

Operating manual

Installation/Configuration Handbook for TLS and sRTP

for NovaTec systems

Doc-ID	DB.HBTLSSRTP-.NT
Version	3.5
Datum	31.10.2014
Status	Final

Copyright 2014 NovaTec Kommunikationstechnik GmbH

Propagation, copying, utilization, saving or publication of this document or its contents in parts, excerpts or in total is forbidden unless explicitly permitted in written form.

Violations will cause indemnities.
All rights reserved.



CONTENTS

1	Introduction – What can be secured with NovaTec systems?.....	4
2	Overview – Handling certificates.....	5
2.1	TLS connection establishment in overview	8
2.2	Installing the TLS certificate in the gateway	9
2.3	TLS connection establishment with one certificate authority	10
2.4	TLS connection establishment with two certificate authorities.....	11
3	Preliminaries	12
3.1	Activating encryption in NovaTec systems	12
3.1.1	Up to NMP version 00.07.03.00	12
3.1.2	From NMP-Version 00.07.03.00	13
3.2	The TraceInfo-CA	15
3.2.1	The basic capabilities of the TraceInfo-CA.....	16
3.2.1.1	Creating a CSR	16
3.2.1.2	Signing the CSR your self.....	17
3.2.1.3	Signing the CSR externally	18
3.2.2	Plain text in certificates	19
3.2.3	Generating the root certificate and key	20
3.3	Configuring SCEP on a Windows server.....	22
4	Configuration	23
4.1	Securing VoIP channels with sRTP	23
4.2	Securing SIP with TLS.....	25
4.2.1	System IP options - enable security	25
4.2.2	Generating a certificate request.....	26
4.2.3	Loading the CA certificate into the trust list	27
4.2.4	SIP-TLS User Mapping – CUCM Trunk	29
4.2.5	SIP-TLS Local Mapping – CUCM Trunk	30
4.2.6	SIP-TLS Optional Flags	31
4.3	SCEP	32
4.3.1	Adjustments for the use of SCEP	32
4.3.2	Registration Authority Certificates.....	33
4.3.3	CA chain	34
4.3.4	Challenge Password.....	35
4.4	NAMES	37
4.4.1	NAMES as CA	38
4.4.2	Secured connection to the gateway	39
4.5	Securing maintenance / call home	40
4.5.1	TI-CA requires a root certificate.....	41
4.5.2	Generating maintenance and call home CSR	41



4.5.3	TI-CA signs MNT- & NMS-CSR	42
4.5.4	Configuration of MNT- & NMS-CSR	43
4.5.5	Creation of MNT- / NMS-CSR.....	46
4.5.6	TI-CA signs the MNT or NMS certificate	46
4.5.7	Loading externally signed MNT- & NMS-CRT into the gateway.....	47
4.5.8	Performing a reset.....	47
4.5.9	Installing MNT- & NMS-CRT on the PC side	48
4.6	Deactivating TLS and sRTP	50
4.6.1	Turning off encryption for SIP and Maintenance	50
4.6.2	Changing the IP transport service.....	51
4.6.3	Deleting TLS ports and changing from sRTP to RTP	54
5	Creating certificates.....	55
5.1	Signing with TI-CA.....	55
5.2	Signing process with SCEP	63
5.3	Signing systems with NAMES.....	65
6	Configuring secured connections in the CUCM	66
6.1	Installing the CISCO CTL client.....	66
6.2	Activating in configuration.....	70
6.2.1	NovaTec on TRUNK connection	70
6.2.2	NovaTec on a phone connection.....	73
6.3	Importing and exporting certificates	75
6.3.1	Exporting CUCM certificates to a NovaTec system.....	75
6.3.1.1	Downloading a certificate from a CUCM	75
6.3.2	Importing a NovaTec certificate into the CUCM	77
6.4	External CA signs Call Manager	78
6.5	Deactivating in the configuration	80
6.5.1	Deactivating TLS and sRTP for a CUCM trunk	80
6.5.2	Deactivating TLS and sRTP for a CUCM line.....	82
7	Appendix	83
7.1	State of LED signals during the signing process	83
7.2	Changeover between 1024/2048 bit RSA key	85
7.3	SCEP application.....	87
7.3.1	NovaTec SCEP implementation	87
7.3.2	SCEP trace output	89
7.4	List of abbreviations	90
7.5	List of illustrations	91



1 Introduction – What can be secured with NovaTec systems?

NovaTec gateways provide secure communication channels for all three instances (Maintenance, SIP, CallHome). The connection via SIP is secured with TLS. The VoIP channels for speech and/or data transfer are encoded with sRTP. In addition to this all connections for configuration and maintenance of the gateways can also be secured with TLS.

The systems use SSL certificates with X.509 standard to verify the authenticity and integrity of the communication partner. These certificates can be generated respectively signed with the NovaTec certification tool "TI-CA", the NovaTec Administration and Management Element Server (NAMES) or by third parties. Certificates may also be signed via SCEP.

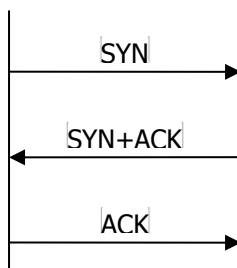
Important: After activating TLS the unsecure access to the systems is blocked. All access requests via V24/UB, ISDN and IP (such as HTTP or TELNET) are denied.



2 Overview – Handling certificates

The tools and procedures as described in this document serve to establish encrypted connections between two partners. Next to the secured speech and data transfer via IP connections with sRTP the following regards the protection of communication channels with TLS. This protocol conducts the necessary exchange of keys and the optional authentication of both of the communication partners with help of certificates. Authentication = Identification of the counterpart by its certificate.

For SIP connections between two gateways or for instance for the connection of the NAME server to a gateway a TCP connection is established first.



Via this TCP channel the TLS handshake protocol is then executed.

The following examines especially the exchange of the certificates.



Steps marked with a * are optional. These depend on configuration.

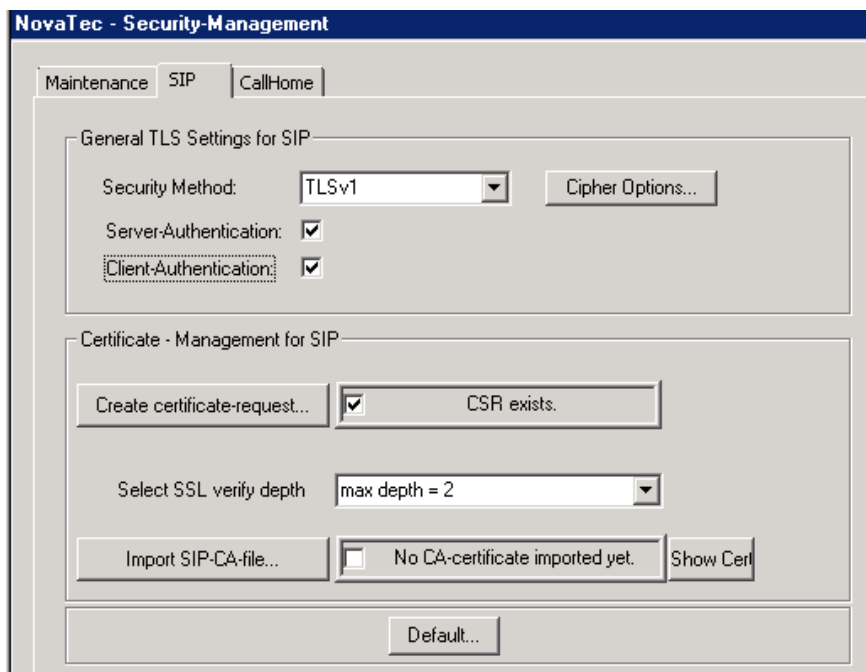


Configuration settings concerning the role during TLS connection.		
Configuration points of the gateways	TLS CLIENT	TLS SERVER
Maintenance		Client authentication
CallHome	Server authentication	
SIP	Server authentication	Client authentication

Configuration points on PC side	TLS CLIENT	TLS SERVER
Maintenance	Server authentication	
CallHome		Client authentication

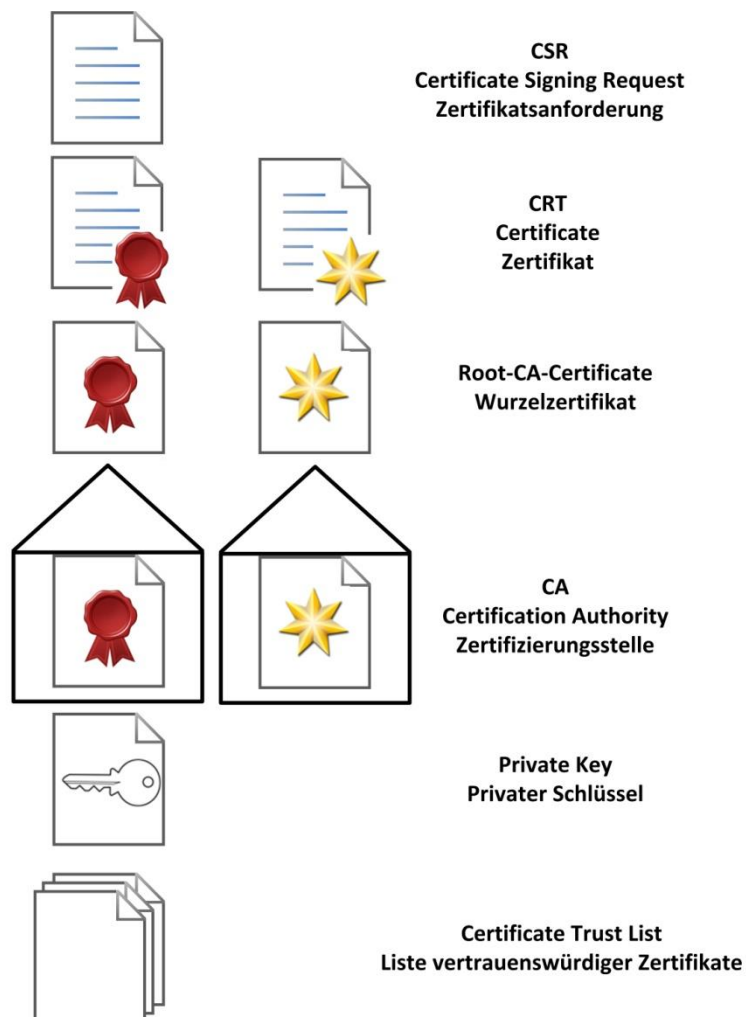
The initiator of a TLS connection, the CLIENT, can verify the SERVER certificate which the SERVER sends to the CLIENT. This verification, e.g. for SIP, is activated with the configuration point „Server-Authentication“. For SIP this point is found under → „System IP options“ → „TLS Security“ → tab „SIP“ (see Picture 1 - Server- / Client-Authentication). If the box „Client-Authentication“ is checked here, the server will demand the client certificate for assessment. In contrast to the instances „Maintenance“ and „CallHome“ the gateways assign both roles when in SIP mode. If a TLS secured call is built up by a gateway, the gateway is the client. If a SIP call arrives at a gateway, it is the TLS server. For a maintenance connection a gateway is always the server as the other party, e.g. NAMES or TI-CA, begins the buildup of the TLS connection. In contrast to this the gateway is in the role of the TLS client as soon as it builds up a „CallHome“ call. Accordingly for „CallHome“ only „Server-Authentication“ can be activated.

Configuration of the three instances



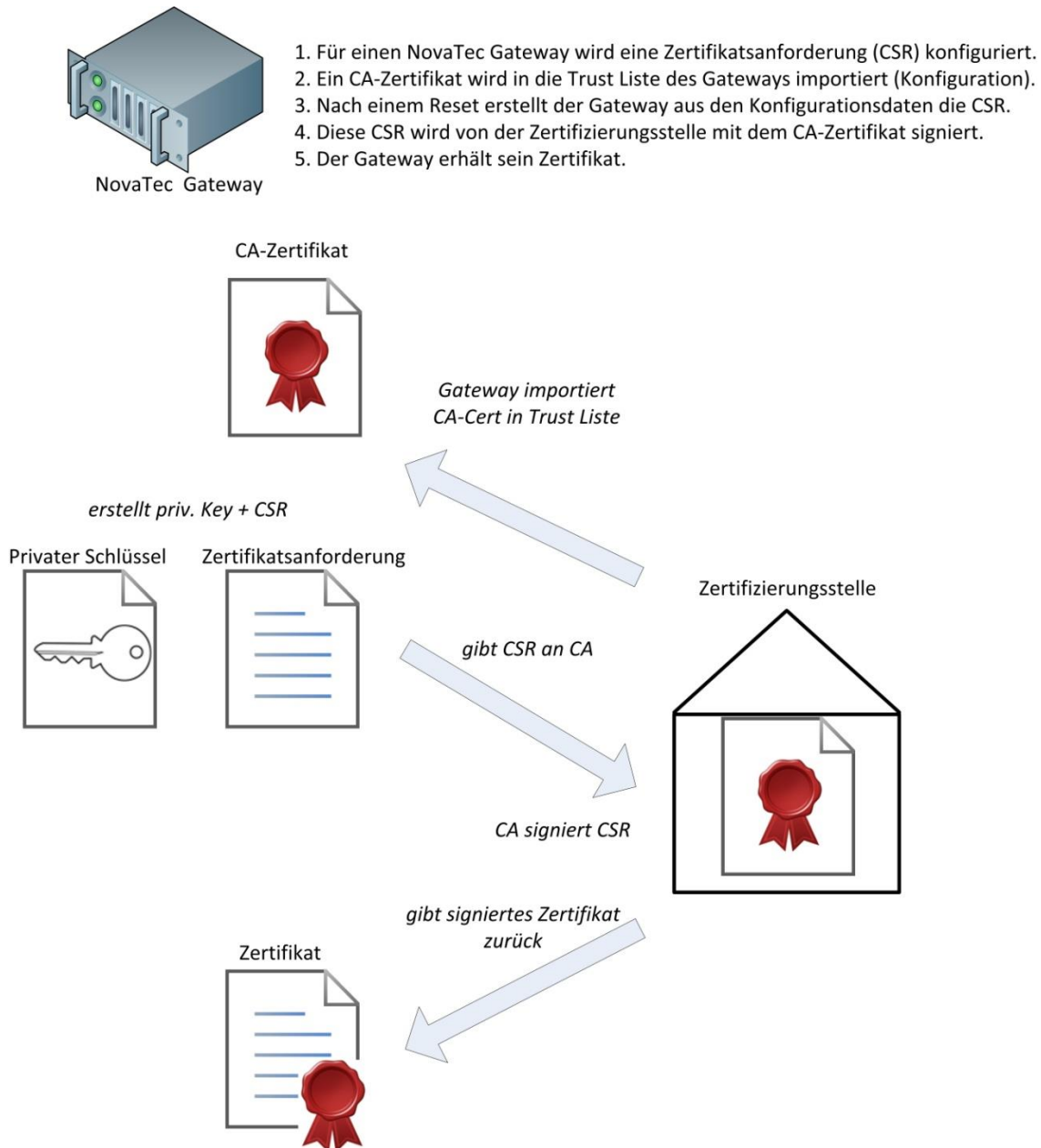
Picture 1 - Server- / Client-Authentication

2.1 TLS connection establishment in overview



Picture 2- Explanation of abridgment diagrams

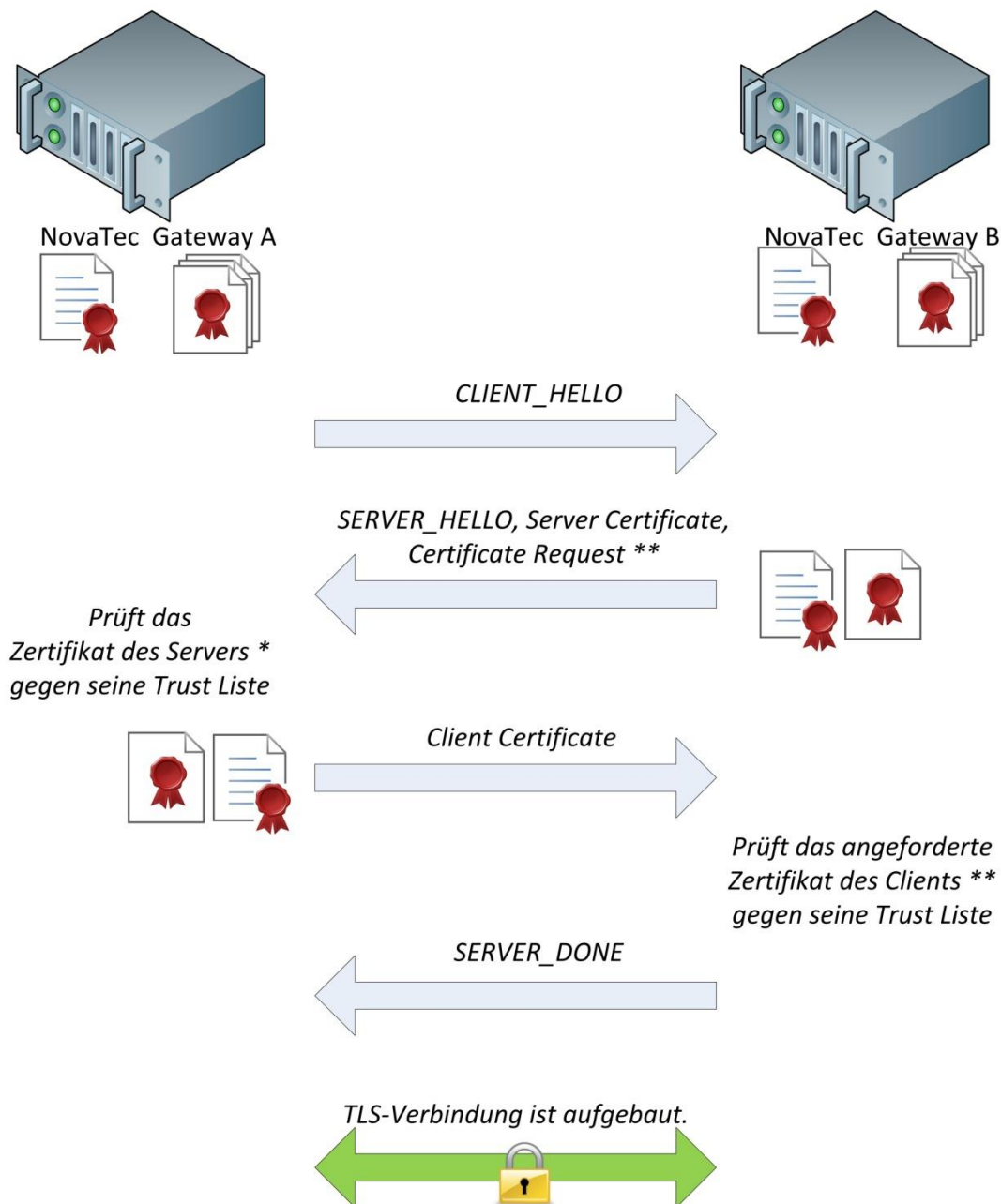
2.2 Installing the TLS certificate in the gateway



Picture 3 – Creation of a TLS certificate of a gateway

2.3 TLS connection establishment with one certificate authority

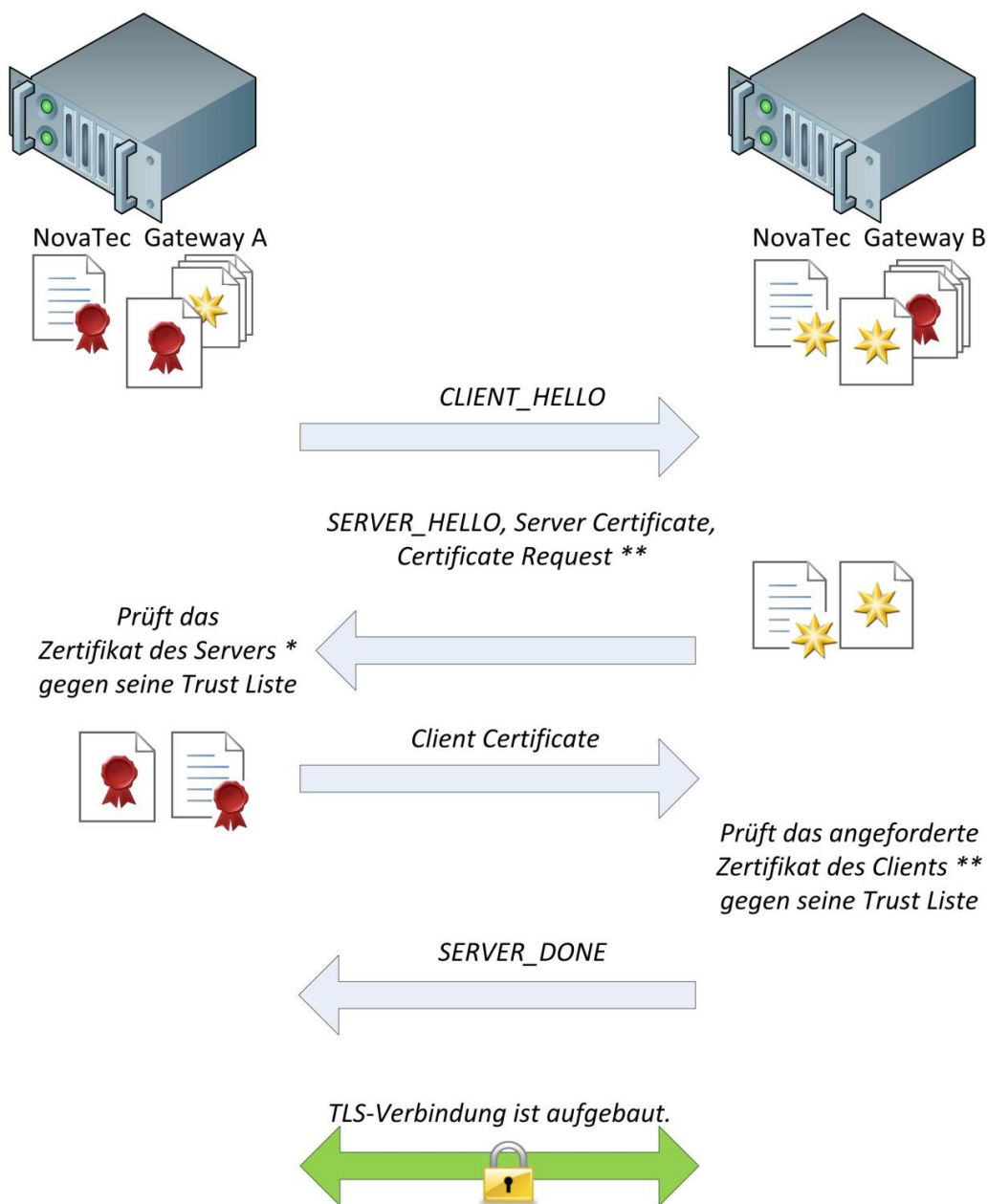
Eine Zertifizierungsstelle hat die Zertifikate beider Gateways signiert.
In der Trust Liste beider Gateways ist das CA-Zertifikat dieser CA gespeichert.
Da in beiden Gateways die Server-Authentication (*) & die Client-Authentication (**) konfiguriert ist, prüft jeder Gateway das Zertifikat der Gegenstelle.
Der Server sendet regulär sein Zertifikat an den Client, und fordert dessen Zertifikat an, um es zu prüfen.
Mit dem CA-Zertifikat in der lokalen Trust Liste, kann die Vertrauenswürdigkeit der empfangenen Zertifikate verifiziert werden.



