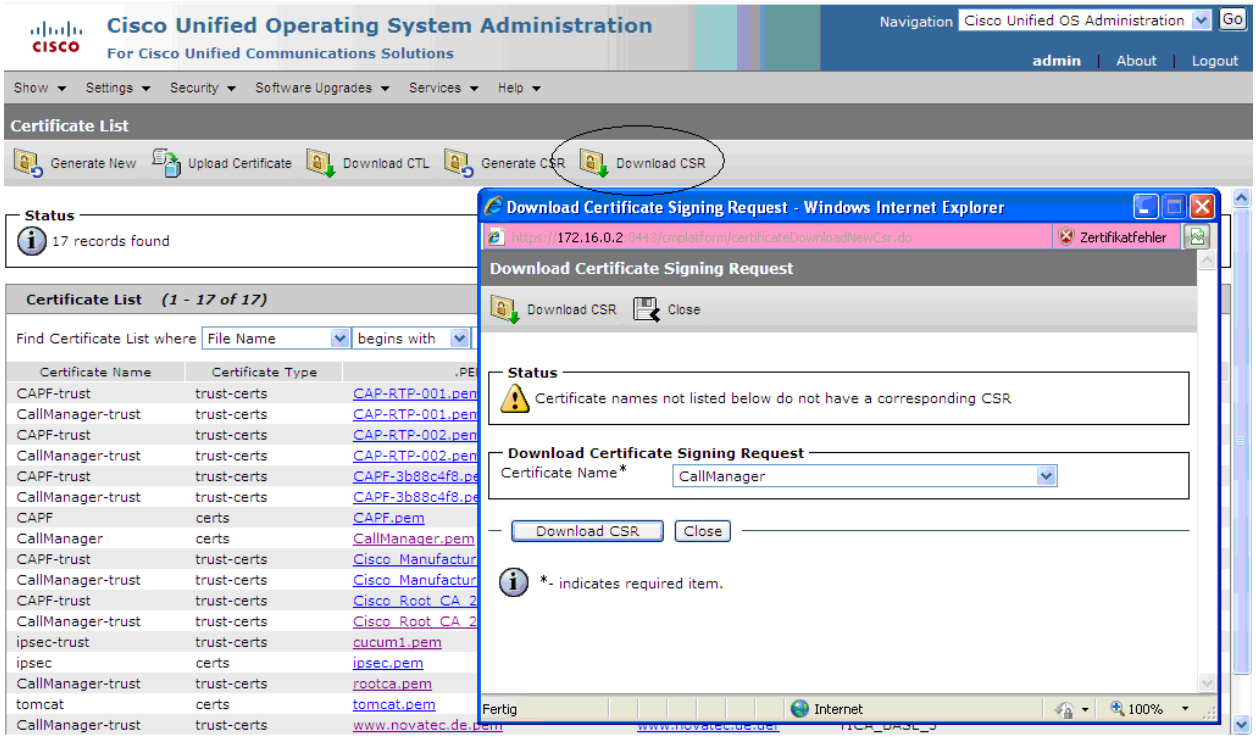
7.1.1 Generate a new CUCM certificate-request

Go to Cisco Unified OS Administration.



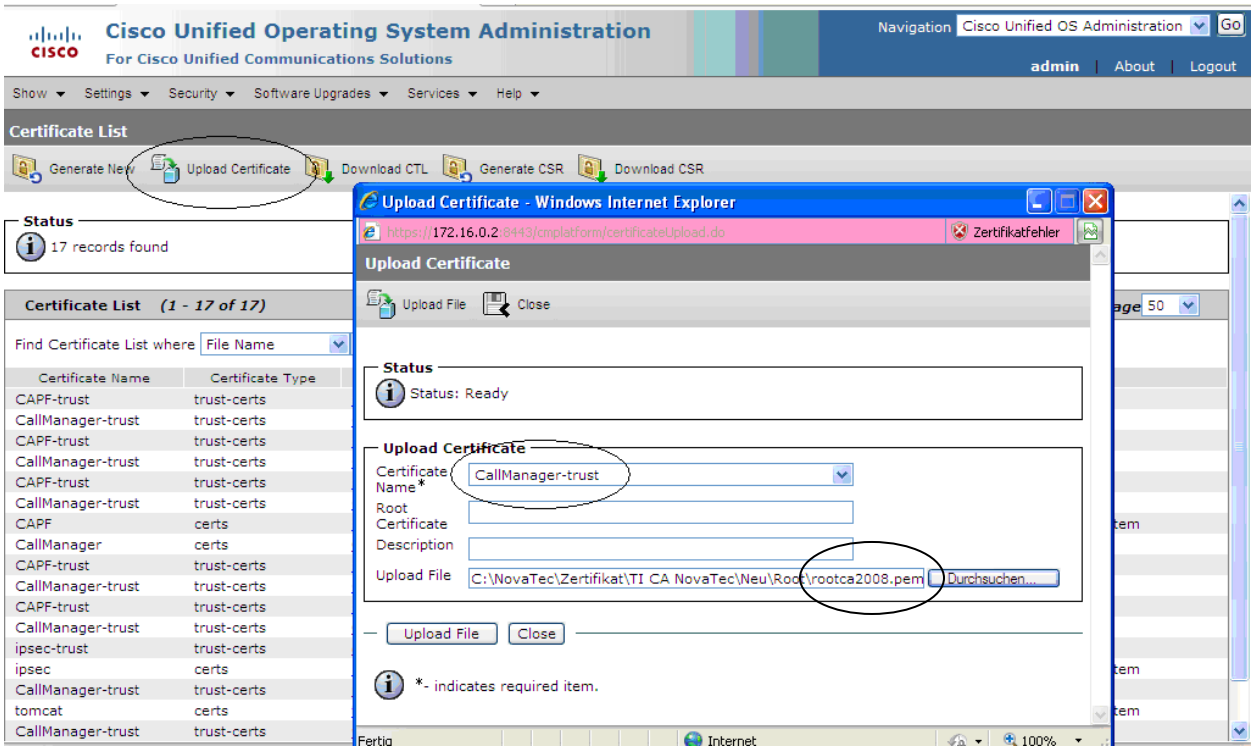
7.1.2 Download a generated certificate request from a CUCM

Download the new request from the CallManager.
Let the third party CA sign the request.
Obtain the certificate from the CA and the RootCAs certificate.



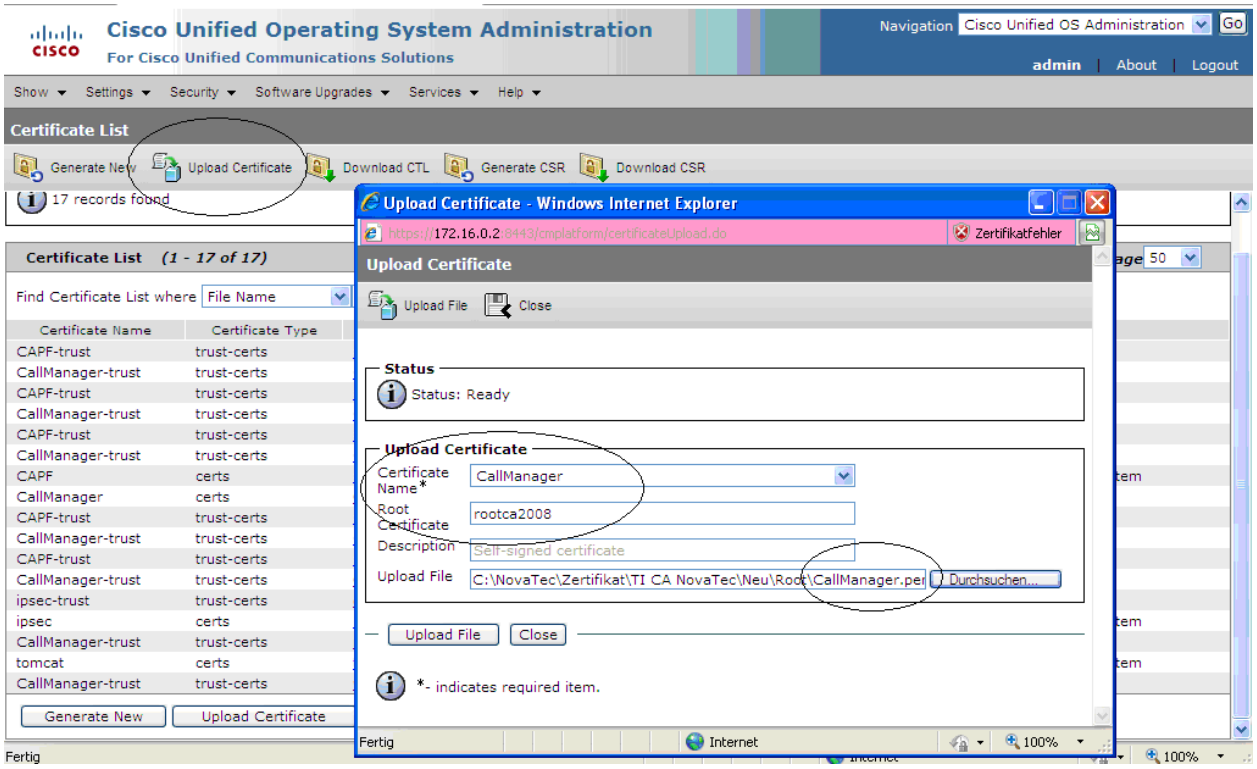
7.1.3 Upload the certificate of the RootCA into CUCM

Select the certificate Name „Callmanager-trust“ to upload the RootCAs certificate.