Picture 4 – TLS connection establishment and one CA

2.4 TLS connection establishment with two certificate authorities

Die Zertifikate beider Gateways sind von zwei unterschiedlichen Zertifizierungsstellen signiert worden. In der Trust Liste der Gateways ist neben dem eigenen auch das fremde CA-Zertifikat abgelegt. Da in beiden Gateways die Server-Authentication (*) & die Client-Authentication (**) konfiguriert ist, prüft jeder Gateway das Zertifikat der Gegenstelle. Der Server sendet regulär sein Zertifikat an den Client, und fordert (**) dessen Zertifikat an, um dieses zu prüfen. Zusammen mit dem TLS-Zertifikat wird jeweils das eigene CA-Zertifikat als Zertifikatskette gesendet. Mit dem externen CA-Zertifikat in der lokalen Trust Liste, kann die Vertrauenswürdigkeit der empfangenen Zertifikate verifiziert werden.



Picture 5 - TLS connection establishment with two CAs

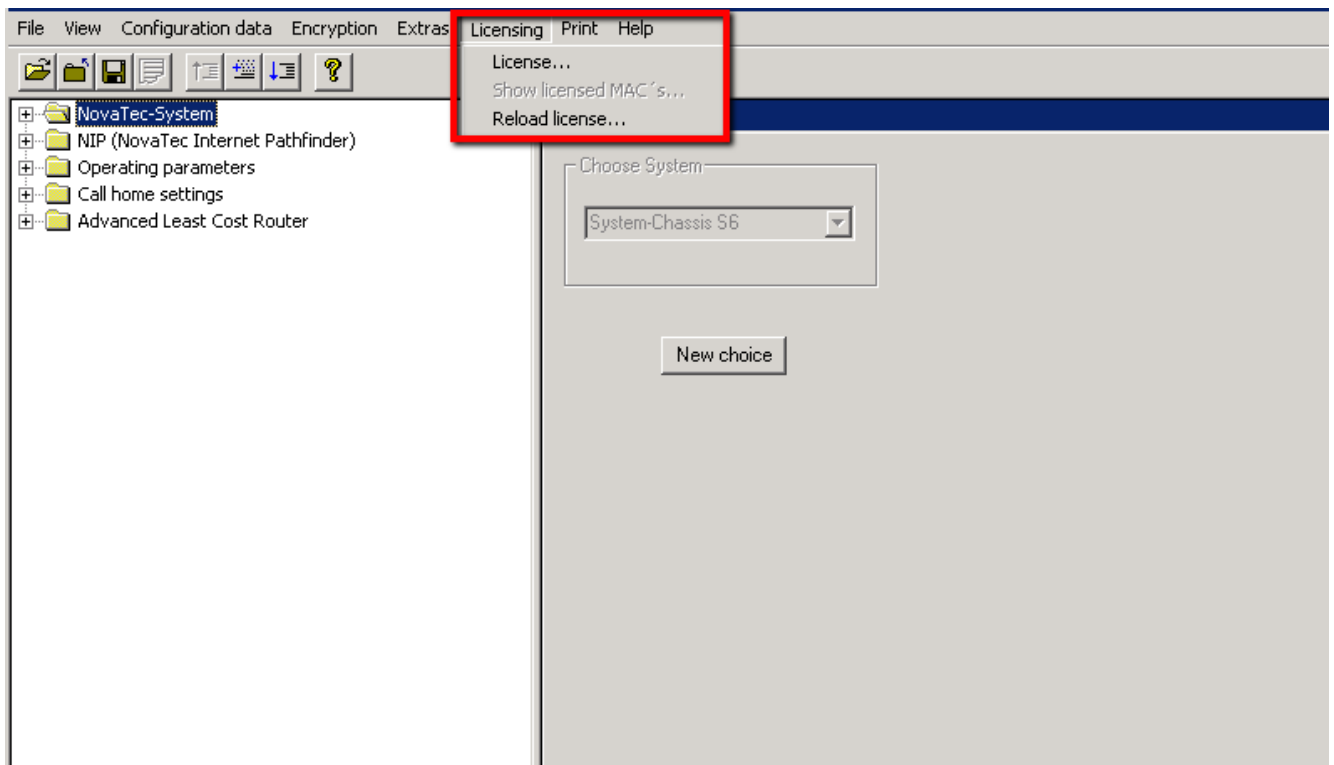
3 Preliminaries

3.1 Activating encryption in NovaTec systems

3.1.1 Up to NMP version 00.07.03.00

Up to NovaTec NMP-Version 00.07.03.00 the separate TLS license „tls.lic“ is necessary next to the firmware license, if you want to activate TLS/sRTP for the system.

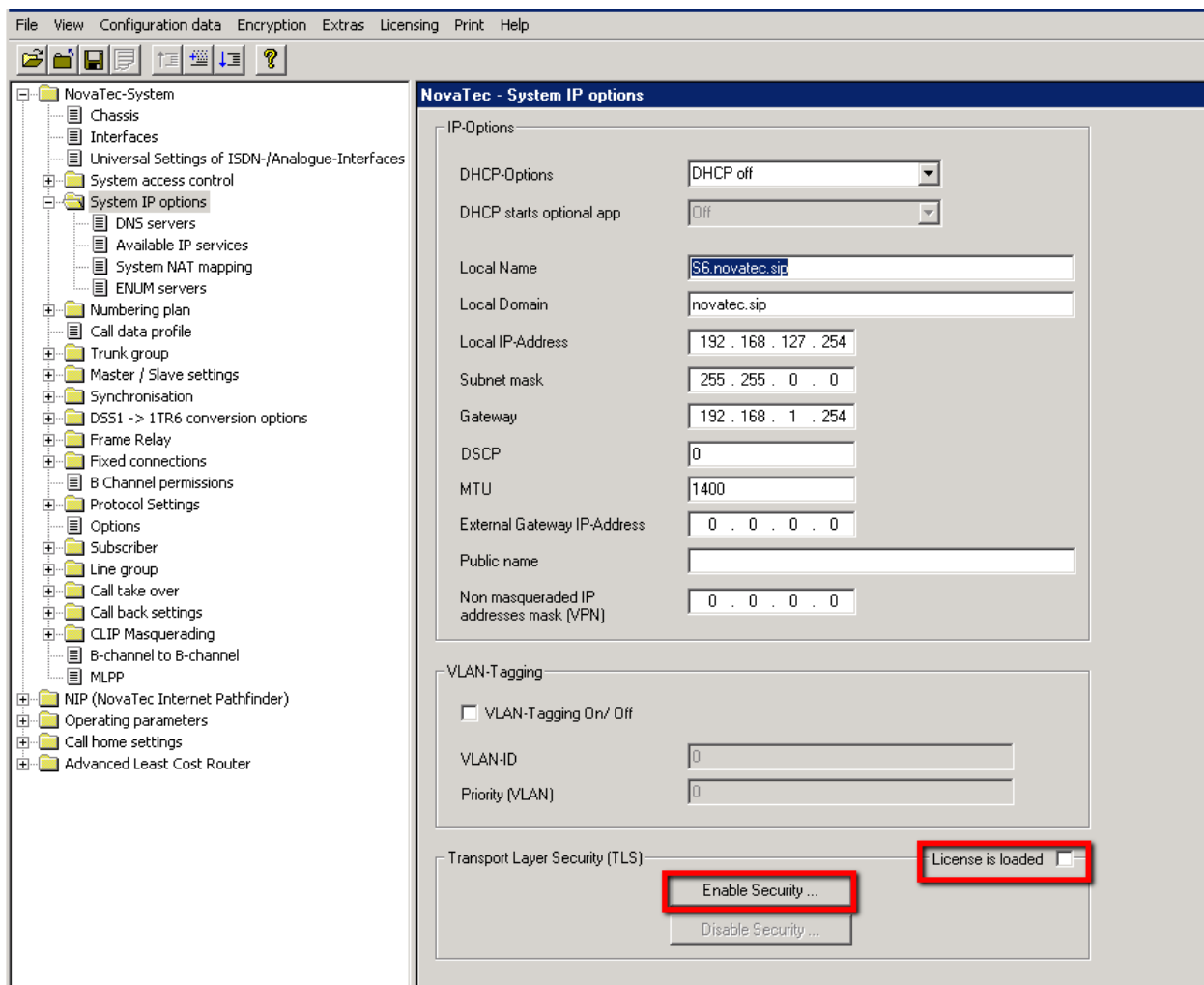
Ask NovaTec for the TLS license. After you have received the „tls.lic“ file from NovaTec , please open the configuration of your system with NovaTec Configuration (from version 7.2.0.4) and upload the TLS license.



Picture 6 – loading the firmware license

Afterwards please select „System IP options“ in the configuration program.

Choose „Enable Security“ at the bottom right and enter the path to the saved file „tls.lic“. Confirm the shown notifications.



Picture 7 - TLS license is loaded

3.1.2 From NMP-Version 00.07.03.00

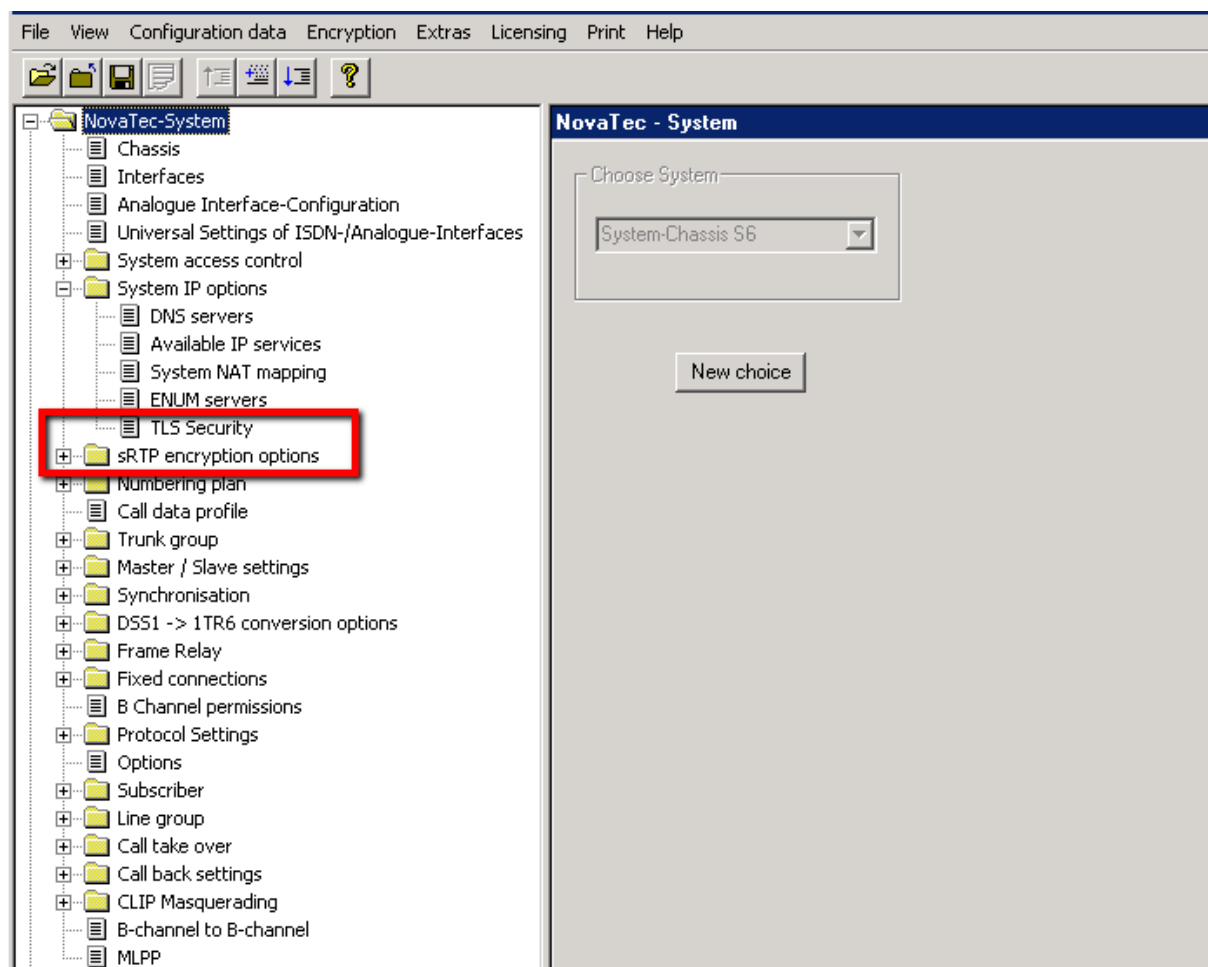
With version 00.07.03.00 a new license management for the protection of the firmware has been introduced. If required you receive your firmware license including activated option "TLS allowed". Please upload your firmware license anew (see chapter 3.1.1 above).

After you have done this please select „System IP options“ in the configuration program.

Now press button „Enable Security“ at the bottom right.

As soon as the box „License is loaded“ is checked, TLS and sRTP are activated.

In the left part of the window now the new node „TLS Security“ is shown within the context menu under the folder "System IP options" and the folder „sRTP encryption options“ is generated.



Picture 8 - TLS Security is licensed

Attention: After the TLS license is uploaded and, in case SIP was configured, some adjustments are made automatically. In the past these had to be made manually. Please check the following adjustments (see also chapter 4.2.4 ff.):

1. „System IP options“ → „Available IP services“: A TCP/IP service for SIP via TLS with port 5061 is installed. The services HTTP and TELNET can now no longer be activated due to security reasons.
2. „NIP“ → „SIP“ → „Mapping lists“ → „User mapping“: Port 5061 is added to the user IP address.
3. „NIP“ → „SIP“ → „Mapping lists“ → „Local mapping“: Port 5061 is added to the registered IP address.

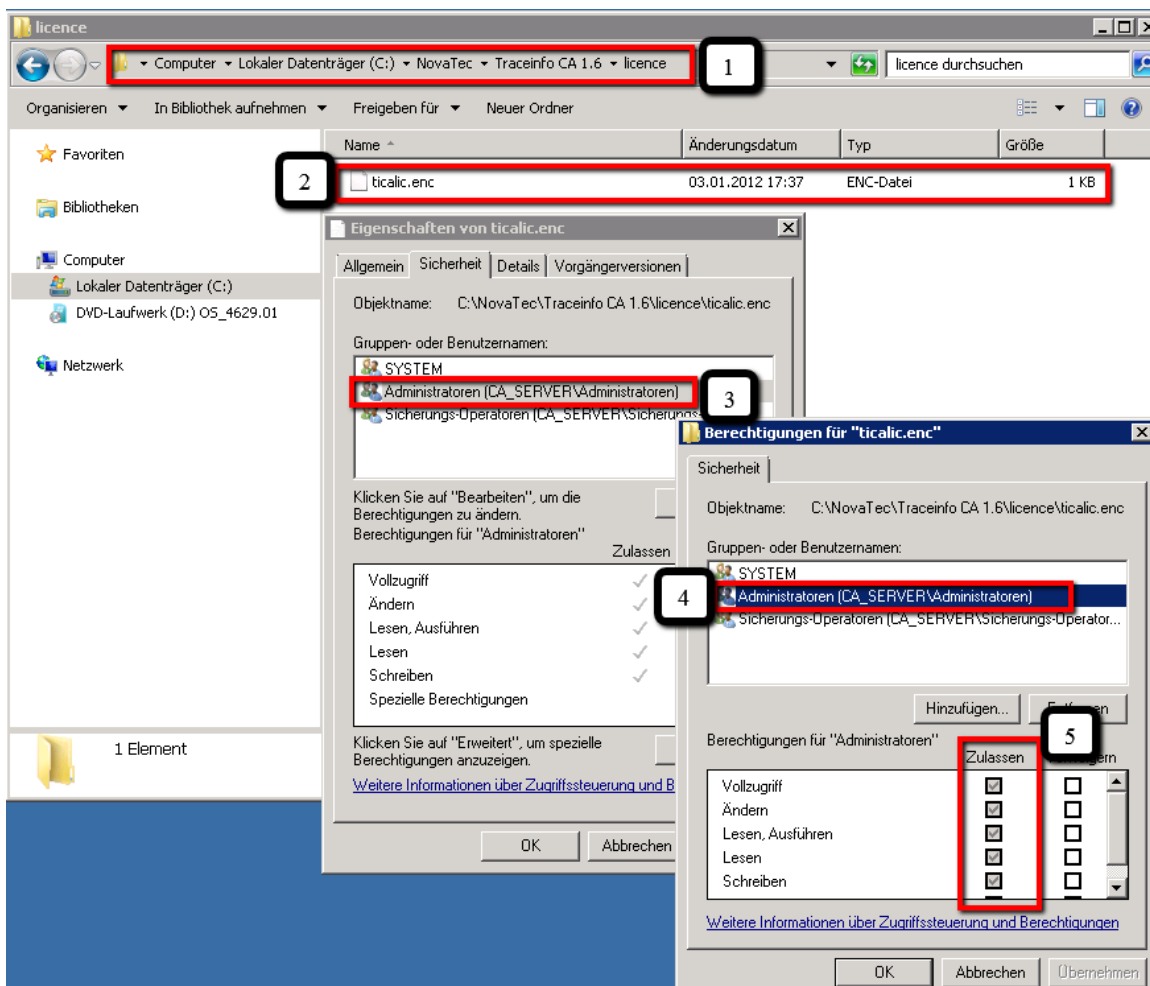
3.2 The TraceInfo-CA

The NovaTec PC application „TraceInfo CA“ is a certification authority (abbreviation: CA). With this CA certificates can be generated and signed.

To start this application a NovaTec dongle is obligatory. Alternatively NovaTec can generate and sign the certificates online.

Please ensure, that only one dongle (e.g. NMS, TI-CA) at a time is connected to the local USB port.

TI-CA requires full access to the file „talic.enc“ on all types of system software. Please find an example for the configuration on a Windows 2008 server below.