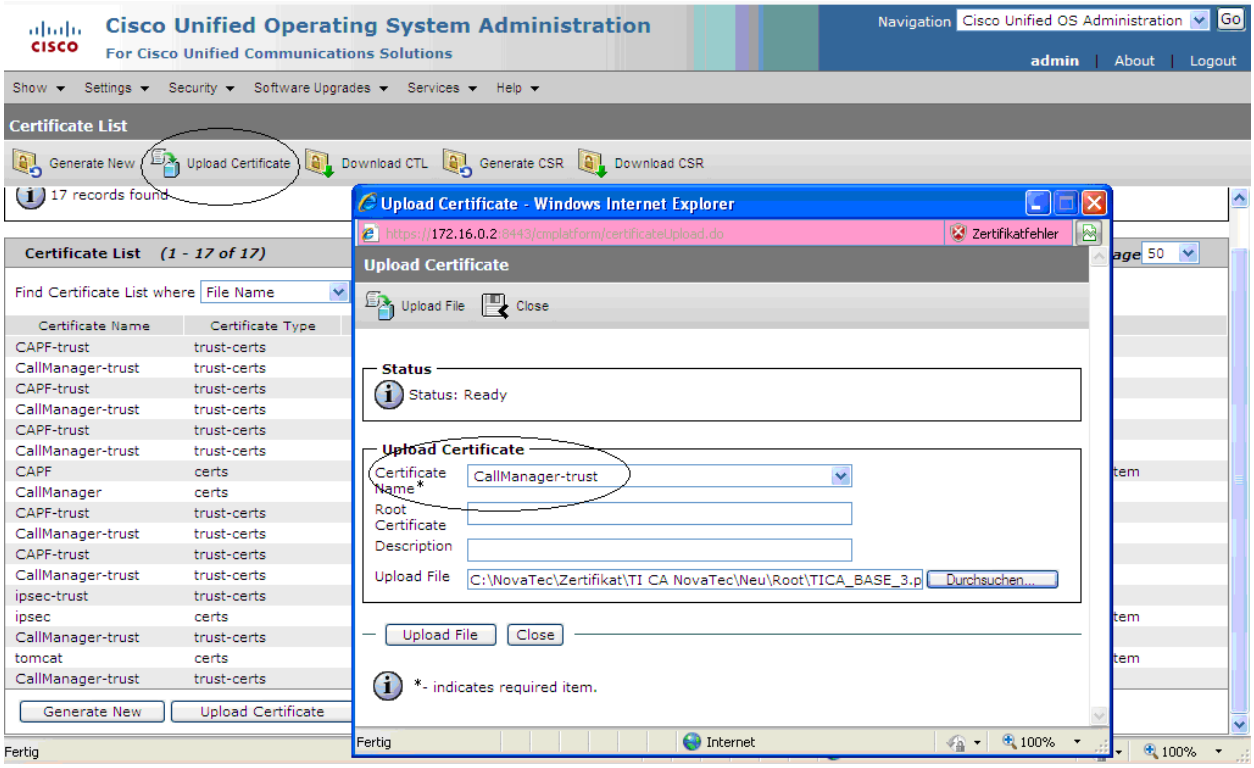


7.1.4 Replace CUCMs self signed certificate

To upload the obtained certificate select Certificate Name „CallManager“ and insert the name of the RootCAs certificate. By referencing to a Root Certificate, the now imported certificate will replace the old CallManager certificate.



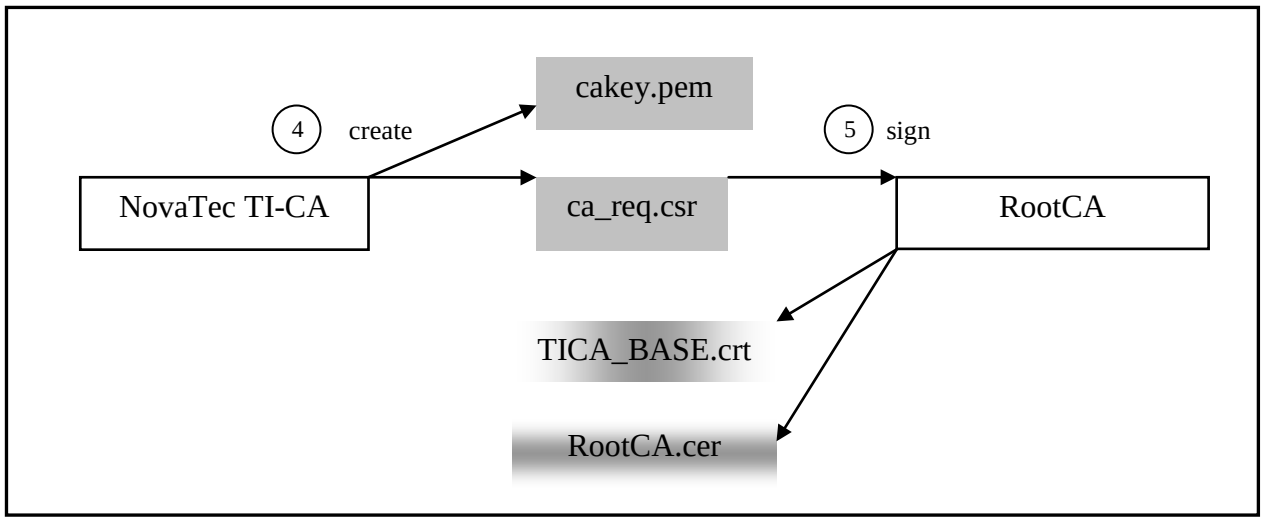
In addition upload a TI-CA_Base certificate (see chapter 7.2) into CUCM.