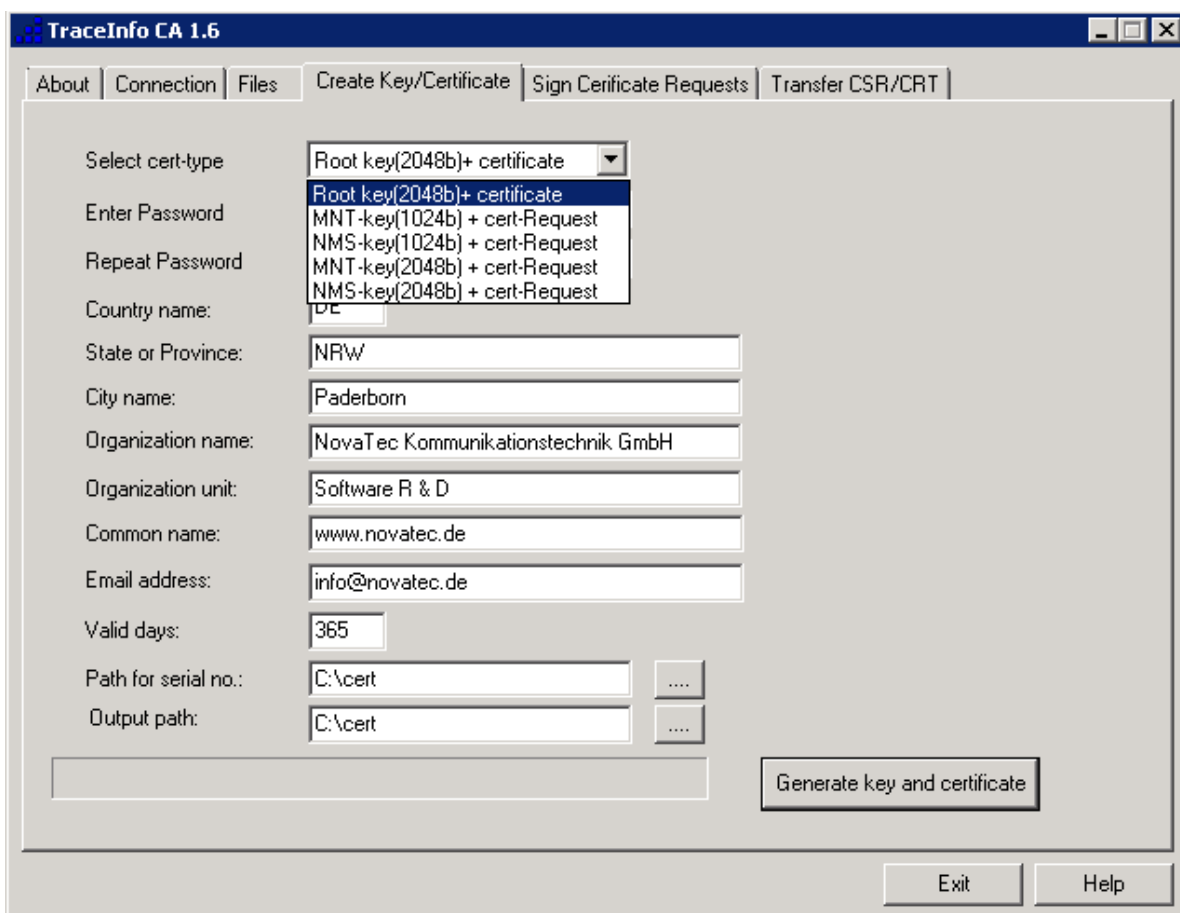
Picture 9 – Configuring TI-CA authorizations

3.2.1 The basic capabilities of the TraceInfo-CA

3.2.1.1 Creating a CSR

Creating a certification request (CSR) including the password secured private key:

- 1) Self-signed ROOT-CA certificate plus CSR and 2048 bit key
- 2) Maintenance-CSR with 1024 or 2048 bit key
- 3) CallHome-CSR with 1024 or 2048 bit key

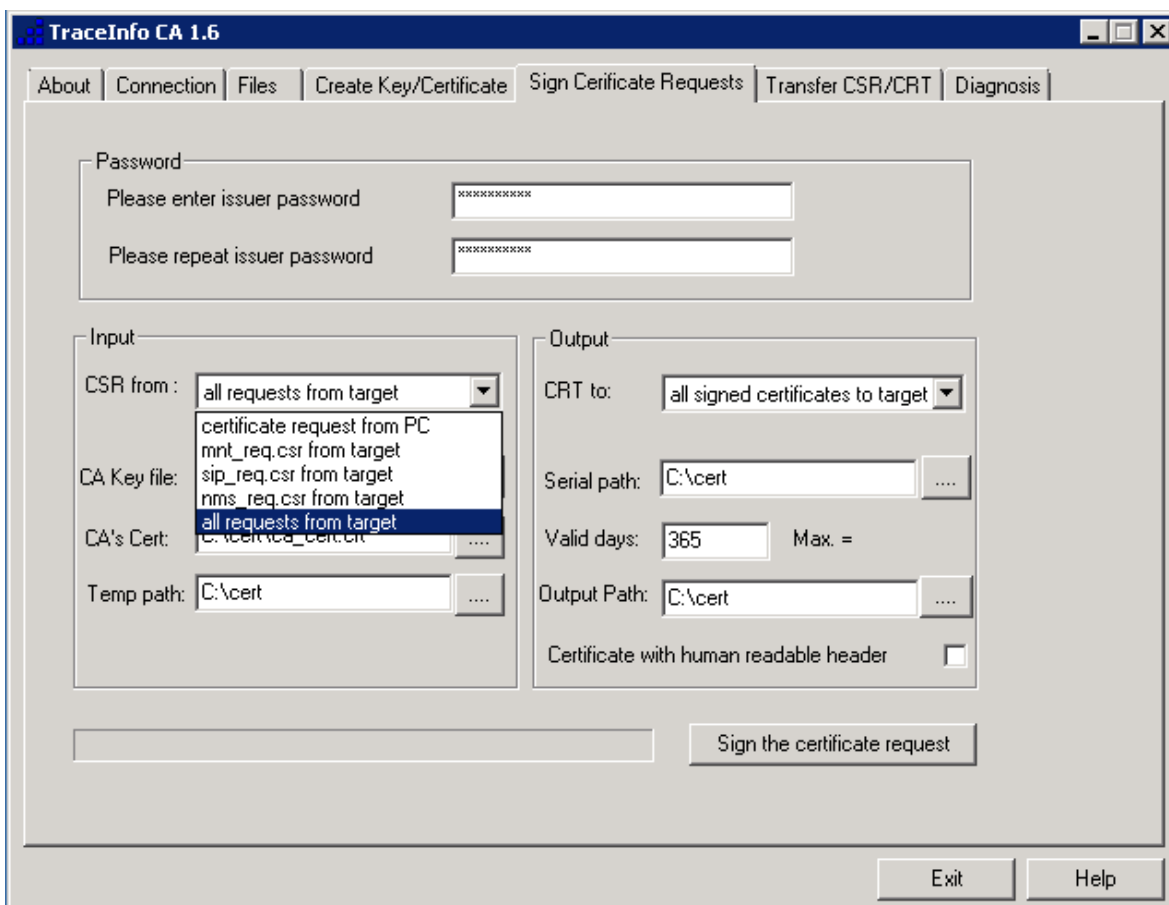


Picture 10 – Creating a CSR

3.2.1.2 Signing the CSR your self

This CSR, but also CSRs generated by a foreign CA, can be signed by TI-CA. The storage location and the certificate generated with this can be as follows:

- 1) Any CSR locally on PC → Certificate locally on PC
- 2) SIP-CSR in the gateway → SIP certificate in the gateway
- 3) Maintenance-CSR in the gateway → Maintenance certificate in the gateway
- 4) CallHome-CSR in the gateway → CallHome certificate in the gateway
- 5) SIP-, MNT- & NMS-CSR in the gateway → SIP-, MNT- & NMS-CSR in the gateway



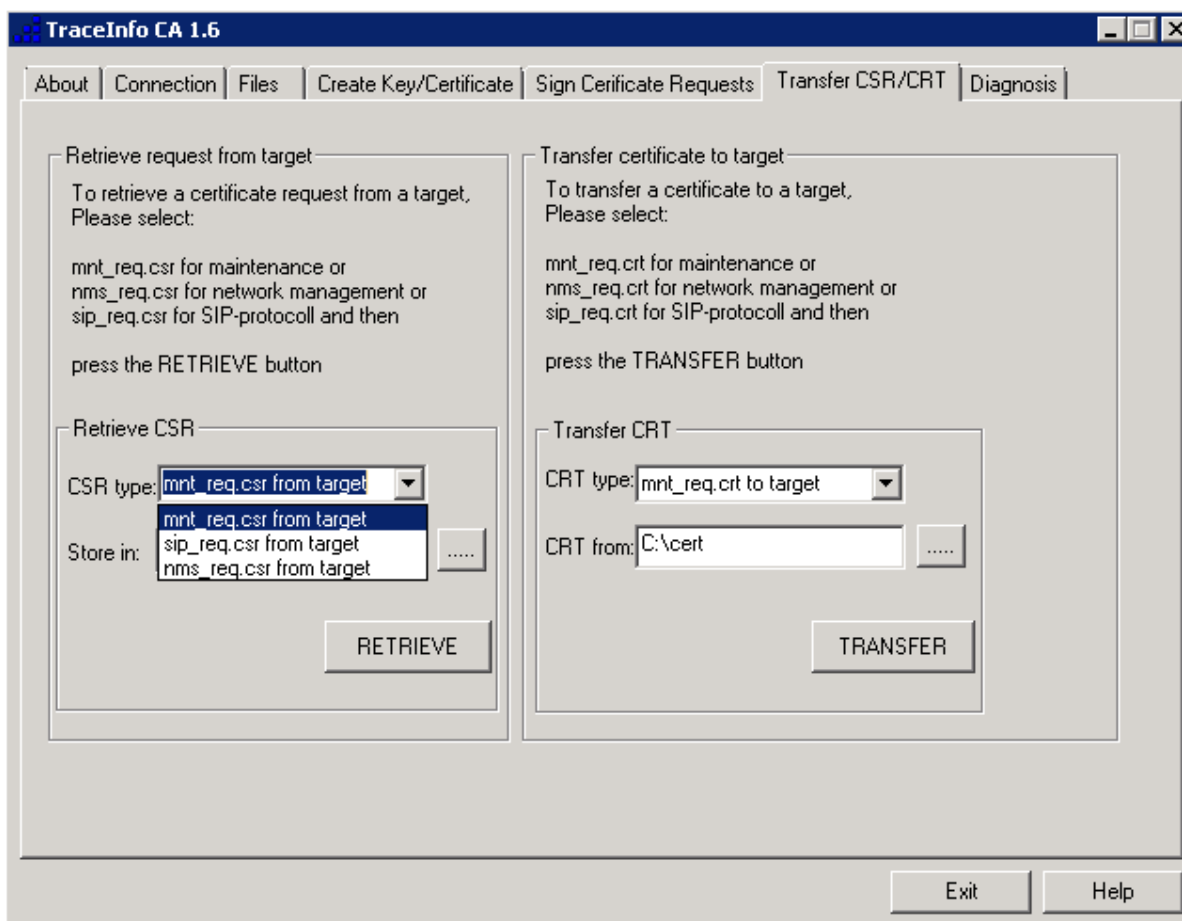
Picture 11 – Signing the CSR your self

3.2.1.3 Signing the CSR externally

The root-, maintenance- and CallHome-CSR (CA-, MNT, NMS-CSR) generated with TI-CA as well as the SIP-, MNT- and NMS-CSR generated within the NovaTec gateways can also be signed by an external certification authority (CA).

Hence CSR can be transferred from a gateway to a PC with TI-CA. After the gateway CSR has been signed by a foreign CA the received certificates (CRT) can be transferred back onto the NovaTec system with TI-CA. The tab „Transfer CSR/CRT“ serves for this purpose:

- 1) Choice of readable CSR type (SIP, MNT or NMS)
- 2) Choice of storage location of the CSR
- 3) Choice of the writing CSR type (SIP, MNT or NMS)
- 4) Choice of the storage location of the CSR



Picture 12 – Signing CSR externally

3.2.2 Plain text in certificates

If you sign a certificate signing request (CSR) for a third party (e.g. CUCM) with TI-CA, the generated certificate includes plain text. Some applications can only work with certificate files without plain text. Hence from release 1.3 on TI-CA has an option to generate certificates without plain text on the tab „Create Key/Certificate“ (see also picture 13 – Creating a certificate with or without plain text).

You can delete the plain text manually from certificates signed with older TI-CA versions as follows.

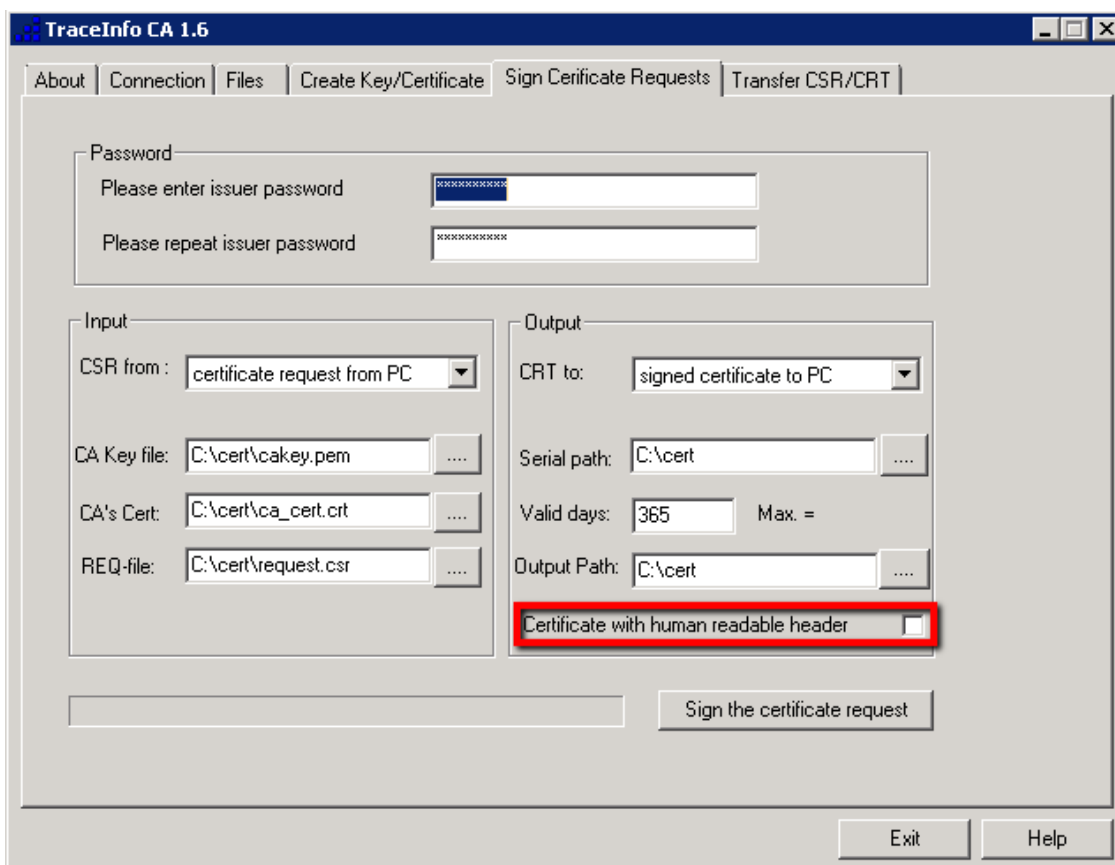
The mandatory part of the certificate begins with the line

„-----BEGIN CERTIFICATE-----“

and ends with the line

„-----END CERTIFICATE-----“.

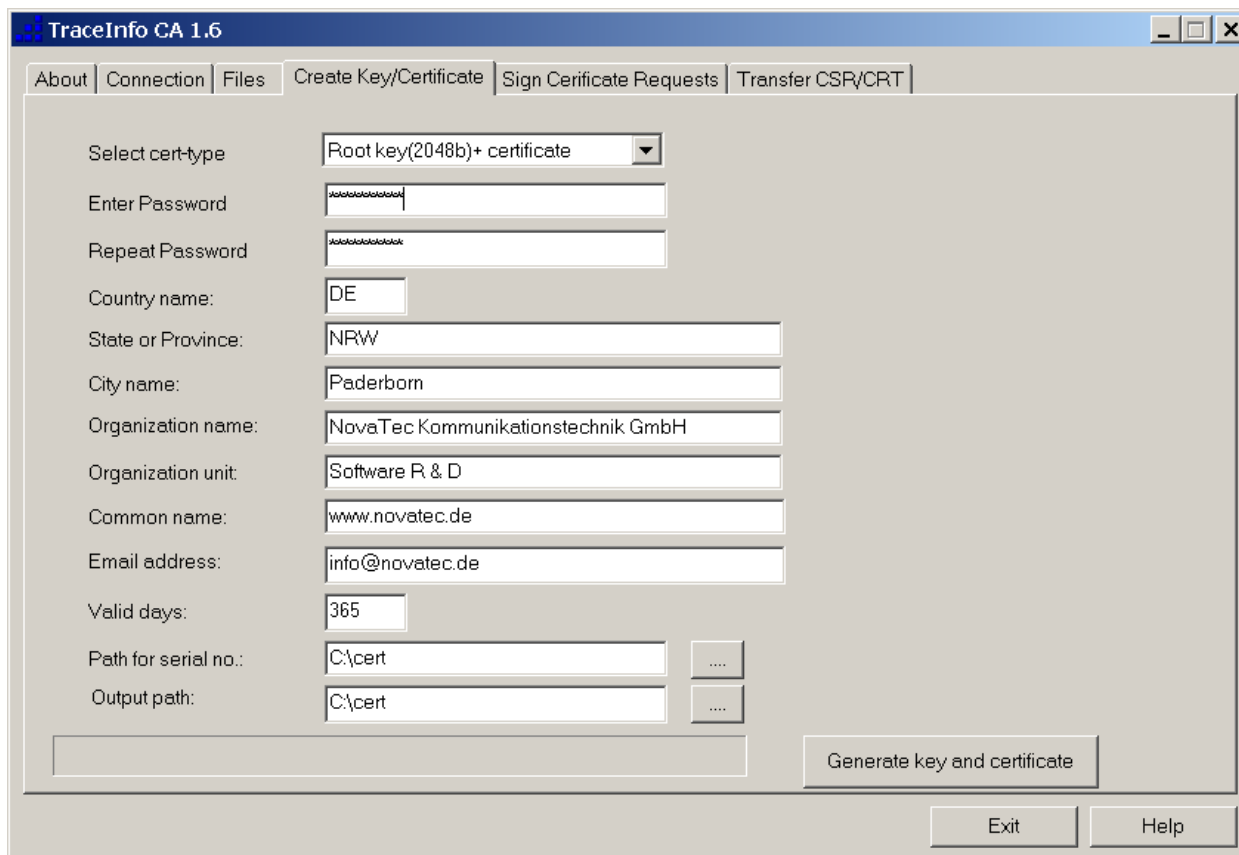
Please use an editor like e.g. WordPad to delete plain text and blank lines and to save the certificate. The two lines given above must **not** be deleted from the certificate. The files generated thus can then be used and e.g. loaded into the CUCM (see also „CUCM Crypto Install Guide“).



Picture 13 - Creating a certificate with or without plain text

3.2.3 Generating the root certificate and key

Generating a self-signed root certificate and the corresponding private key „CA private key“.



The screenshot shows the 'TraceInfo CA 1.6' application window with the 'Create Key/Certificate' tab selected. The form contains the following fields and values:

- Select cert-type: Root key(2048b)+ certificate
- Enter Password: [masked]
- Repeat Password: [masked]
- Country name: DE
- State or Province: NRW
- City name: Paderborn
- Organization name: NovaTec Kommunikationstechnik GmbH
- Organization unit: Software R & D
- Common name: www.novatec.de
- Email address: info@novatec.de
- Valid days: 365
- Path for serial no.: C:\cert
- Output path: C:\cert

Buttons: 'Generate key and certificate', 'Exit', 'Help'.

- A connection between the TI-CA application and the target system is not compulsory.
- Choose "Root key (2048b) + Certificate" in the drop down menu.
- Choose a CA password consisting of at least 4 and maximum 20 characters.
- Repeat entering the CA password. If this step fails an error message is shown in the lower line and the button „Generate key and certificate“ is deactivated.
- Now enter federal land, state, town, company, department, name and email address for the CA. The federal land has to be given with 2 characters, the other information is restricted to 64 characters.
- Enter the validity period of the root certificate in days.
- Enter the path under which the serial number of the certificate is to be saved. (1)
- Enter the path under which the „CA Private Key“ is to be saved. The generated key and the certificate are saved here in the format .pem/.crt with default name: cakey.pem and ca_cert.crt.
- After these entries have been made please press button „Generate key and certificate“. It will take a few seconds to generate the private key. Several status messages are shown.
- Please confirm these by pressing "OK".



- Under the entered path you will now find the created root certificate „ca_cert.crt“ and the corresponding 2048-bit RSA key „cakey.pem“.

Note (1):

The serial number is saved in the file serial.txt. If this file cannot be found under the given path the application will create a new file with a default serial number. The user can define the starting number himself by creating a serial.txt file with a hexadecimal code, e.g. 0123456789ABCDEF. The application will always use the current serial.txt file.



3.3 Configuring SCEP on a Windows server

From release 00.07.02.03 on the signing of TLS certificates on NovaTec gateways with the simple certificate enrollment protocol (SCEP) is supported.

For SCEP „Windows Server 2003 R2 Standard Edition“ or „Windows Server 2008 Enterprise Version“ can be used as CA server.

You can load a description of the installation of a Windows server as SCEP certificate authority as well as the necessary add-on (cepsetup.exe) from the „Microsoft Download Center“:

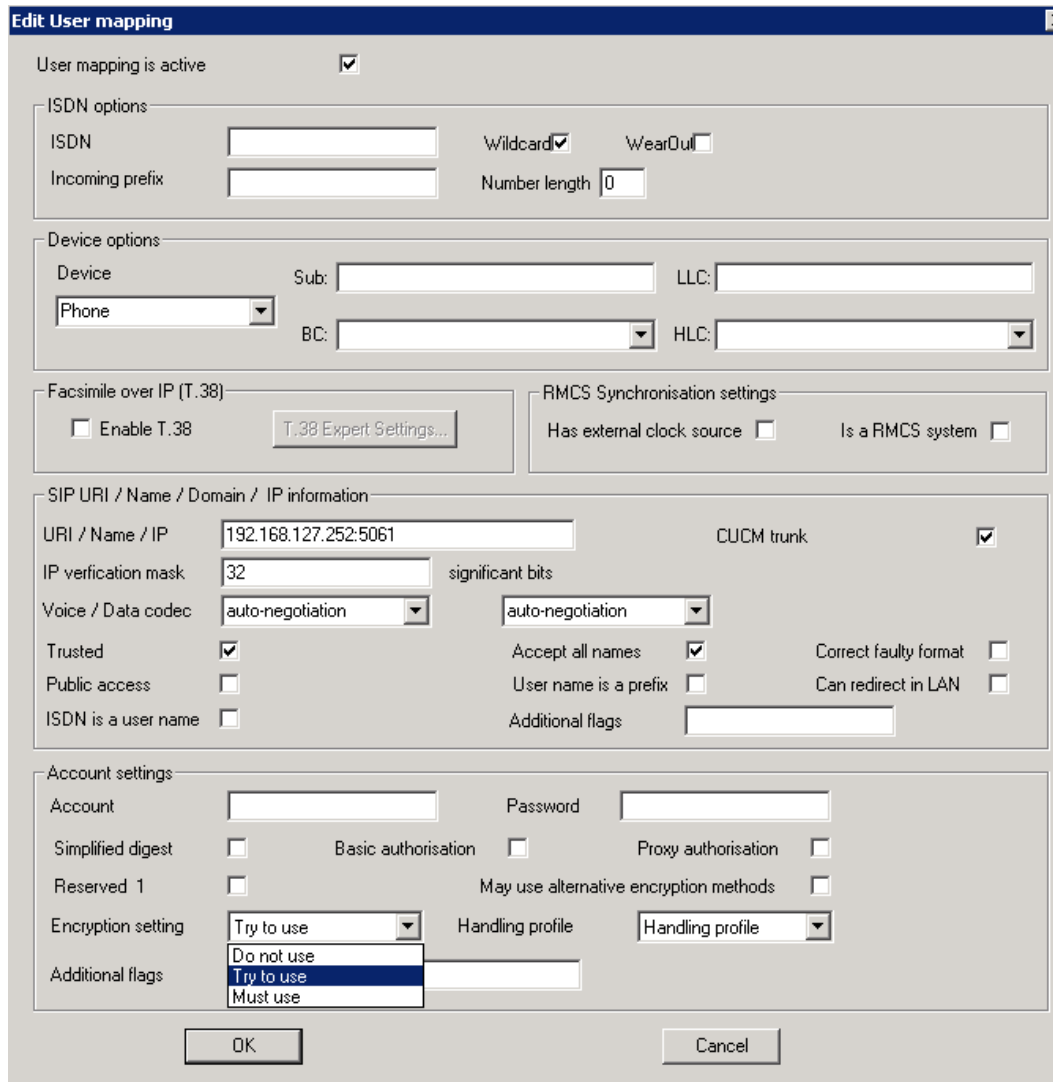
<http://www.microsoft.com/downloads/en/details.aspx?familyid=9f306763-d036-41d8-8860-1636411b2d01&displaylang=en>

With Windows server 2008 the enterprise and the datacenter version are able to execute the SCEP protocol through the active directory certificate service (ADCS) with the network device enrollment Service (NDES).

Microsoft declares that both implementations act in accordance with the standard of <http://tools.ietf.org/html/draft-nourse-scep-18> .

Both CA servers can execute the enrollment automatically or manually as well as with or without password. The servers generate the password as one-time-password with a validity of 60 minutes (this is not convenient for the rollout of NovaTec systems).

The combination of automatic and without password is not recommended due to safety aspects as a rule, but is convenient for the rollout of NovaTec systems.



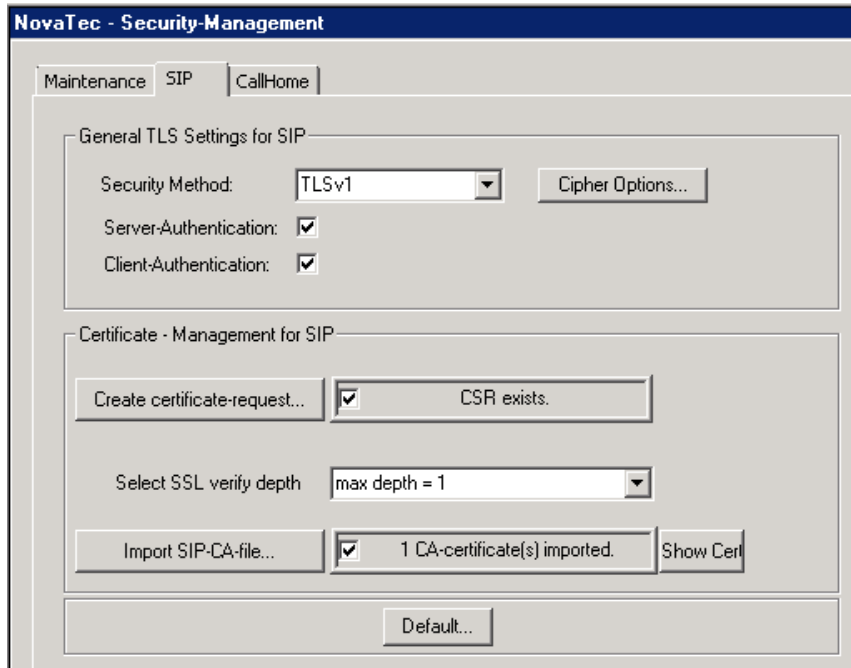
Picture 15 – Assigning sRTP to SIP

At the bottom right a generated „Handling profile“ can be selected. On the left next to this choice under „Encryption setting“ the sRTP encryption can be configured.

- „Do not use“ → Despite selected handling profile sRTP remains inactive.
- „Try to use“ → If the receiver has not activated sRTP the connection is established unencrypted.
- „Must use“ → Only if the receiver supports sRTP the connection is established.

4.2 Securing SIP with TLS

4.2.1 System IP options - enable security



Picture 16 - SIP – enable security

Go to „System IP options“ → „TLS Security“ and select tab „SIP“

- Set TLSv1 as “Security Method”.
- Tick the checkbox „Server-Authentication“ to verify the certificate received from the TLS server (e.g. S3, S6 and S20 connected to a CUCM).
- Tick the checkbox “Client-Authentication” to request and verify a certificate from a TLS client (e.g. a NovaTec-System connected as trunk to a CUCM).
- The SSL verifying depth is no configurable (Values from 1 to 9 – see also OpenSSL documentation). The verifying depth is the limit up to which the chain of certificates is used during the verification process. If the chain of certificates is longer than permitted the certificates that exceed the limit are ignored. Error messages are generated as though these are not existent: e.g. (depth = 0) SIP-CRT → (= 1) Sub-CRT → (= 2) Root-CA.
- Click „Cipher Options“ to define the method used for the TLS encryption (with CUCM AES128-SHA is recommended). Select the method „NULL SHA“ only for debugging as encryption is out of action in this case. If sRTP is configured in the CUCM, don't choose the method „NULL SHA“. In general it is not obligatory to choose a method. If you do not choose a method the NovaTec gateway will offer 19 standard methods during TLS connection establishment. If you select one or more methods at this point only the selected methods are offered and used during TLS connection establishment. If the receiver does not support any of the selected method the TLS connection establishment will fail.



4.2.2 Generating a certificate request

In this form the data for the certificate signing request (CSR) is entered and the CSR is signed by a certification authority (CA). You receive a certificate (CRT) with the entered data. Special attention has to be given to the entry for the „Common Name“ as this name is verified in some scenarios (e.g. TLS connection establishment with CUCM). Choose this name with care.

Exemplary scenarios:

- 1.) If the NovaTec gateway is configured as line device, „SEP“ followed by the MAC address of the system has to be entered.
- 2.) If the NovaTec gateway is configured as CUCM trunk, the common name has to be the same as the „X.509 Subject Name“ in the „SIP Trunk Security Profile Configuration“ of the CUCM.

Tip: If the SIP-CSR of the NovaTec gateway is signed by NAMES in the 2nd scenario (CUCM trunk), the common name in the NAMES-CA root certificate can be given analogue to the „X.509 Subject Name“ of the CUCM. If the „Policy“ in the NAMES-CA for the signing of the SIP-CSR is also set to „Match“ only SIP-CSR are signed whose common name is identical with the „X.509 Subject Name“ (see NAMES handbook 1.6.0a, chapter 5.5.3, passage 6. „Configuring the policy“). If the common name in the SIP-CSR is not identical to the common name of the NAMES-CA root certificates, an error message is shown.

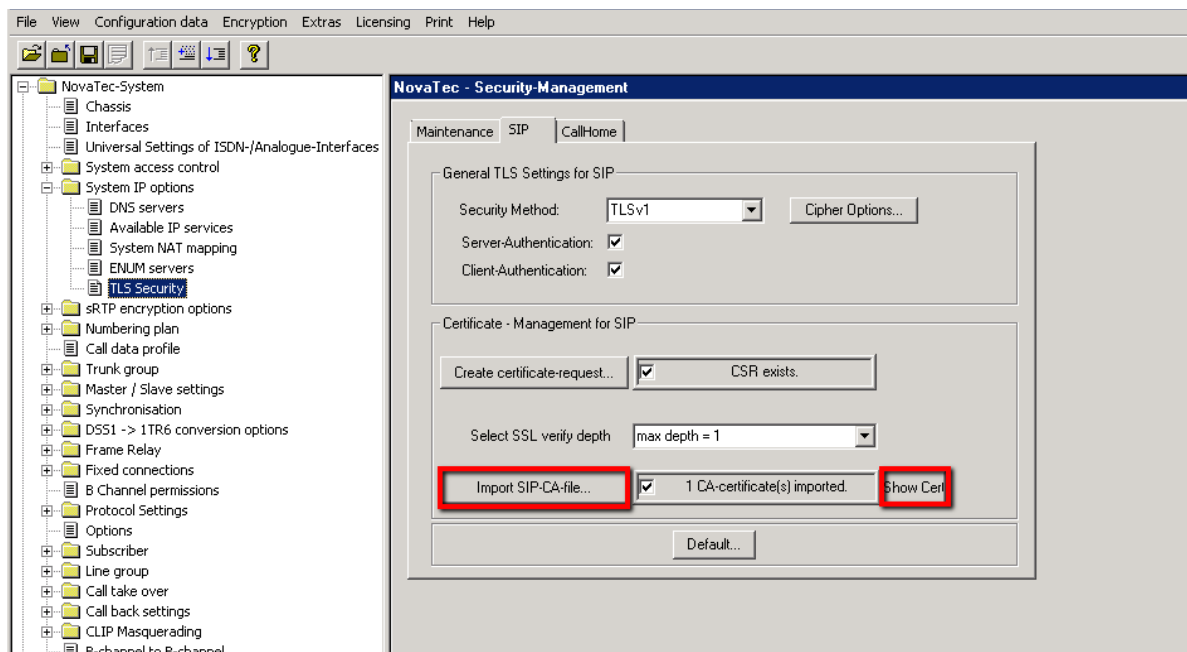
A screenshot of a software dialog box titled "Edit CSR ...". The dialog contains several input fields for CSR attributes. The fields are: Country (DE), State/ Province (NRW), Location/ City (Paderborn), Organization Name/ Company (NovaTec), Organizational Unit/ Section (RD), Common Name (SEP00603513AB0B), E-Mail-Address (sip53-Line@cisco), and Challenge Password (A challenge password). A callout box with a black border points to the Common Name field, containing the text "oder 'novatec' für Trunk". At the bottom of the dialog are "OK" and "Cancel" buttons.

Picture 17 - SIP-CSR Common Name

4.2.3 Loading the CA certificate into the trust list

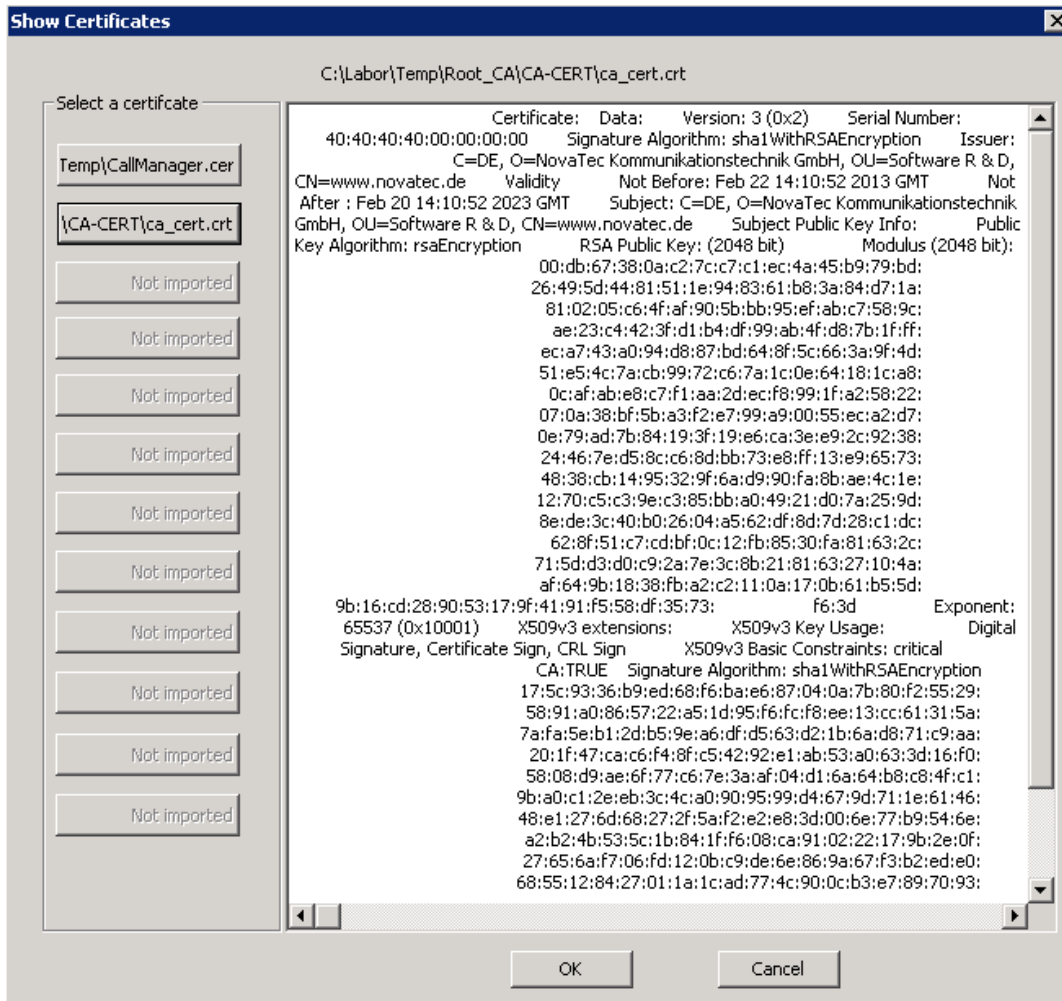
Received certificates are verified with help of the CA certificates in the local list of trustworthy certificate authorities (trust list). As the issuer of a certificate, whose CA certificate is saved within the local trust list, is held as trustworthy, a certificate is held as verified which was signed by this issuer. The issuer is named in every certificate.

CA certificates of trustworthy issuers can be imported into the trust list of the SIP instance over the button „Import SIP-CA file...” on the tab shown below. Before the chosen CA certificate is actually imported its content is shown. The user may still cancel the import if the certificate does not meet his expectations. The amount of certificates already imported to the trust list is also shown in the lower box. At all times the contents of the imported certificates can be shown by pressing the button “Show Cert”.



Picture 18 - Trust List – Loading a CA certificate

Usually a complete chain of certificates is delivered during the TLS connection establishment, e.g. for SIP, and not only the requested SIP certificate. As such it is sufficient to import only the highest CA certificate into the local trust list. Next to the CA certificate a chain may consist of CA sub certificates down to the one with which the SIP certificate has been signed. The receiver only delivers a certificate chain if the chain is completely available to it. If an element, a certificate, is missing only the requested SIP certificate is sent. In this case the chain has to be completed by the recipient with certificates from his local trust list. These have to be imported there.



Picture 19 - Trust List – Showing certificates

4.2.4 SIP-TLS User Mapping – CUCM Trunk

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

The following settings are relevant for a secured SIP connection:

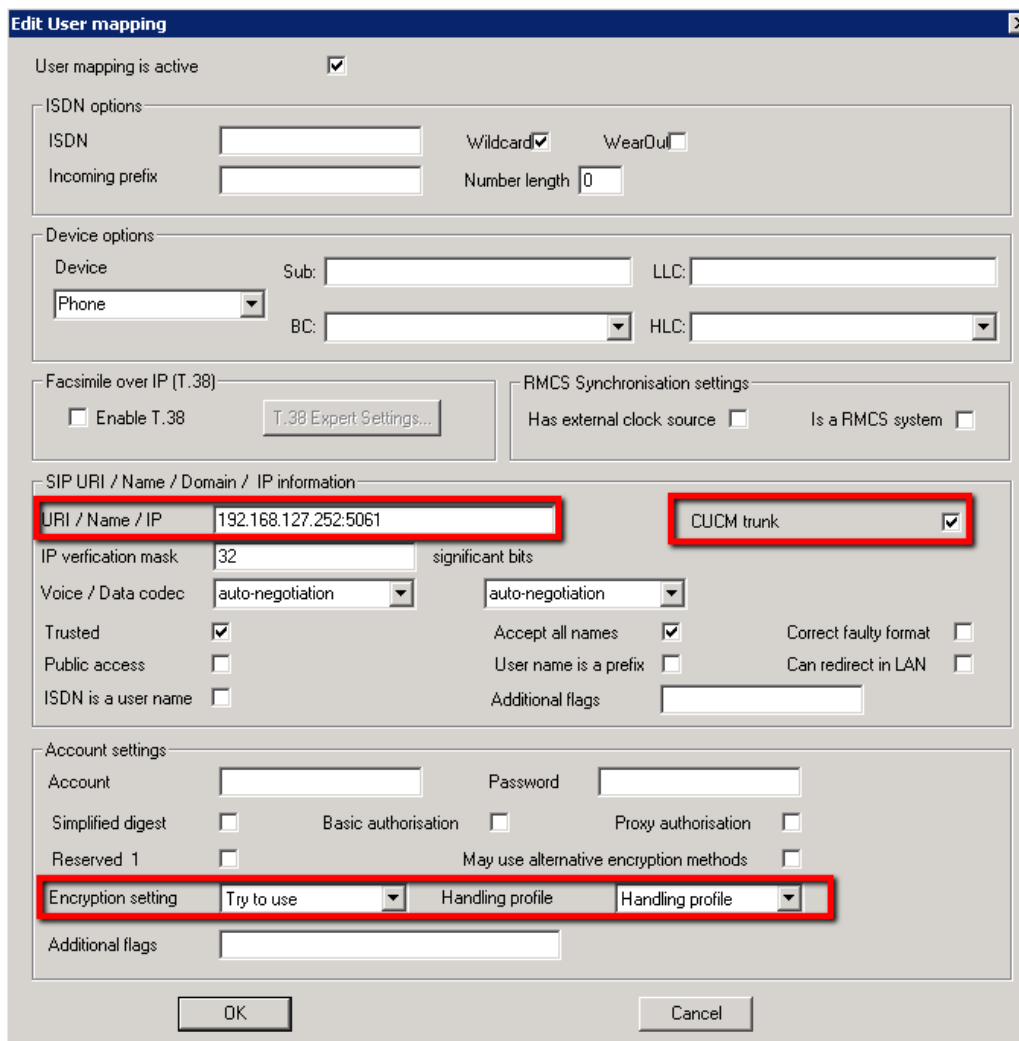
- The entry of TLS port number 5061 in box "URI / Name / IP".

In case the NovaTec gateway is connected to a TLS secured CUCM trunk:

- Tick checkbox „CUCM trunk“.

If the actual voice or data channel has to be secured with sRTP:

- Adjust the sRTP configuration boxes „Encryption setting“ and „Handling profile“.