7.2 Replace a self signed TI-CA certificate by a third party signed one

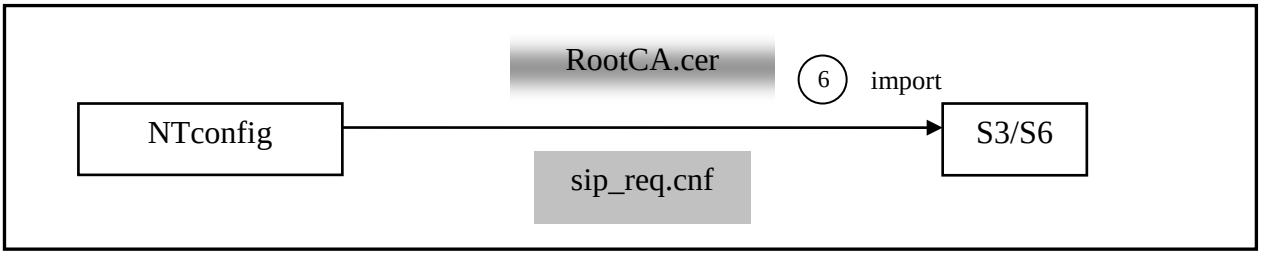
See chapter 3.1 to create a certificate request for a S3 or S6.

Let the third party CA sign the request.
Obtain the certificate (here called TI-CA_BASE) from the CA and the RootCAs certificate.



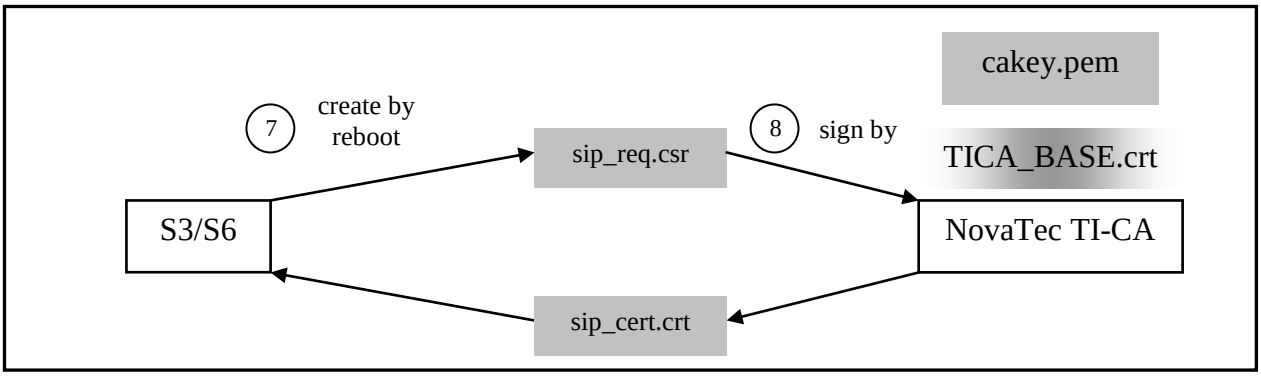
7.3 Import a third party RootCA certificate into a S3 or S6

See chapter 3.2 to load the RootCAs certificate into a S3 or S6.

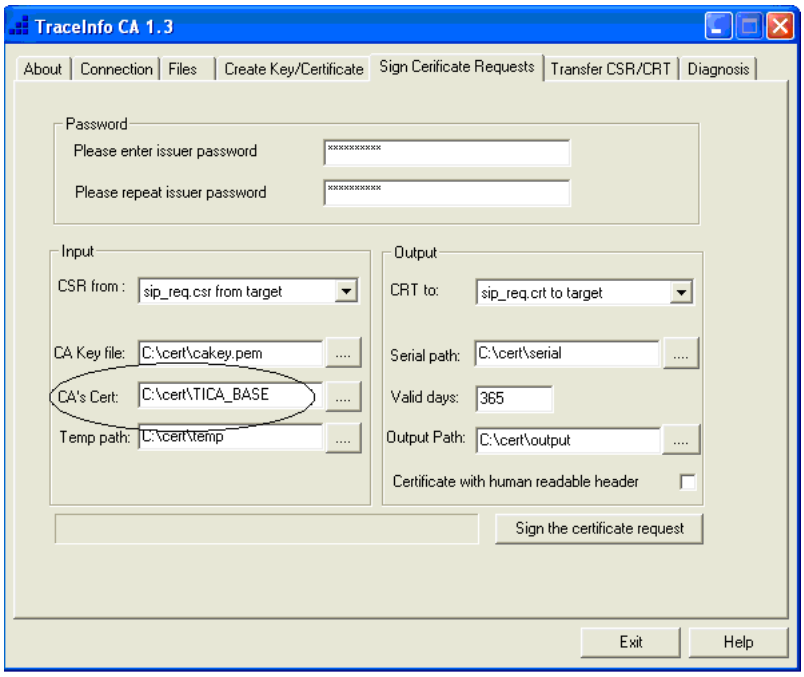


7.4 Sign a S3 or S6 SIP certificate by a third party signed certificate

See chapter 3.3 to sign the SIP certificate by the third party certificate called TI-CA_BASE.

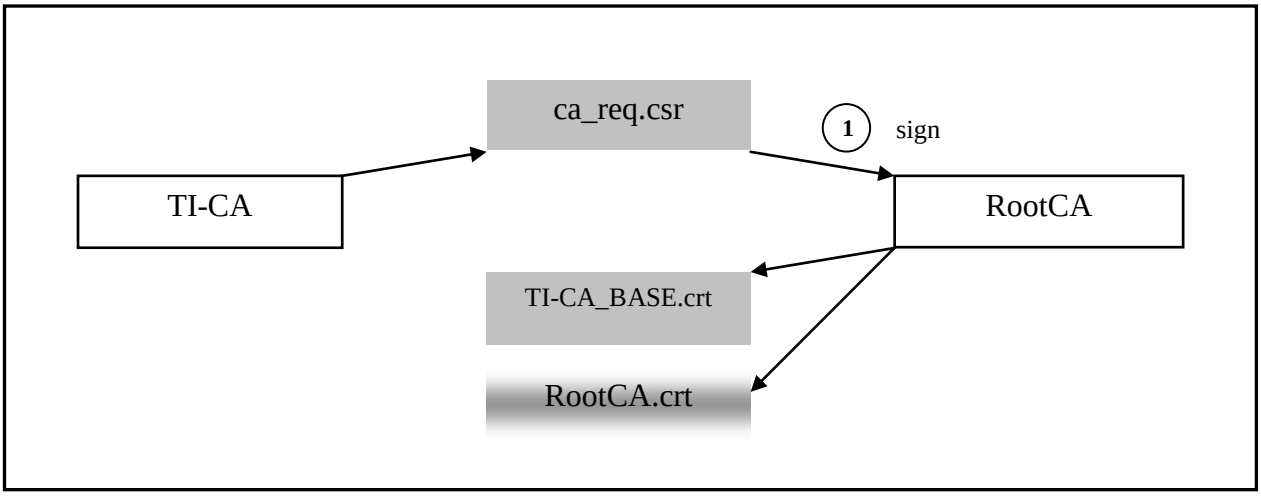


Here select TI-CA_BASE instead of ca_cert.



8 RootCA signs TI-CA:

- TI-CA creates a private key (cakey.pem 2048 bit) and a request (ca_req.csr). The request will be signed by RootCA. RootCA issues three certificates: in Base64, DER and P7B format.
- The certificate in Base64 contains a PUBKEY from TI-CA and a PUBKEY from RootCA.
- The certificate in P7B contains two certificates: a TI-CA certificate as described above and a self-signed root certificate from RootCA.

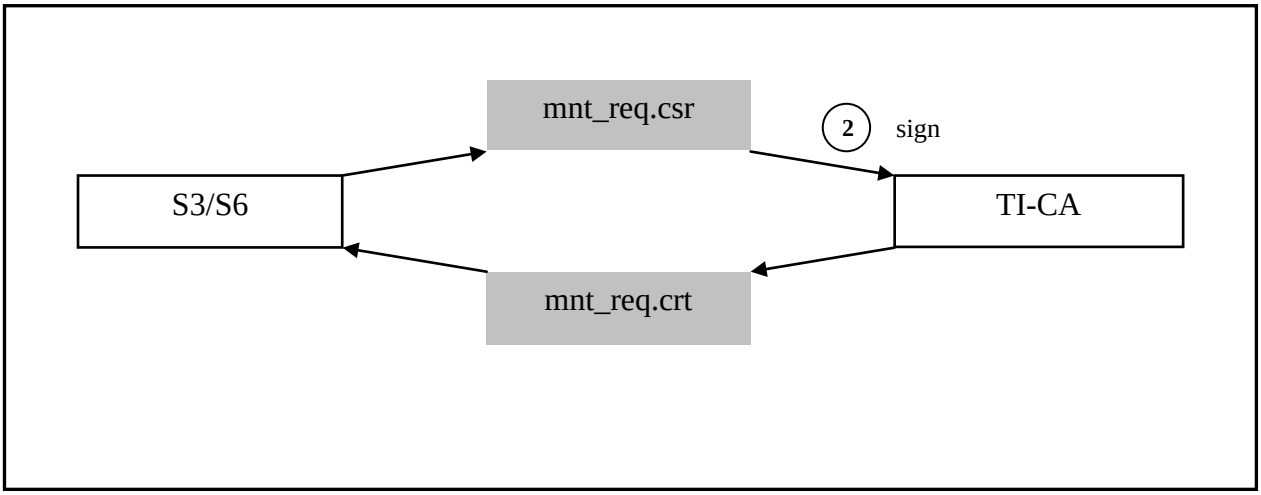


9 TI-CA signs Novatec Gateway MNT:

- If the Novatec Gateway MNT is adequately configured, i. e.
  - enable TLS security,
  - Tls.lic is loaded,
  - the config data for its Key/Request is available,