Picture 20 - SIP-TLS User Mapping

4.2.5 SIP-TLS Local Mapping – CUCM Trunk

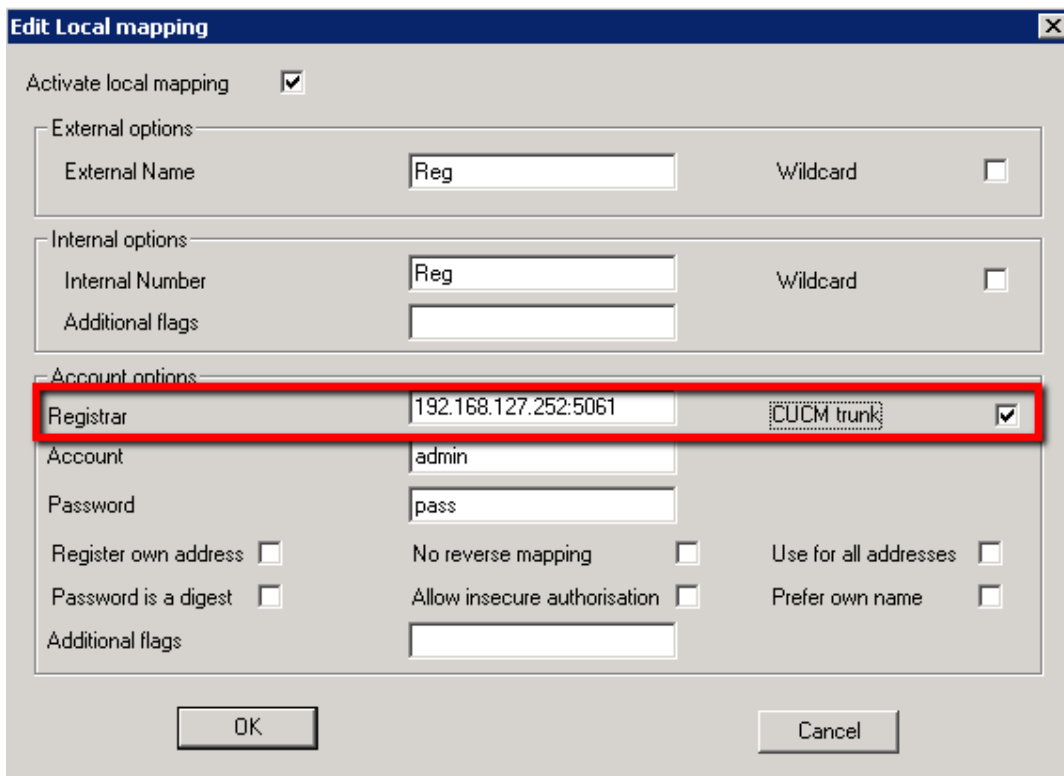
Open „NIP“ → „SIP“ -> „Mapping lists“ → „Local mapping“.

The following settings are relevant for a secured SIP connection:

- The entry of TLS port number 5061 in box "Registrar".

If the NovaTec gateway is connected to a TLS secured CUCM trunk:

- Tick checkbox „CUCM trunk“.



The screenshot shows the 'Edit Local mapping' dialog box with the following fields and settings:

- Activate local mapping:
- External options:
 - External Name: Reg
 - Wildcard:
- Internal options:
 - Internal Number: Reg
 - Wildcard:
 - Additional flags: (empty)
- Account options:
 - Registrar: 192.168.127.252:5061 (highlighted with a red box)
 - CUCM trunk: (highlighted with a red box)
 - Account: admin
 - Password: pass
 - Register own address:
 - No reverse mapping:
 - Use for all addresses:
 - Password is a digest:
 - Allow insecure authorisation:
 - Prefer own name:
 - Additional flags: (empty)

Buttons: OK, Cancel

Picture 21 - SIP-TLS Local Mapping

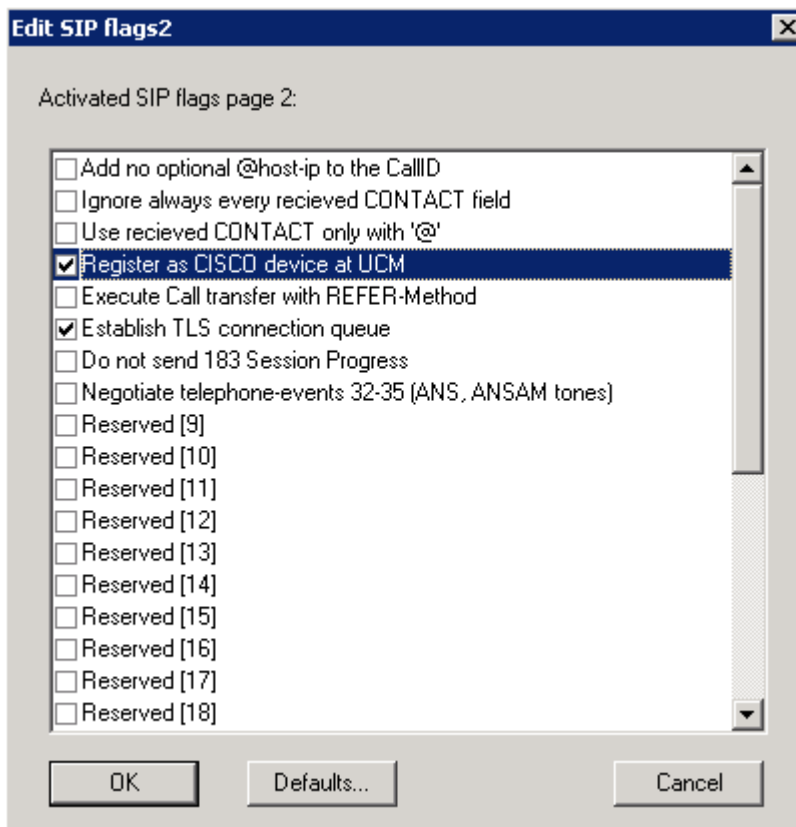
4.2.6 SIP-TLS Optional Flags

Go to „NIP“ -> „SIP“ -> „General Settings“ -> „Optional Flags 2“.

Tick box „Register as CISCO device at UCM“, if the NovaTec gateway – often a S3 – is used with a (also unsecured) line connection at a CUCM.

Tick box „Establish TLS connection queue“, if the NovaTec gateway is used with multiple TLS secured CUCM trunks. By doing so multiple simultaneous requests to establish a TLS connection do not block each other.

Please only tick box if more than three CUCM trunk addresses are entered in SIP user and local mapping and it was discovered that the TLS connection establishment with many trunks does not work as expected.

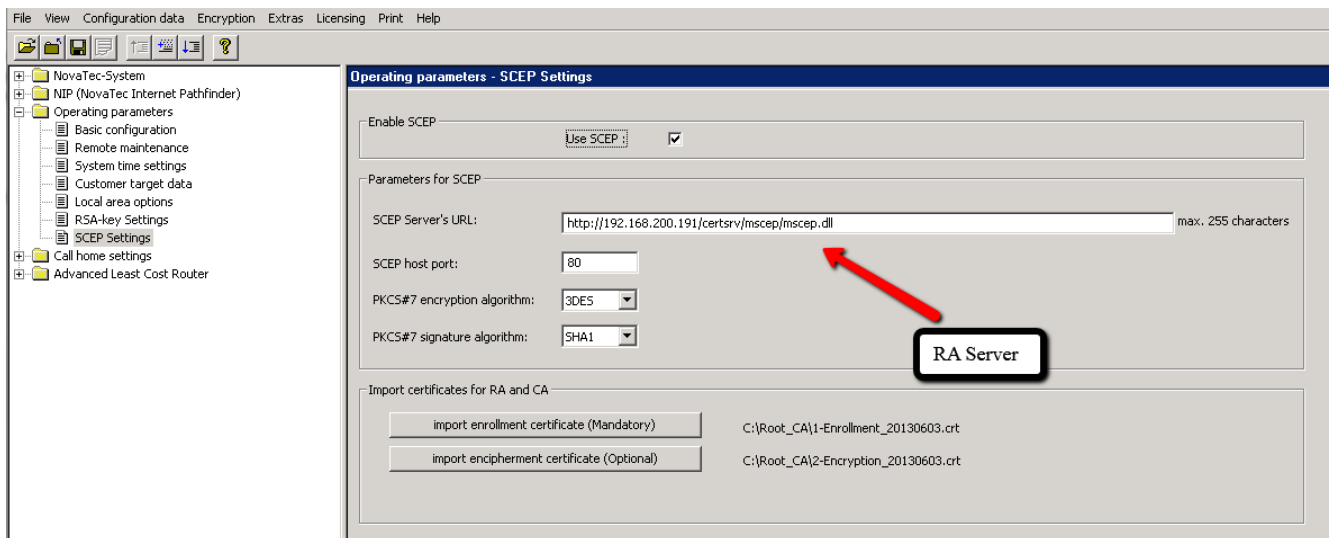


Picture 22 - SIP-TLS Optional Flags 2

4.3 SCEP

From release 00.07.02.03 on the "Simple Certificate Enrollment Protocol (SCEP)" is supported. The NovaTec configuration menu was extended by the „SCEP Settings“ under „Operating parameter“. These contain the global adjustments for all three instances (NMT, SIP, CallHome). All adjustments are identical with Windows 2003 and 2008 Server. Please find explanations under 7.3 SCEP applicatione.

4.3.1 Adjustments for the use of SCEP

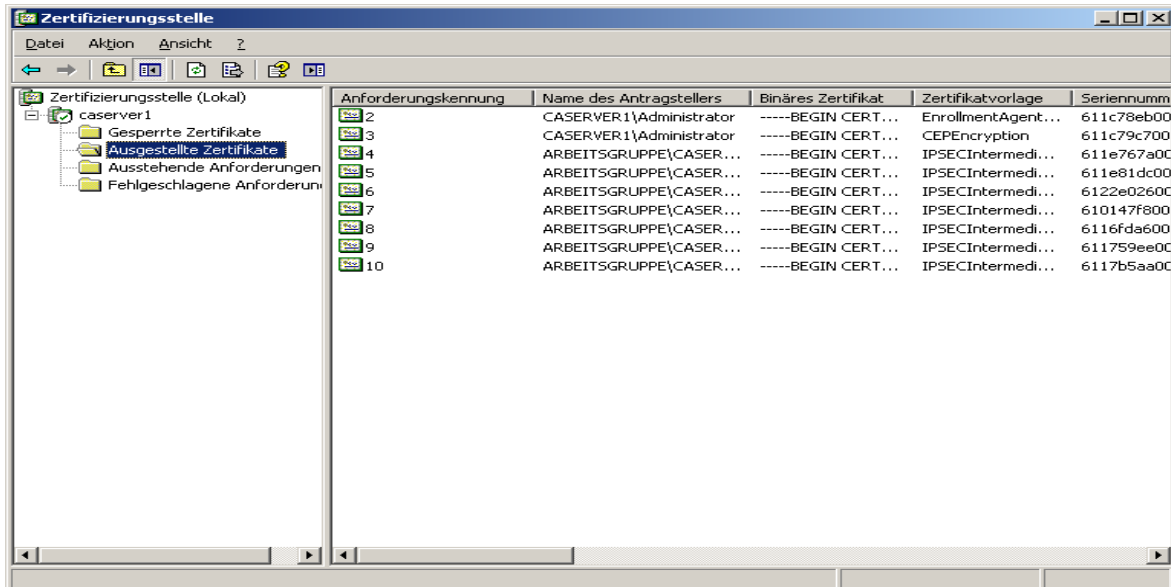


Picture 23 - SCEP Server URL

By activating the „UseSCEP“ box variable additional parameter have to be adjusted. The Microsoft standard URL <http://FQDN/certsrv/mscep/mscep.dll> is entered into the box for the SCEP server URL. The entry of the „FQDN“ server domain (caserver1.novanet.local) requires an additional DNS resolution and so provides the trustworthiness of the remote. Instead of the „FQDN“ you can also enter a server IP address. As the SCEP protocol is „http“ based, the default port is 80. Next you can assign the PKCS#7 based algorithms for encryption and signature. By standard these are: DES, 3DES, Blowfish as well as md5 and sha1.

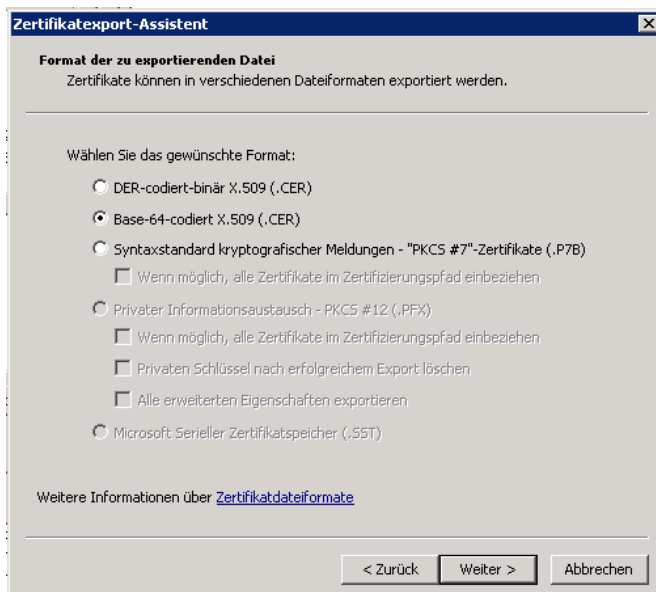
4.3.2 Registration Authority Certificates

If a Microsoft server is used as CA certificate authority for the enrolment with SCEP, two registration authority (RA) certificates have to be imported for the enrolment by it. "*usage: Digital Signature, Non Repudiation*" is a signed RA certificate (enrolment certificate) , "*usage: Key Encipherment, Data Encipherment*" is used for encryption (Encipherment Certificate). Both have to be exported from the certificate authority of the CA server in bas64 format.



Picture 24 - Export of the two enrolment certificates

In the list (Picture 24 - Export of the two enrolment certificate) the two upmost certificates are responsible for the enrolment. The export is started by double clicking the correspondent row. Both certificates have to be Base-64 encoded. For the import of the certificates into the NovaTec configuration program the extension *.cer has to be renamed into *.crt.

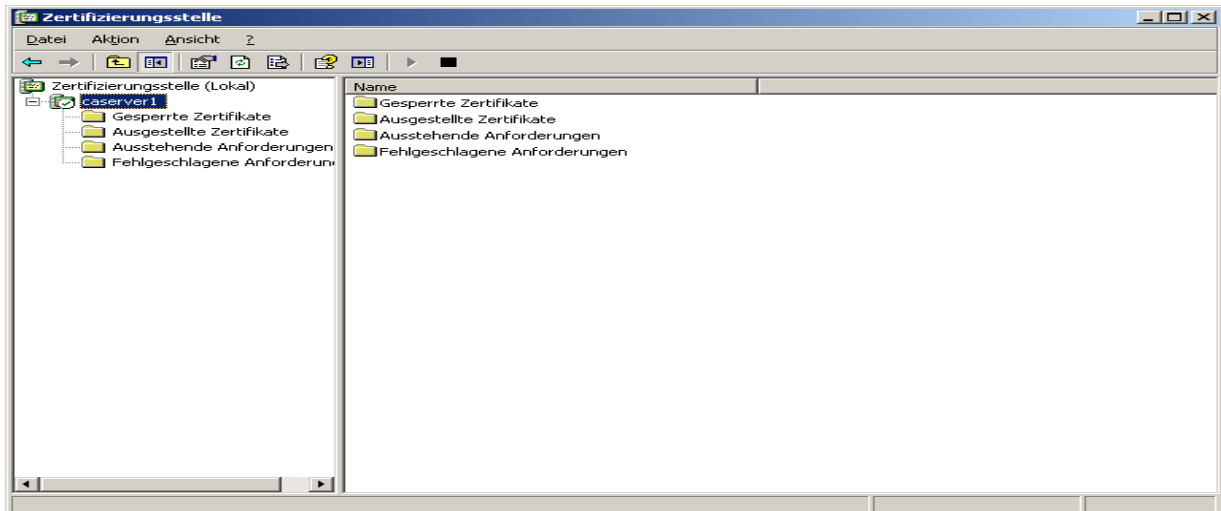


Picture 25 – Export data format

4.3.3 CA chain

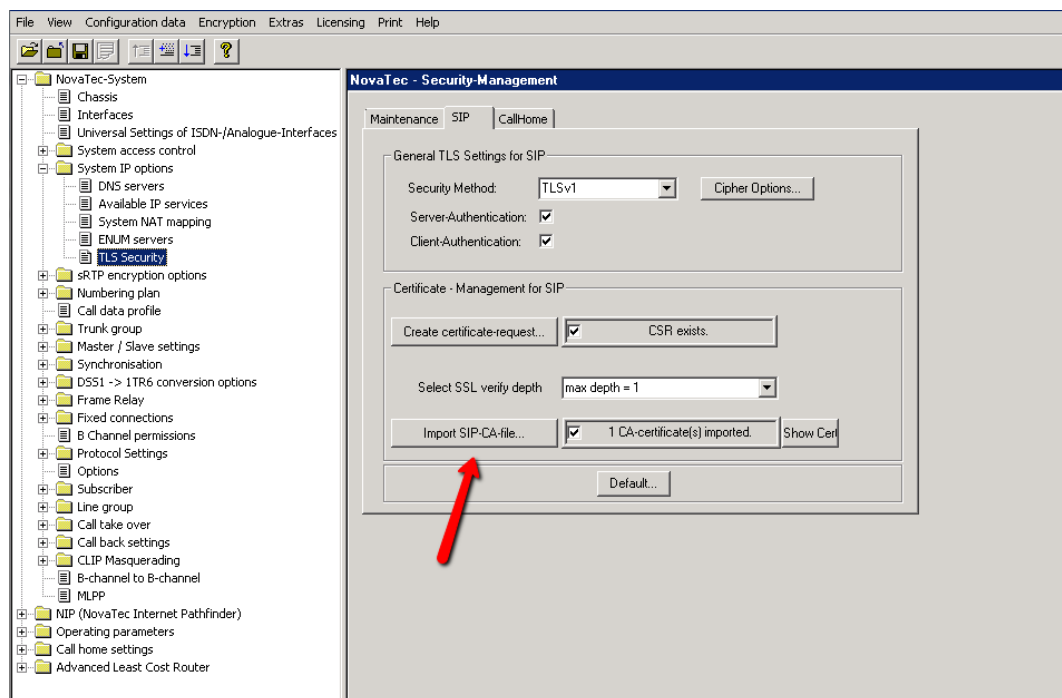
All three instances (MNT, SIP and CallHome) of the NovaTec gateway also need the „Public CA Certificate“ or a certificate chain.

On the Microsoft CA server the export is started by right-clicking the menu tree of the certificate authority -> CA Server -> properties -> Show certificate -> details -> copy to file...



Picture 26 - SCEP CA export

The certificates are imported into the NovaTec configuration over „NovaTec-System“ -> „System IP options“ -> „TLS Security“. Choose the particular tab „Maintenance“, „SIP“ or „CallHome“ and start download by clicking „Import ...CA-file“.



Picture 27 - SCEP CA import

If the optional challenge password is not used (see chapter 4.3.4), the configuration of SCEP is hereby finished.

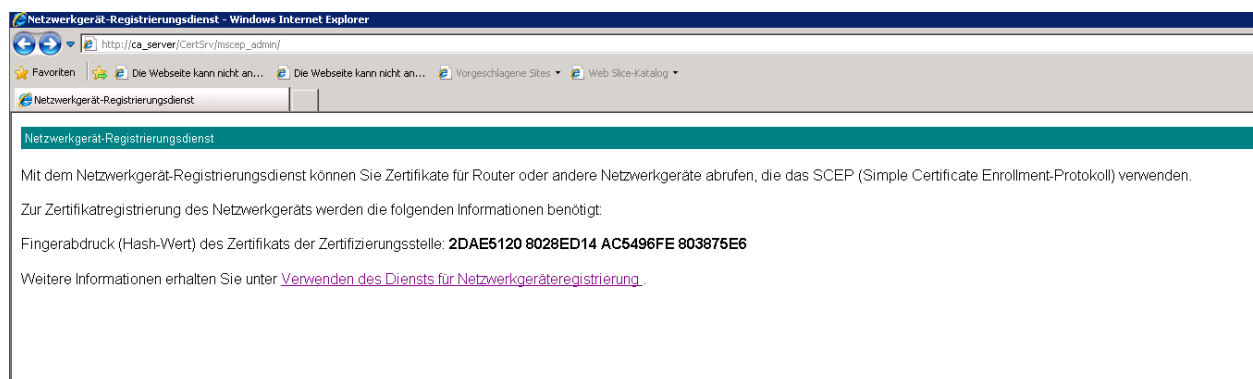
After the transfer of the configuration onto the system and its restart, the TLS certificates of the three instances are signed in the gateway with SCEP.

The process of signing certificates with SCEP and the manual steps required subsequently are described in chapter 5.2.

4.3.4 Challenge Password

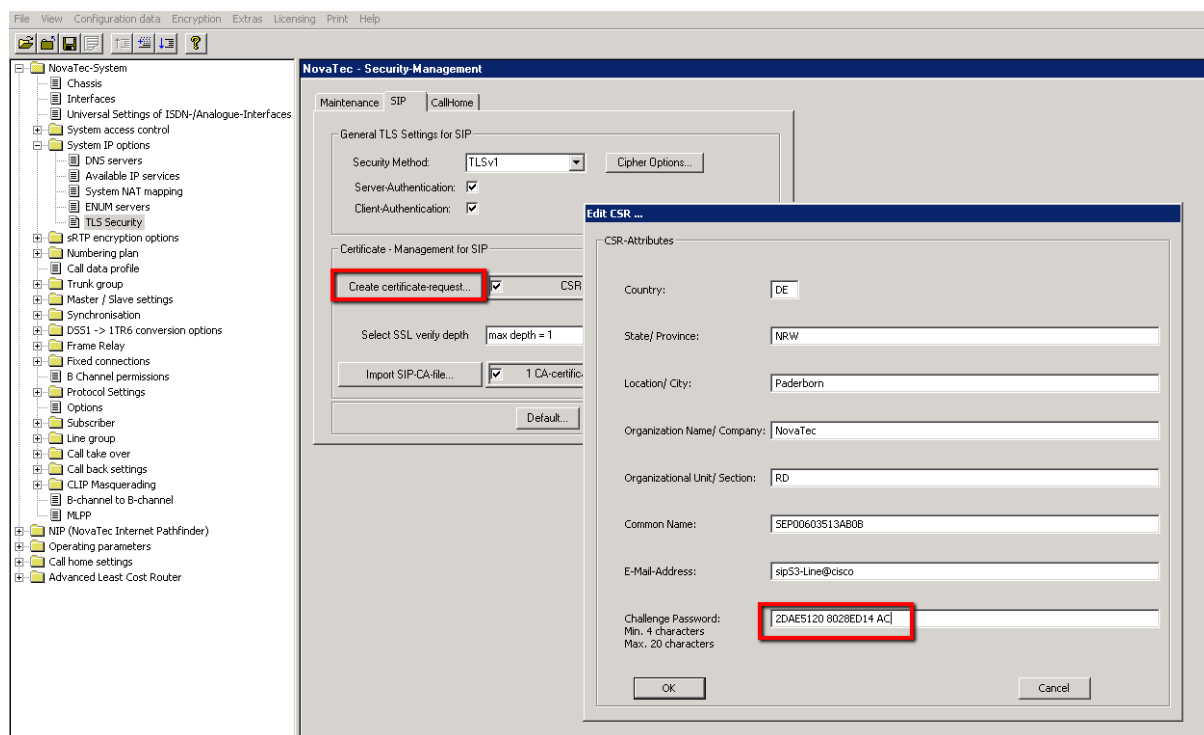
If the optional challenge password is activated in the registry of the CA server, all three instances (MNT, SIP and CallHome) of the NovaTec gateway require a onetime password.