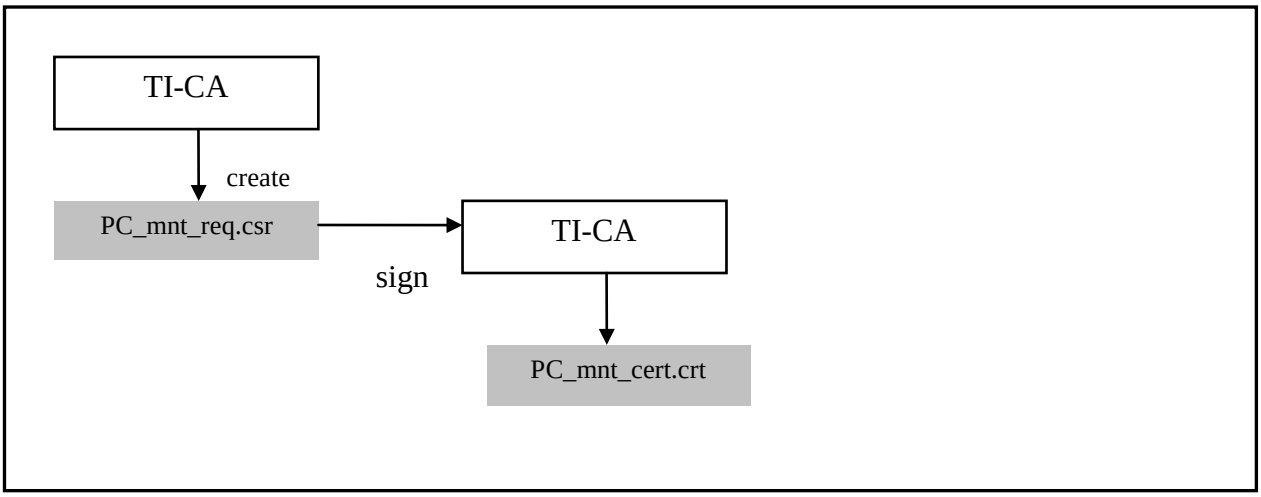
  then the NovaTec Gateway creates a private key and a request (mnt_req.csr) after the reboot.

- The request (mnt_req.csr) in the NovaTec Gateway can be signed by TI-CA. The signed certificate remains in the NovaTec Gateway.



10 On the PC side: create and sign a request:

- A request (PC_mnt_req.csr in 1024bit) can be created with TI-CA in the PC.
- The created request, PC_mnt_req.csr, can again be signed with TI-CA => PC_mnt_cert.crt.
- The signed certificate (PC_mnt_cert.crt) can now be used by all PC clients to communicate with the NovaTec Gateways.