Open the page „http://CA Server Name/certsrv/mscep“ with your browser if you are using Windows 2003 and „http://CA Server Name/certsrv/mscep_admin“ when using Windows 2008.



Picture 28 – Copying the challenge password

The challenge password is character string generated randomly and can be transferred by copy and paste from the web browser into the NovaTec configuration (Picture 29 – Inserting the challenge password).



Picture 29 – Inserting the challenge password

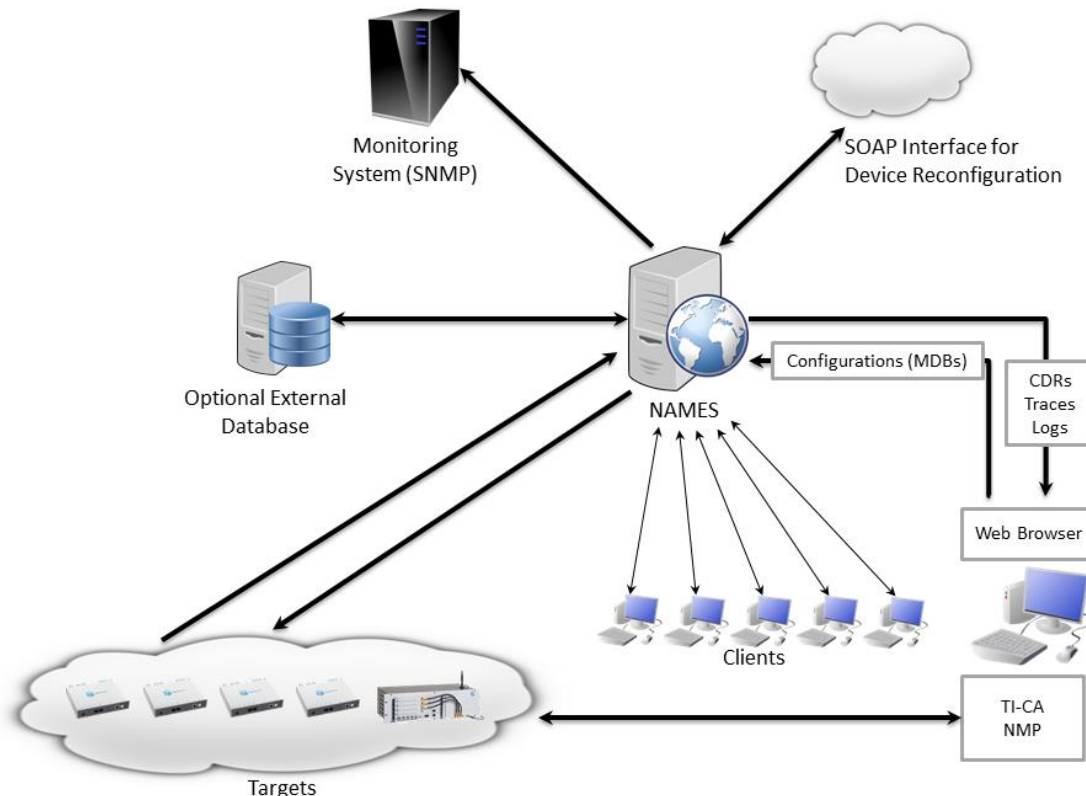
The configuration of SCEP is now completed.

After the configuration has been transferred to the system and this has restarted, the TLS certificates of the three instances are signed with SCEP within the gateway.

The process of signing certificates with SCEP and the manual steps required subsequently are described in chapter 5.2.

4.4 NAMES

NovaTec Administration and Management Element Server (NAMES) is an element manager for all NovaTec gateway products. Rollout and implementation as well as monitoring, administration, configuration and software updates of the gateways can be carried out with NAMES whilst the systems are active.



Picture 30 - NAMES architecture

The above shown connections have to be possible for the use of NAMES. Possibly existing firewalls in between the components have to be configured in accordance with the specifications in the document „IP port matrix of NovaTec systems and applications“ in order to allow communication. The document can be downloaded from the NovaTec website under <http://www.novatec.de/handbooks/IP-Portmatrix.pdf>.

A certification authority (CA) is integrated into NAMES. As such NAMES is capable of signing certification requests (CSR) of the three instances (MNT, SIP, NMS) on NovaTec systems. You do not have to adjust any additional parameter in the configuration of the systems to enable NAMES to sign these.

NAMES is also able to establish a MNT connection secured by TLS to the administrated gateways.

The NAMES handbook provides detailed instructions.

A short instruction follows.



4.4.1 NAMES as CA

A CA certificate and a private key are required for the NAMES CA. An externally generated certificate file and the related key file can be uploaded. But NAMES can also generate a self-signed certificate and the related private key. If Names is used as a sub CA in an existing PKI a CSR has to be generated and sent to the superior certificate authority, which then has to provide a new CA certificate for this CSR. The certificate provided by an external CA has to be uploaded into the NAMES CA.

Now NAMES can sign NovaTec gateways when the job „sign certificate“ is carried out and configured CSRs are installed in the gateway.



4.4.2 Secured connection to the gateway

If a secured connection is configured in the gateway for maintenance purposes and the TLS certificate for this instance is signed within the gateway, NAMES can use this secured connection. NAMES assigns an SSL context to a target for this purpose by which a TLS connection to the gateway is established.

These SSL contexts can be configured within NAMES. For a secure connection several SSL parameter are combined in a SSL context (ROOT CA certificate, own certificate, private key). Additionally the CA certificate of one or more trustworthy certificate authorities can be uploaded into the context.



4.5 Securing maintenance / call home

Premise for the security of TLS on TCP/IP connections between NovaTec applications and NovaTec gateways is a firmware license with active TLS option, which can be requested from NovaTec, and the upload of this license with the configuration onto the gateway (see chapter 3.1 Activating encryption in NovaTec systems).

Afterwards a TLS secured connection between a NovaTec gateway and NovaTec applications like NAME server, TraceInfo-Client, TI-CA or a call home server can be setup with the following procedure.

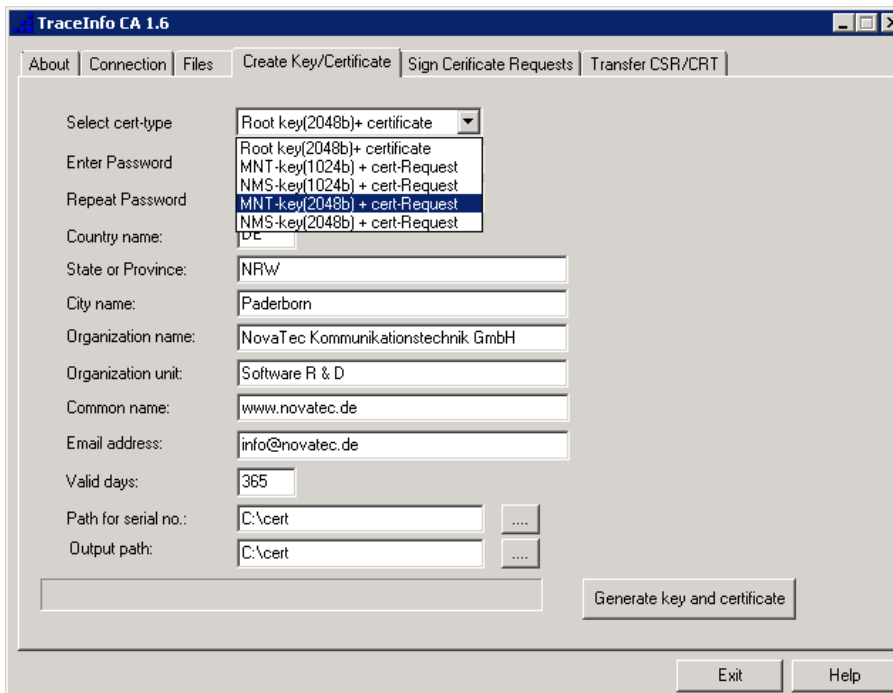
- 1) TI-CA requires a ROOT certificate.
- 2) TI-CA generates certificate signing requests (CSR) for the PC side certification of maintenance or call home connections.
- 3) These CSR for the PC side are signed by TI-CA or sent to an external CA for signing.
- 4) In the configuration of the gateways the necessary adjustments for maintenance and call home CSR of the NovaTec gateways are made. Also the adequate root CA certificate needs to be loaded into the trust list.
- 5) After reboot with this configuration the NovaTec gateway will generate the configured certification requests.
- 6) The CSR on the NovaTec gateway are either signed by TI-CA or downloaded from the gateway with TI-CA and sent to an external CA for signing.
- 7) The certificates issued by an external CA are transported to the NovaTec gateways with TI-CA. Certificates signed directly by TI-CA are already saved within the gateway.
- 8) After rebooting the certificates in the gateway are enabled.
- 9) The certificates issued in 3) are installed on the PC side. For example they can be loaded into a NAMES SSL context (see NAMES handbook) or be imported into TI-CA via the "Connection – Network Options" menu. Now TLS secured connections between NovaTec gateways and NovaTec applications can be used.

4.5.1 TI-CA requires a root certificate

The root certificate can be signed either by TI-CA itself or by an external CA as described in chapter 3.2.3 „Generating the root certificate and key“. The further use of self-signed and externally signed root certificates do not differ from one another.

4.5.2 Generating maintenance and call home CSR

With TI-CA certificate requests (CSR) are generated under tab „Create Key/Certificate“. As described in chapter 3.2.1.1 „Creating a CSR“ it is possible to generate CSR with 1024 or 2048 bit key length for maintenance (MNT) and call home (NMS).



Picture 31 – Creating MNT & NMS CSR

By pressing button „Generate key and certificate“ the files with the private key and CSR are generated. These are saved in the file entered under „Output path“. The CSR can be sent to an external certification authority (CA) for signing or be signed with TI-CA.

4.5.3 TI-CA signs MNT- & NMS-CSR

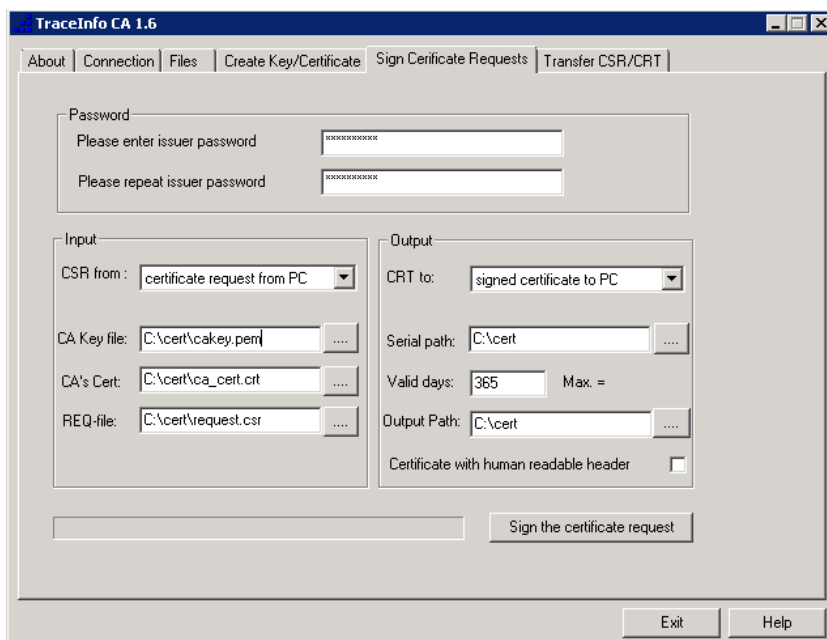
- TI-CA tab „Sign Certificate Requests“

Input:

- Choose “CSR from:” “certificate request from PC”
- Choose the files of the root certificate for „CA Key file:” and „CA’s Cert:” with which the MNT or NMS-CSR is to be signed.
- The „REQ-file:” is the MNT- or NMS-CSR created above.

Output:

- Choose “CRT to:” “certificate request to PC”
- “Serial Path:” Enter path for the used serial number of the certificate, which is to be generated.
- „Valid days:” Enter the required validity duration in days.
- „Output Path:” is where the generated certificate is saved.
- Deactivate „Certificate with human readable header”.
- By pressing button „Sign the Certificate request” the certificate is created and saved in the chosen „Output Path:”.



Picture 32 - TI-CA signs MNT- & NMS-CSR

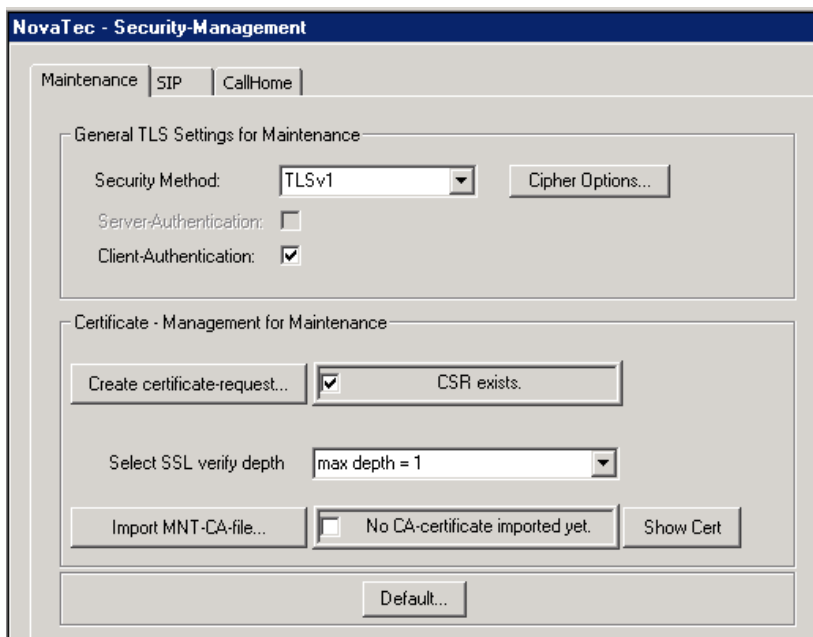
4.5.4 Configuration of MNT- & NMS-CSR

Choose → „NovaTec-System“ → „System IP options“ → “TLS-Security” and then tab „Maintenance“ (MNT) or CallHome (NMS) in the menu of the NovaTec configuration.

The certificate requests (CSR) for the instances maintenance and call home are both configured similar.

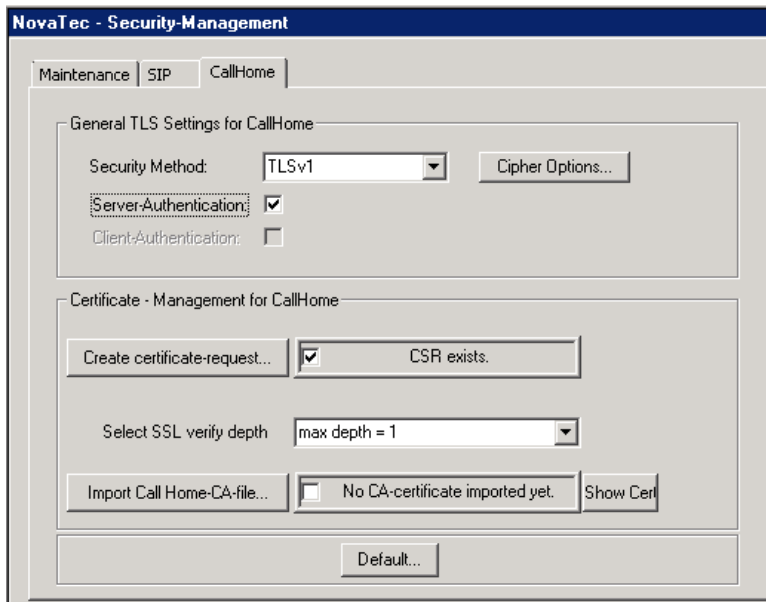
- As „Security Method:“ you have to choose „TLSv1“.

The only difference is, that you can activate „Client-Authentication“ in the gateway for MNT, as the gateway takes the part of the server during TLS connection establishment. If the feature is activated, the server requests the client certificate from the PC application and verifies it.



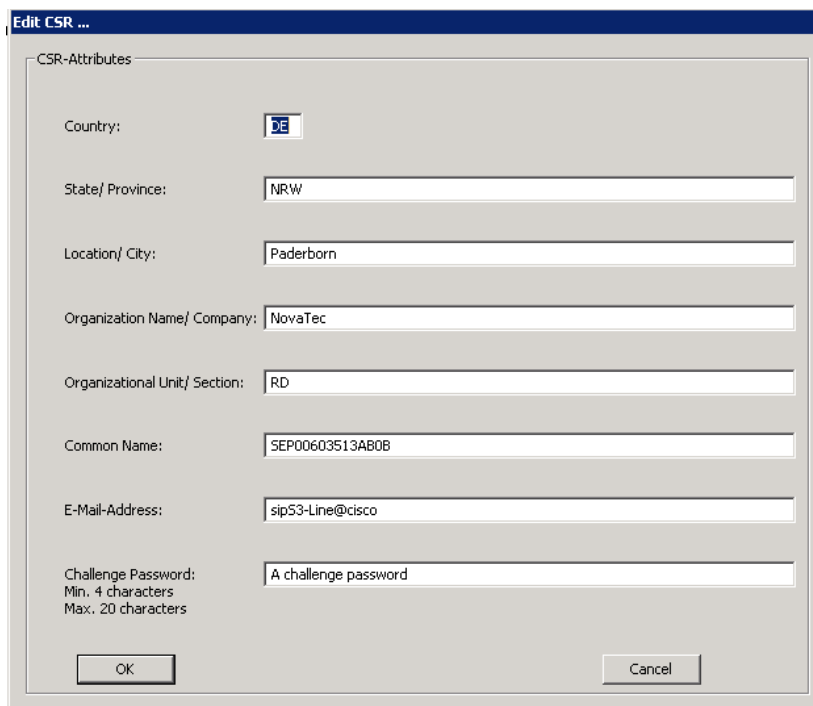
Picture 33 – Configuring CSR for MNT

The call home connection though is initiated by the gateway. During the TLS connection establishment it acts as client. The server as receiver does indeed always send its certificate to the client in the context of the TLS protocol, but only verifies it if the feature „Server-Authentication“ is configured on his side.



Picture 34 – Configuring CSR for NMS

- It is recommended to activate „Client-Authentication“ and „Server-Authentication“ to enable the verification of the identity of the TLS receiver and so to achieve a higher security of the connection.
- „Create certificate-request...“: Please complete form for the CSR content. If the MNT- or NMS-CSR are signed with SCEP (e.g. Windows 2008 Server) in the gateway it is possible to enter a fitting „Challenge Password“. All other details have to be given in accordance with the PKI directive agreed upon for the installation or at one's own discretion.



Picture 35 - MNT- / NMS-CSR form



- „Select SSL verify depth“: In this box you define the verification depth of the certificate chain.
- „Import Call Home-CA-file...“: The CA certificates can be imported into the trust list of the gateway. The content of the certificates can be shown before and after importing them. The number of imported CA certificates is shown. By means of these CA certificates the gateway verifies the identity of the TLS receiver for MNT or NMS connections.

4.5.5 Creation of MNT- / NMS-CSR

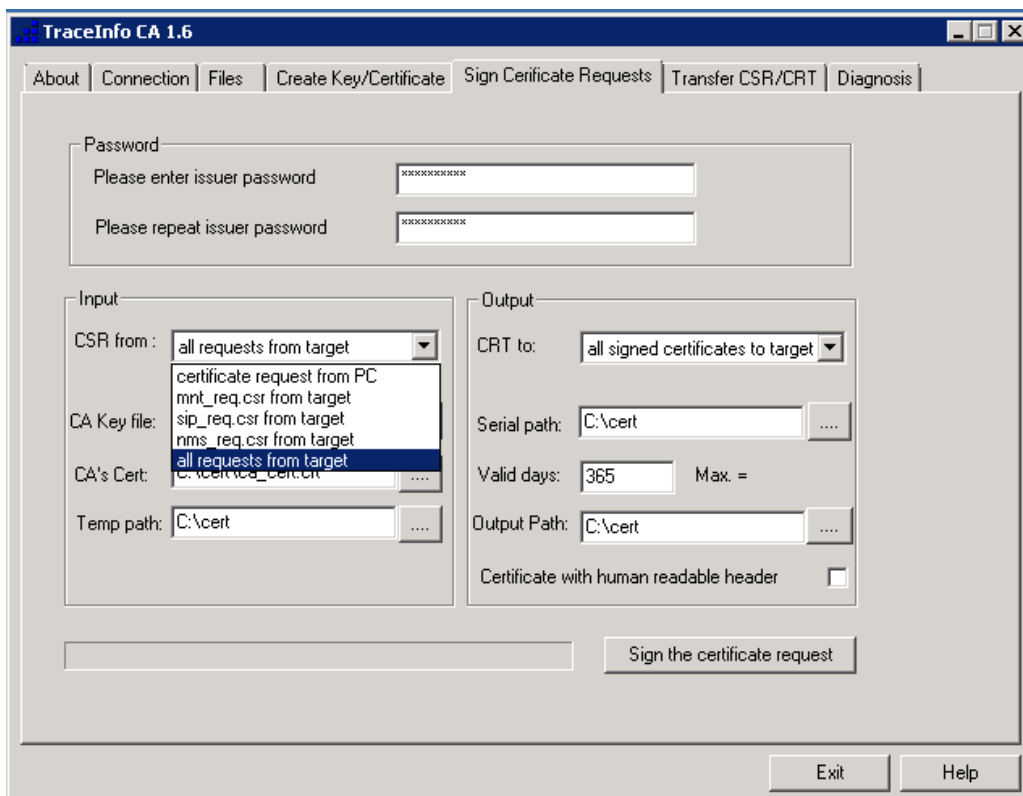
The configured certification requests are created in the gateway after a reset.

4.5.6 TI-CA signs the MNT or NMS certificate

If TI-CA is connected to the gateway it can sign the MNT- or NMS-CSR separately on the gateway. If there also is a SIP-CR all three can also be signed together in one go.

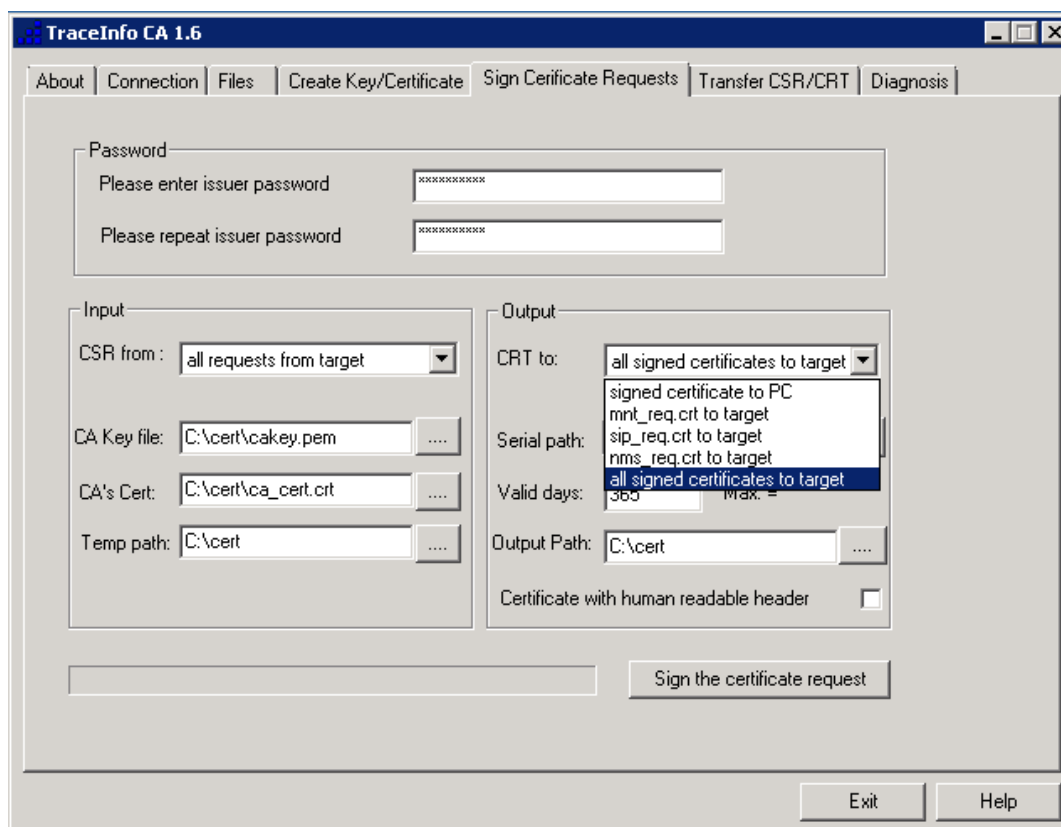
→ Please pursue the steps for the 3rd and 4th case as described in chapter 5.1 „Signing with TI-CA“. Choose input “CSR from:” as follows:

- „mnt_req_csr from target“ if only the MNT-CSR is to be signed.
- „nms_req_csr from target“ if only the NMS-CSR is to be signed.
- „all requests from target“ if all existent CSR (MNT, NMS & SIP) in the gateway are to be signed together in one go.



Picture 36 - Input: TI-CA signs MNT- / NMS-CSR on the gateway

The target adjustments for „output“ are automatically set analogue to the input adjustments.



Picture 37 - Output: TI-CA signs MNT- / NMS-CSR on the gateway

4.5.7 Loading externally signed MNT- & NMS-CRT into the gateway

If TI-CA is connected to the gateway it can also upload an externally signed MNT or NMS certificate.

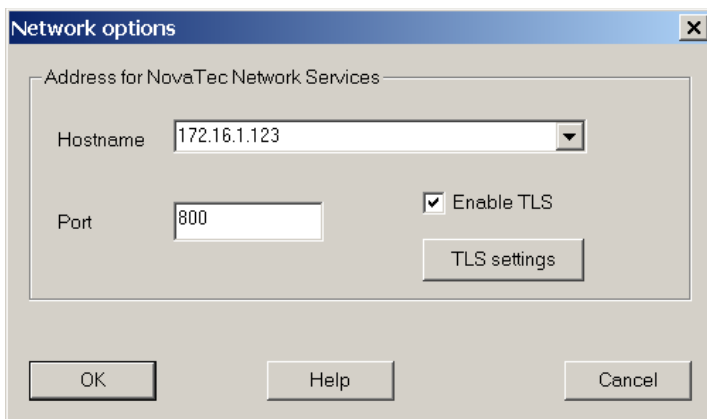
Please pursue the steps in chapter 3.2.1.3 „Signing the CSR externally

4.5.8 Performing a reset

After a reset the certificates on the gateway are active.

4.5.9 Installing MNT- & NMS-CRT on the PC side

The certificates as given in the chapter „TI-CA signs the MNT or NMS certificate“ are installed on the PC side. They can be loaded into a NAMES SSL context (see NAMES handbook) for example or imported into TI-CA or the NovaTec configuration program under “Connection – Network Options” in the menu. After this TLS secured connections between NovaTec gateways and NovaTec applications can be used.



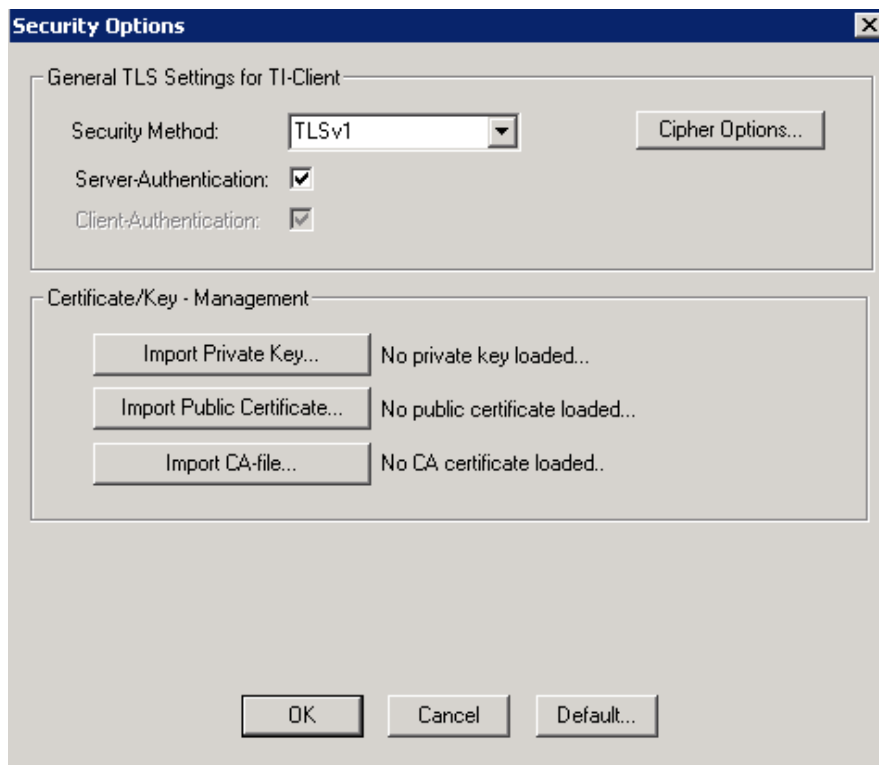
Picture 38 – Activating TLS for MNT

Start the NovaTec application on a PC whose connection to a gateway is to be secured with TLS

- Enter IP address of the gateway in window „Network options“ and activate TLS by clicking „Enable TLS“

Open window for the settings as required for TLS connections by clicking button „TLS settings“.

- „Security Method:“ choose „TLSv1“ .
- The “Cipher Options...” can remain on standard settings.
- We recommend activating „Server-Authentication“. The PC application will then verify the TLS certificate of the gateway and confirm its identity.
- With „Import Private Key...” the private key file „mnt_key.pem“, generated by TI-CA together with the MNT certificate signing request, is loaded.
- With „Import Public Key...” the signed MNT certificate (CRT) is imported.
- In a final step the CA certificate, with which TI-CA or an external CA signed the MNT certificate, is loaded into the trust list of the application under „Import CA-file...”.
- With „OK“ the settings are confirmed and activated.



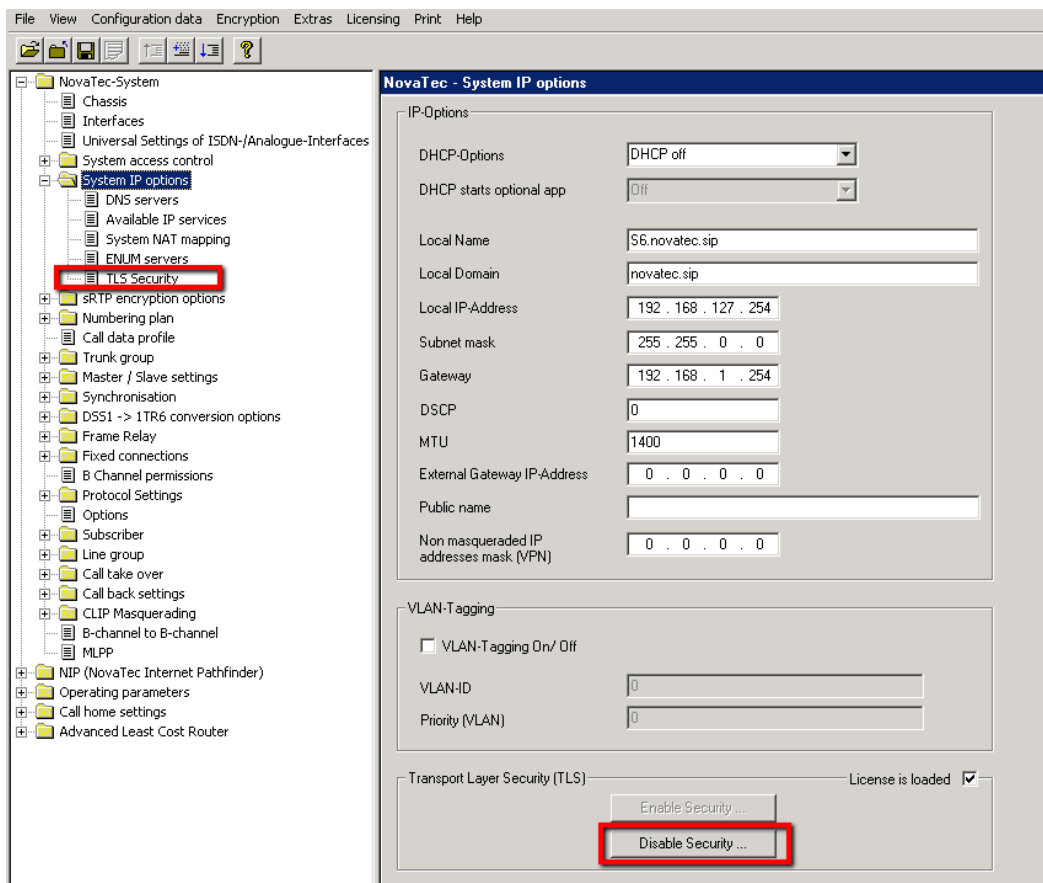
Picture 39 – Loading TLS certificate for MNT

4.6 Deactivating TLS and sRTP

4.6.1 Turning off encryption for SIP and Maintenance

Go to NovaTec-System -> System IP options.

Choose "Disable Security ..." and confirm the shown windows. The node "TLS security" under "System IP options" in the tree on the left hand side is no longer shown.



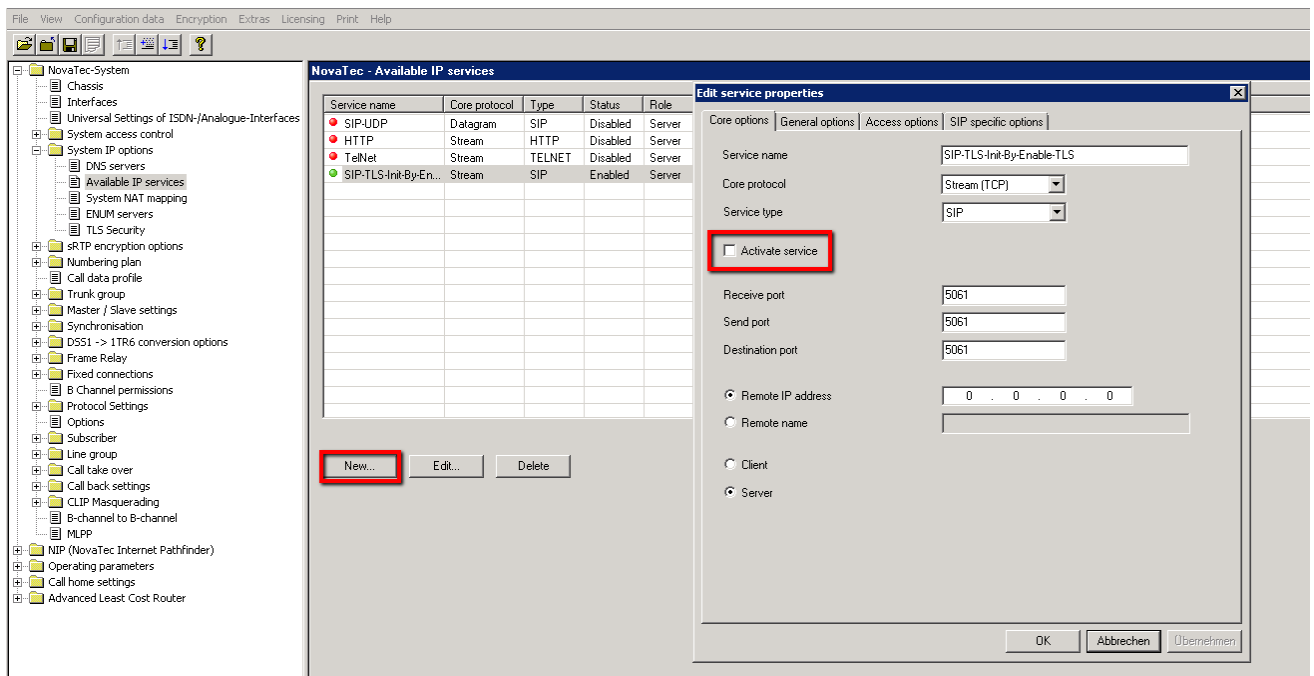
Picture 40 – Deactivating TLS in the configuration

4.6.2 Changing the IP transport service

Now please turn off transmission protocol TCP for TLS and activate UDP.

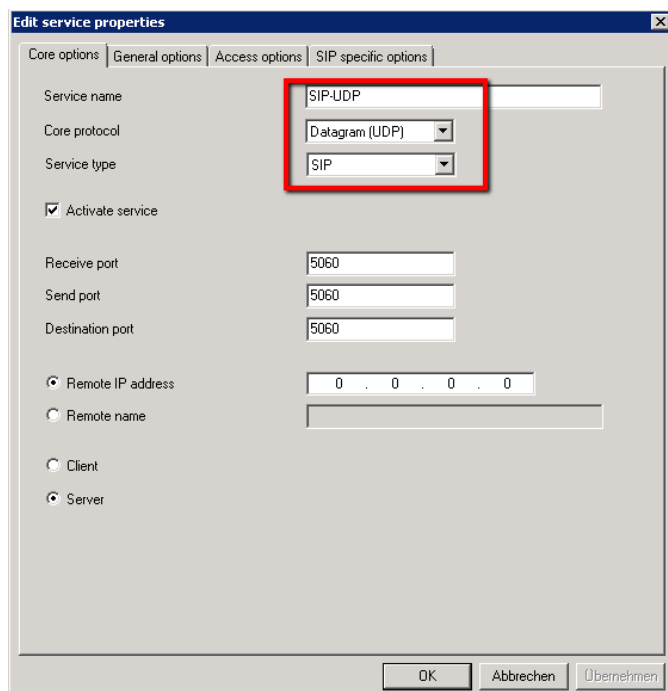
The change to SIP-UDP takes place automatically from Version 6.6, if using an older version please execute the following steps:

- Go to NovaTec-System -> System IP options -> Available IP services.
- Double-click TLS-SIP service (description may vary) and delete tick in check box „Activate service“.
- Confirm with “OK”.



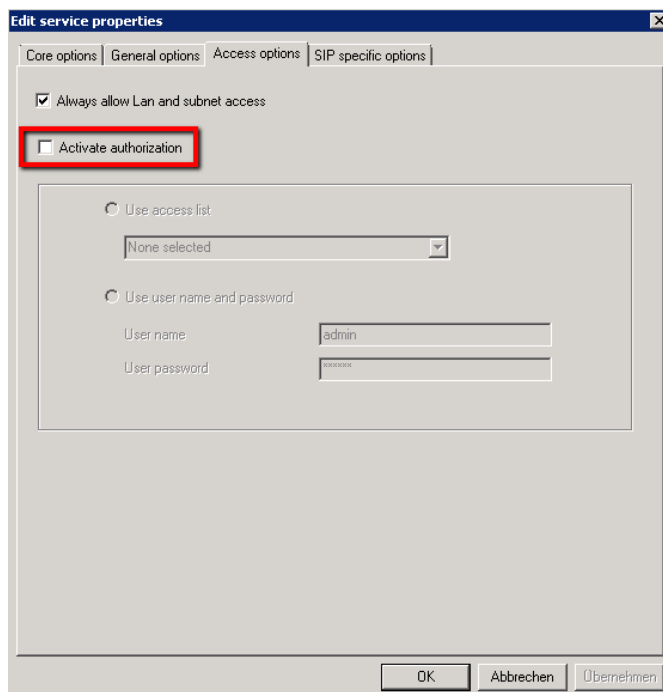
Picture 41 – Checking the unsecured IP service

- If there is no active UDP service in the IP services list please double click inactive UDP service and set tick in box „Activate service“. Confirm with „OK“.
- In case no UDP service is available please click button „New...“ to set up this service for SIP.
- Enter Name for the service and choose „Datagram (UDP)“ as new IP protocol.



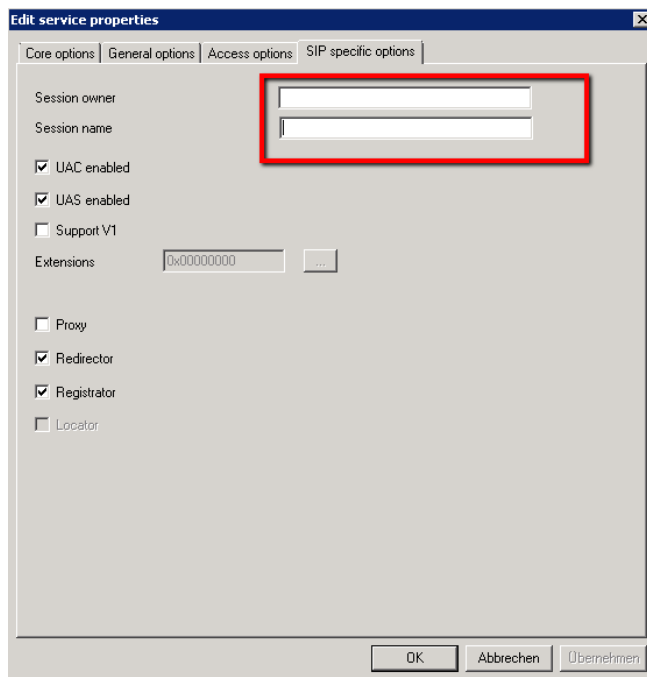
Picture 42 – Setting up UDP service for SIP

- Delete tick in box "Activate authorization" on tab "Access options".