11 Import of CA certificates:

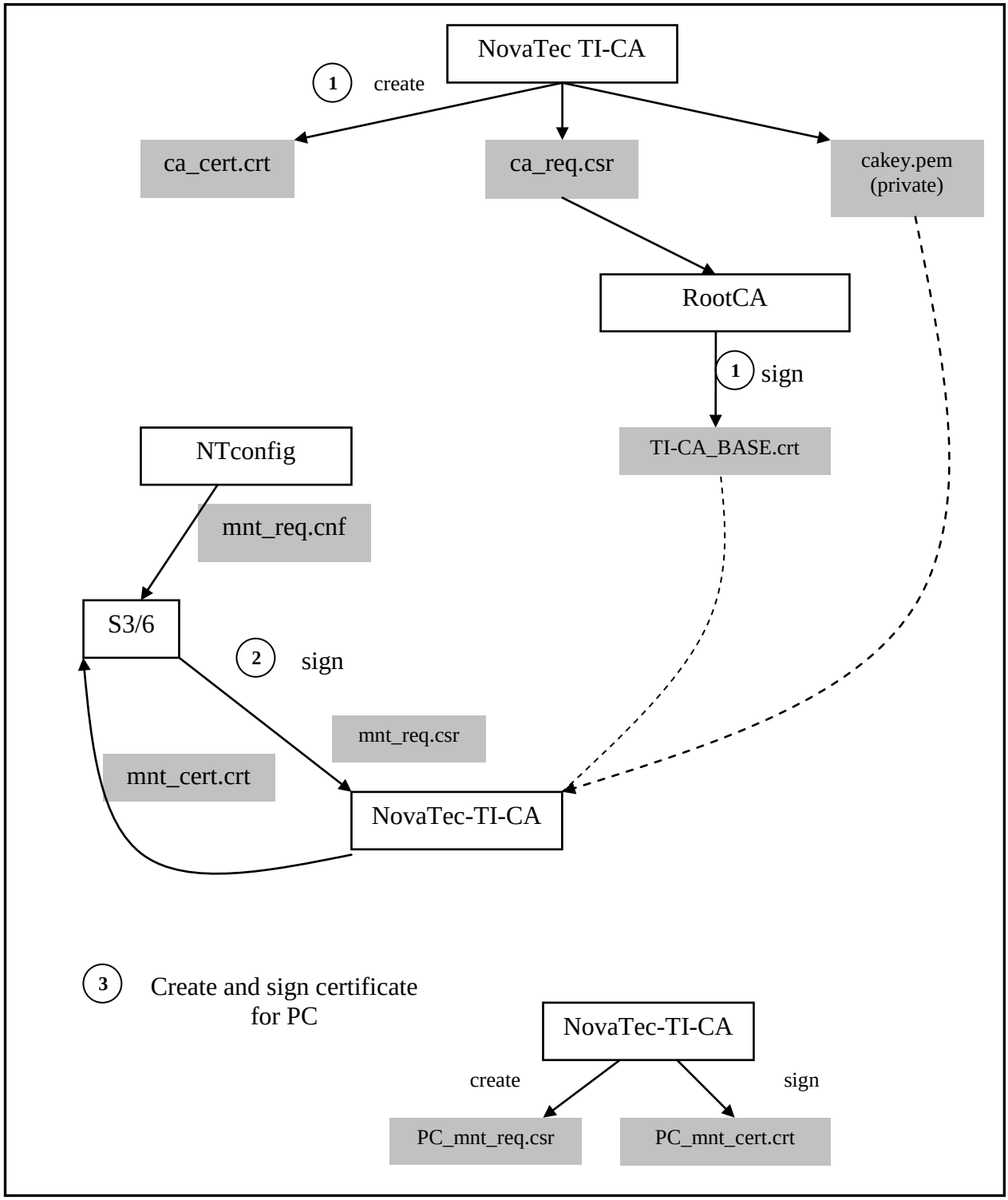
Option 1
To be able to validate a Certificate Chain continuously to the Root, the NovaTec Gateway and the PC Client only need the self signed certificate from TI-CA as they find the “Common CA” there.

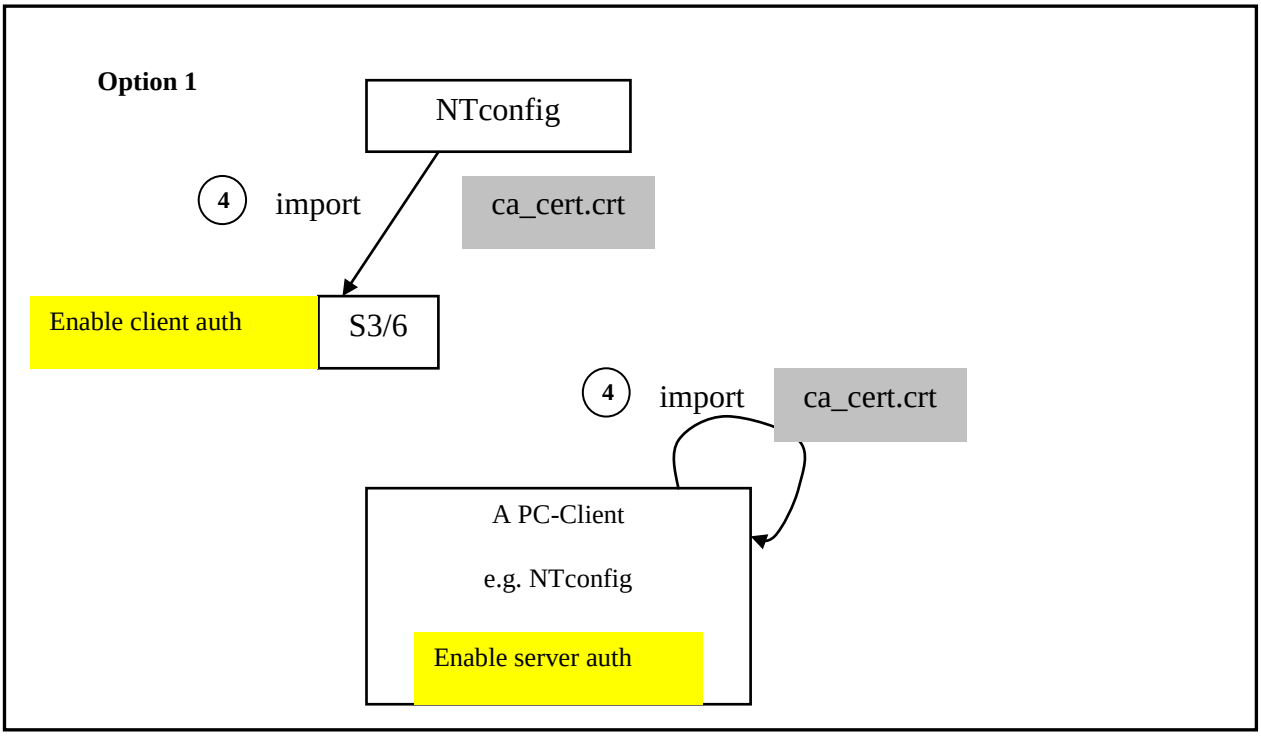
Opton 2
To be able to validate a Certificate Chain continuously to the RootCA (Server 2008), the NovaTec Gateway and the PC Client need the self-signed certificate from RootCA and the TI-CA-BASE.crt signed by the RootCA.

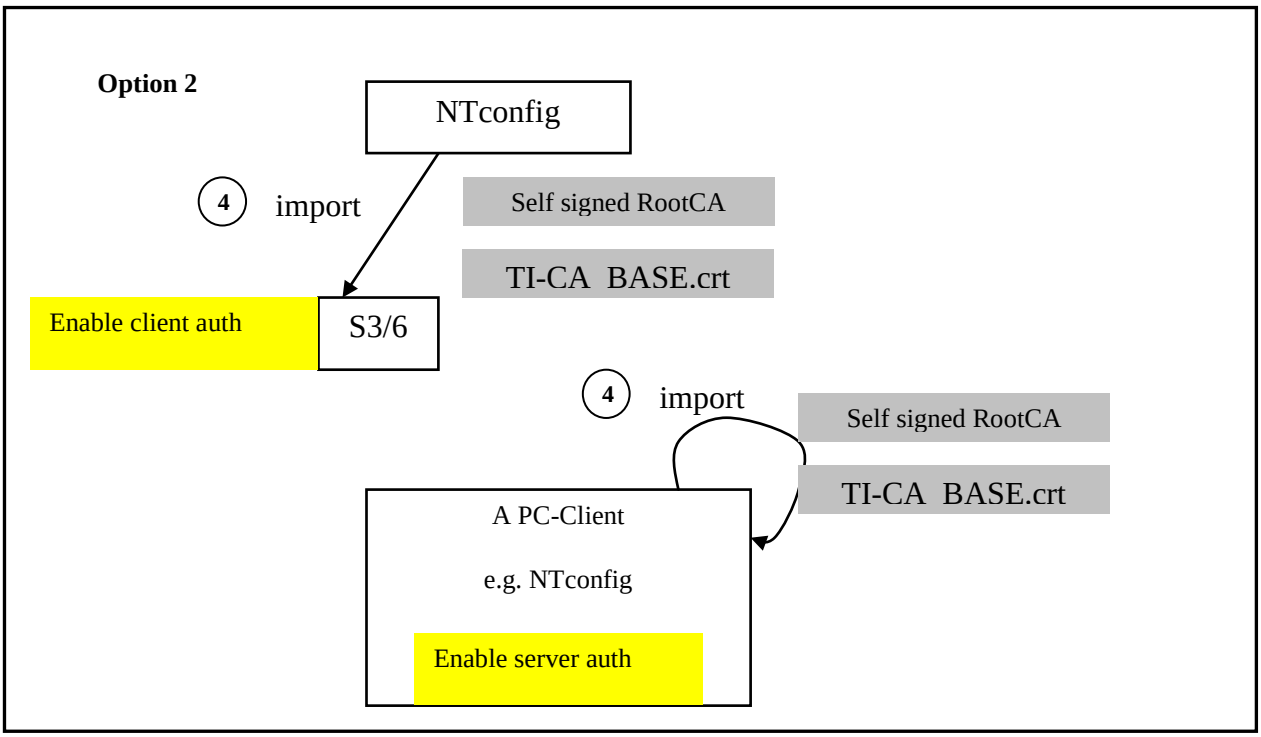
Note:
- The import of CA certificates to the NovaTec Gateway is realised with NT-Conf.
- The import of CA certificates to the PC Client is realised via a „TLS Settings“ window in GUI.
- The setting of the flag „Client-Authentication“ in the NovaTec Gateway is realised with NT-Conf.
- The setting of the flag „Server-Authentication“ in the PC-Client is realised via a „TLS Settings“ window in GUI.
- Option 2 does not work with NMP 6.4 as NMP 6.4 currently supports one-level validation. It malfunctions when an authentication check is made during the connection establishment.

12 Workaround for option 2:

As stated before, option 2 does not work with NMP 6.4 up to now. However, if the „Server-Authentication“ flag is NOT set in the PC Client, then the server authentication check will not be executed and a connection can be established.




Option 1
NTconfig
4
import
ca_cert.crt
Enable client auth
S3/6
4
import
ca_cert.crt
A PC-Client
e.g. NTconfig
Enable server auth


Option 2
NTconfig
4
import
Self signed RootCA
TI-CA BASE.crt
Enable client auth
S3/6
4
import
Self signed RootCA
TI-CA BASE.crt
A PC-Client
e.g. NTconfig
Enable server auth

Establish a TLS secured MNT connection from PC-Client to S3/S6

S3/S6		E.g. NTConf
	← Client Hello	
Server Hello, *Cerificate (mnt_cert.crt signed by TI-CA_BASE.crt)*, Certificate Request	→	
	← *Cerificate (signed by Server_2008)*	
	.	
	.	