Picture 43 - Access Options

- Choose Name for „Session Owner“ freely on tab “SIP specific options”.
- Confirm with “Ok”.

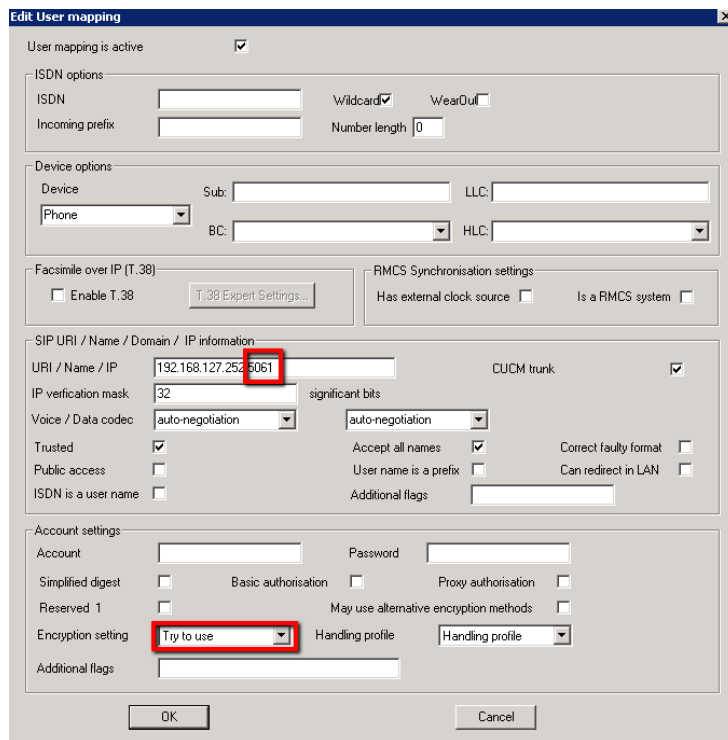


Picture 44 - SIP Session Owner

The new unsecured transmission protocol is now installed.

4.6.3 Deleting TLS ports and changing from sRTP to RTP

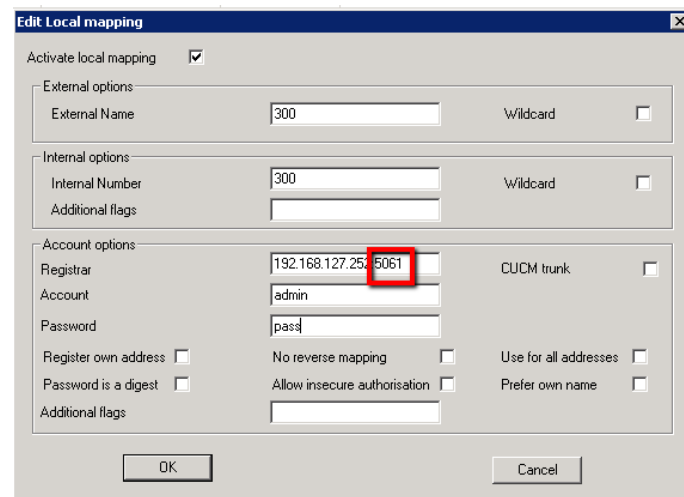
- Go to „NIP“ → „SIP“ → „Mapping lists“ → „User mapping“.
- Delete port “:5061” in box „URI/Name/IP“.
- To deactivate sRTP confirm “Do not use” for “Encryption setting”.



The screenshot shows the 'Edit User mapping' dialog box. The 'URI / Name / Domain / IP information' section has a red box around the IP address '192.168.127.252:5061'. The 'Account settings' section has a red box around the 'Encryption setting' dropdown menu, which is currently set to 'Try to use'.

Picture 45 – Deactivating user mapping sRTP

- Go to „NIP“ → „SIP“ → „Mapping lists“ → „Local mapping“.
- Delete port “:5061” in box „Registrar“.



The screenshot shows the 'Edit Local mapping' dialog box. The 'Registrar' field in the 'Account options' section has a red box around the IP address '192.168.127.252:5061'.

Picture 46 - Local mapping

5 Creating certificates

When restarting the NovaTec system for all three instances – if configured – certificate signing requests (CSR) are created. These can be signed by a certificate authority (CA). You then receive the required TLS certificate. TI-CA, a Windows server with SCEP or NAMES can also be used as registration authority.

5.1 Signing with TI-CA

With TI-CA you can sign certificate signing requests (CSR files) for certificates.

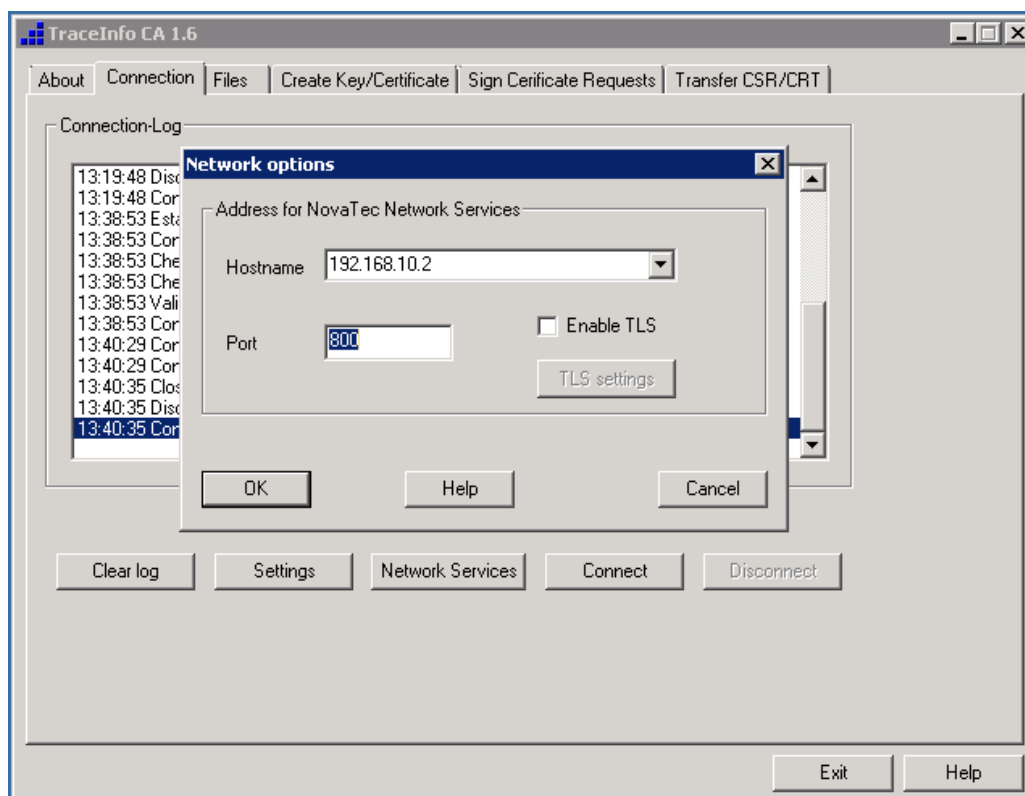
TI-CA can also sign CSR files which are saved locally on a PC or sign CSR files directly on a NovaTec system.

1. Case – The CSR is saved locally on a PC and the certificate is saved there, too.
 2. Case – The CSR of a NovaTec system is at hand locally but the signed certificate is written back onto the corresponding NovaTec system.
 3. Case – The CSR is on a NovaTec system and the signed certificate is written back there.
 4. Case – Like case 3, but the CSR of all three instances (MNT, SIP, NMS) are signed in one go on the system.
- Start TI-CA application.
 - If the following message is shown, the USB dongle is missing, which is necessary to unlock the application.



Picture 47 - TI-CA was started without dongle

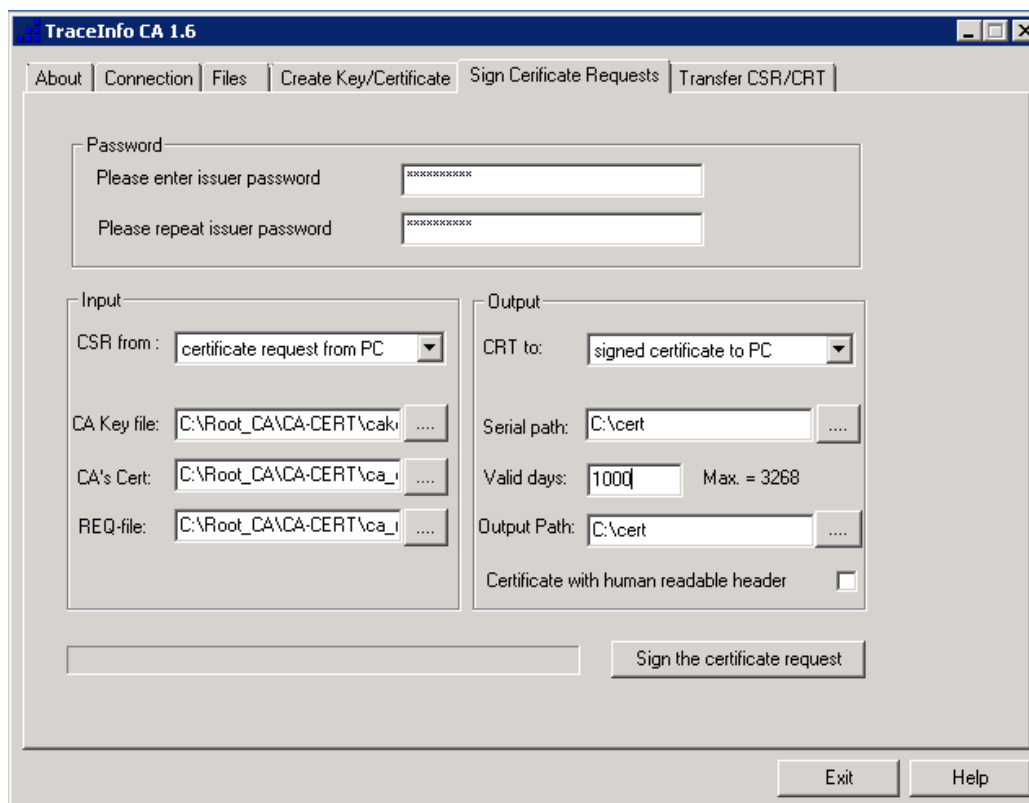
- Only in case 1 an online connection to the NovaTec system is not required.
- In all other cases, if the issued certificate is on a NovaTec system before or after the CSR was signed, you establish a connection to the target system with TI-CA. Please enter the IP address of the target system on tab „Connection“ → „Settings“.
- Afterwards establish the connection with „Connect“. You may have to enter your chosen login under „Username“ and „Password“.



Picture 48 – Addressing the target system

- All other adjustments for signing with TI-CA can be made on tab „Sign Certificate Requests“.
- Please enter the CA password connected to the „CA private key“ (cakey.pem).
- Repeat the password entry. Should this step go awry, an error message is shown in the bottom line and the button “Sign the certificate request” is deactivated.
- The further entry mask is composed of the „input“ box on the left and the „Output“ box on the right. Under “Input” you can enter the data for the CSR and the storage location for the CA certificate and the corresponding private key file. Under “Output” you can enter the data for the certificate to be issued.

Case 1) The locally available CSR, which is to be signed, does not have to be created with TI-CA. Certificate signing requests created by external applications can also be signed in this particular way.



Picture 49 - TI-CA "Sign Certificate Requests" PC-to-PC

- Please select as follows in the input box:

- Choose "certificate request from PC" under „CSR from:” .
- Choose the private key file for the „CA Private Key”.
- Select the CA certificate.
- Select the certificate demanding file under „REQ-file" (here: „Beispiel.csr”).

- Please select as follows in the output box:

- Choose "Signed certificate to PC" under "CRT to:".
- Enter path for the serial number file.(1)
- Enter the validity of the root certificate in days under „Valid days”.
- Enter the local destination directory for the backup of the signed certificate file under "Output Path”.



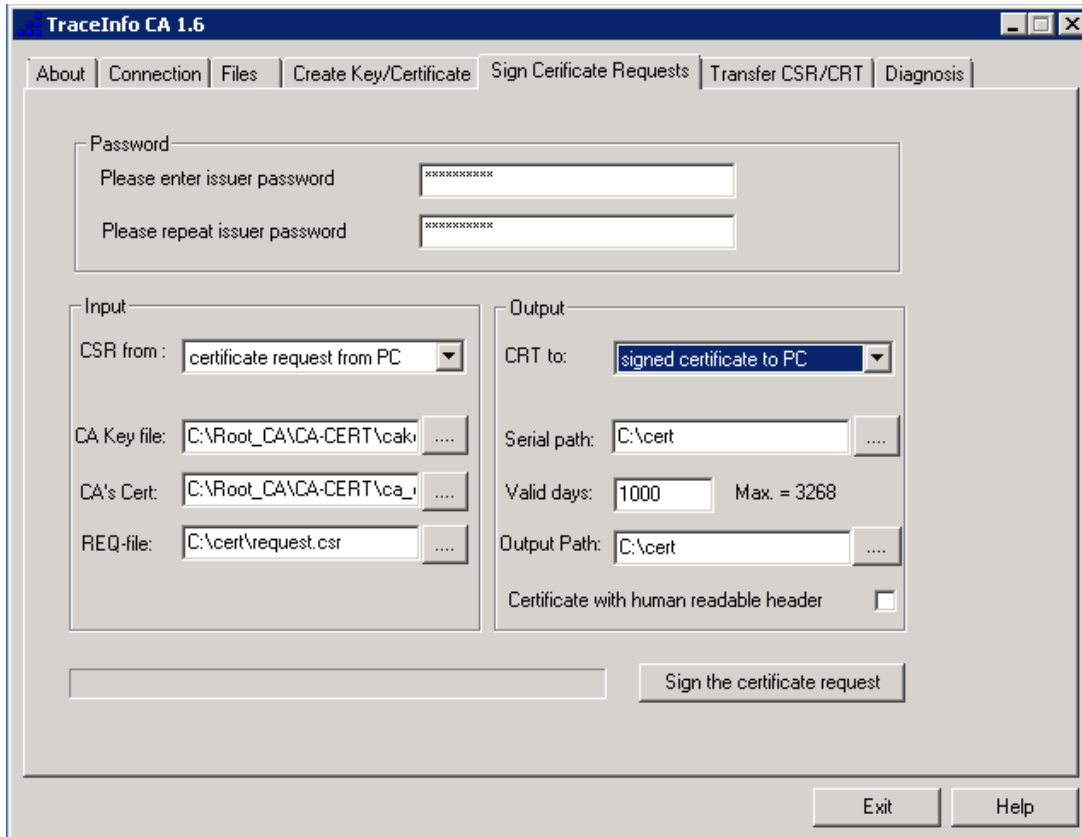
- Please deactivate "Certificate with human readable header".
- After you have carried out all settings as described above please press button "Sign the certificate request".

After the CSR has been signed the certificate "Beispiel.crt" lies in the entered destination directory.

Note (1):

The serial number is saved in a file by the name serial.txt. If this file is not detectable in the entered path the application will create a new file with a default number. The user can determine the number himself by creating a file name serial.txt with a 16-digit hexadecimal number, e.g. 0123456789ABCDEF. The application will use the serial number currently given in the serial.txt file. After the current serial number has been used the application will count up the serial.txt file.

Case 2) The CSR of a NovaTec system is available locally; the signed certificate is afterwards rewritten to the corresponding NovaTec system. This option is provided by TI-CA – but with at present without practical use.



Picture 50 - TI-CA "Sign Certificate Requests" PC-to-Target

- Connect TI-CA with the target system. Enter the IP address of the target system on tab „Connection“ → „Settings“ (see also Picture 48 – Addressing the target system).
 - All further adjustments for signing with TI-CA are made on tab „Sign Certificate Requests“.
 - Please enter the CA password connected to the „CA private key“ (cakey.pem).
 - Repeat the password entry. Should this step go awry, an error message is shown in the bottom line and the button "Sign the certificate request" is deactivated.
- Please select as follows in the input box:
- Choose "certificate request from PC" under „CSR from:" .
 - Choose the private key file for the „CA Private Key“.
 - Select the CA certificate.
 - Select the certificate demanding file under „REQ-file“ (here: „Beispiel.csr“).



- Please select as follows in the output box:

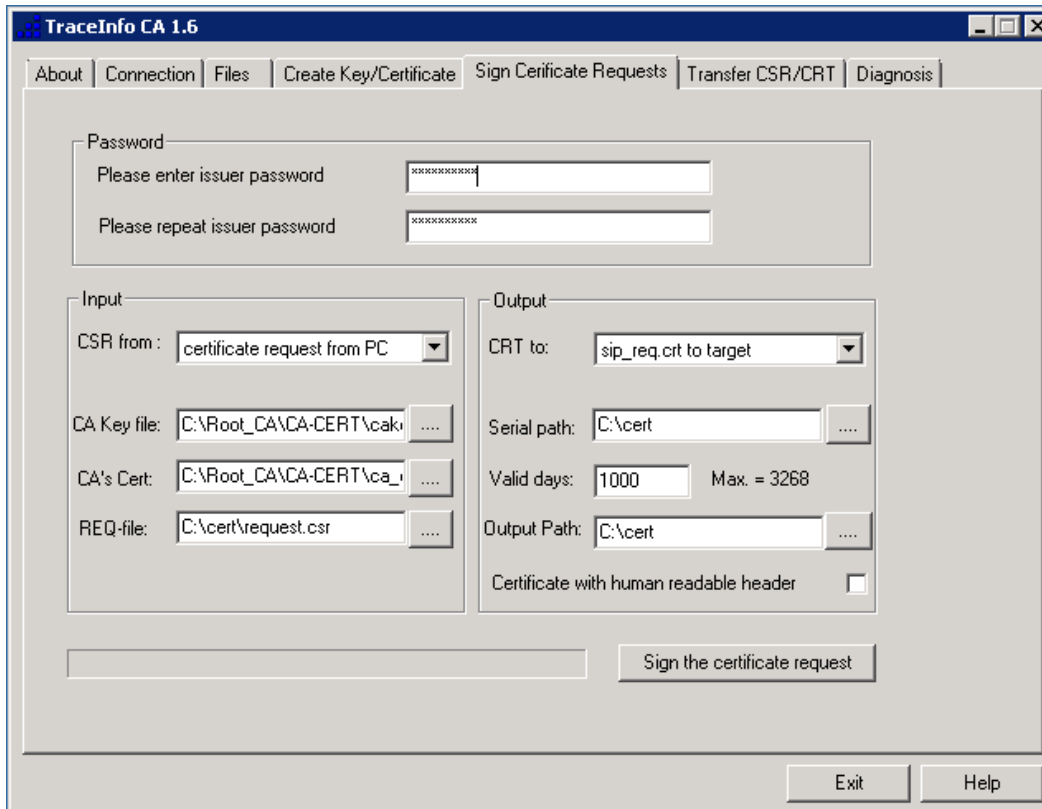
- As example select „sip_req.crt to target“ for SIP under “CRT to:”.
- Enter the path for the serial number file.(1)
- Enter the validity of the root certificate in days under „Valid days”.
- Enter local destination directory for the temporary storage of the signed certificate file under „Output Path”. This file is transferred to the target system and then deleted locally.
- Please deactivate “Certificate with human readable header”.
- After finishing all settings as described above please press button "Sign the certificate request".

After the certificate signing request (CSR) has been signed the SIP certificate „sip_req.crt”, here used as example, is written onto the target system.

Note (1):

The serial number is saved in a file by the name serial.txt. If this file is not detectable in the entered path the application will create a new file with a default number. The user can determine the number himself by creating a file name serial.txt with a 16-digit hexadecimal number, e.g. 0123456789ABCDEF. The application will use the serial number currently given in the serial.txt file. After the current serial number has been used the application will count up the serial.txt file.

Case 3 and 4) These two cases can be treated in one fell swoop. The only difference is, that in case 3 one CSR and in case 4 several CSR are signed together in one go. The CSR files are available on a NovaTec Gateway. The created certificates are also deposited on this NovaTec gateway after being signed



Picture 51 - TI-CA Sign Certificate Requests PC-to-Target

- Connect TI-CA with the target system. Tragen Sie unter dem Reiter „Connection“ → „Settings“ die IP-Adresse des Zielsystems ein (siehe Picture 48 – Addressing the target system).
 - All further adjustments for signing with TI-CA are made on tab „Sign Certificate Requests“.
 - Please enter the CA password connected to the „CA private key“ (cakey.pem).
 - Repeat the password entry. Should this step go awry, an error message is shown in the bottom line and the button “Sign the certificate request” is deactivated.
- Please select as follows in the input box:
- Choose “certificate request from PC” under „CSR from:“.
 - Choose the private key file for the „CA Private Key“.
 - Select the CA certificate.
 - Select the certificate demanding file under „REQ-file“ (e.g.: „sip_req.csr“) .



- Please select as follows in the output box:

- As example select „sip_req.crt to target“ for SIP under “CRT to:”.
- Enter the path for the serial number file.(1)
- Enter the validity of the root certificate in days under „Valid days”.
- Enter local destination directory for the temporary storage of the signed certificate file under „Output Path”. This file is transferred to the target system and deleted locally afterwards.
- Please deactivate “Certificate with human readable header”.
- After finishing all settings as described above please press button "Sign the certificate request".

After the certificate signing request (CSR) has been signed the SIP certificate „sip_req.crt”, here used as example, is written onto the target system.

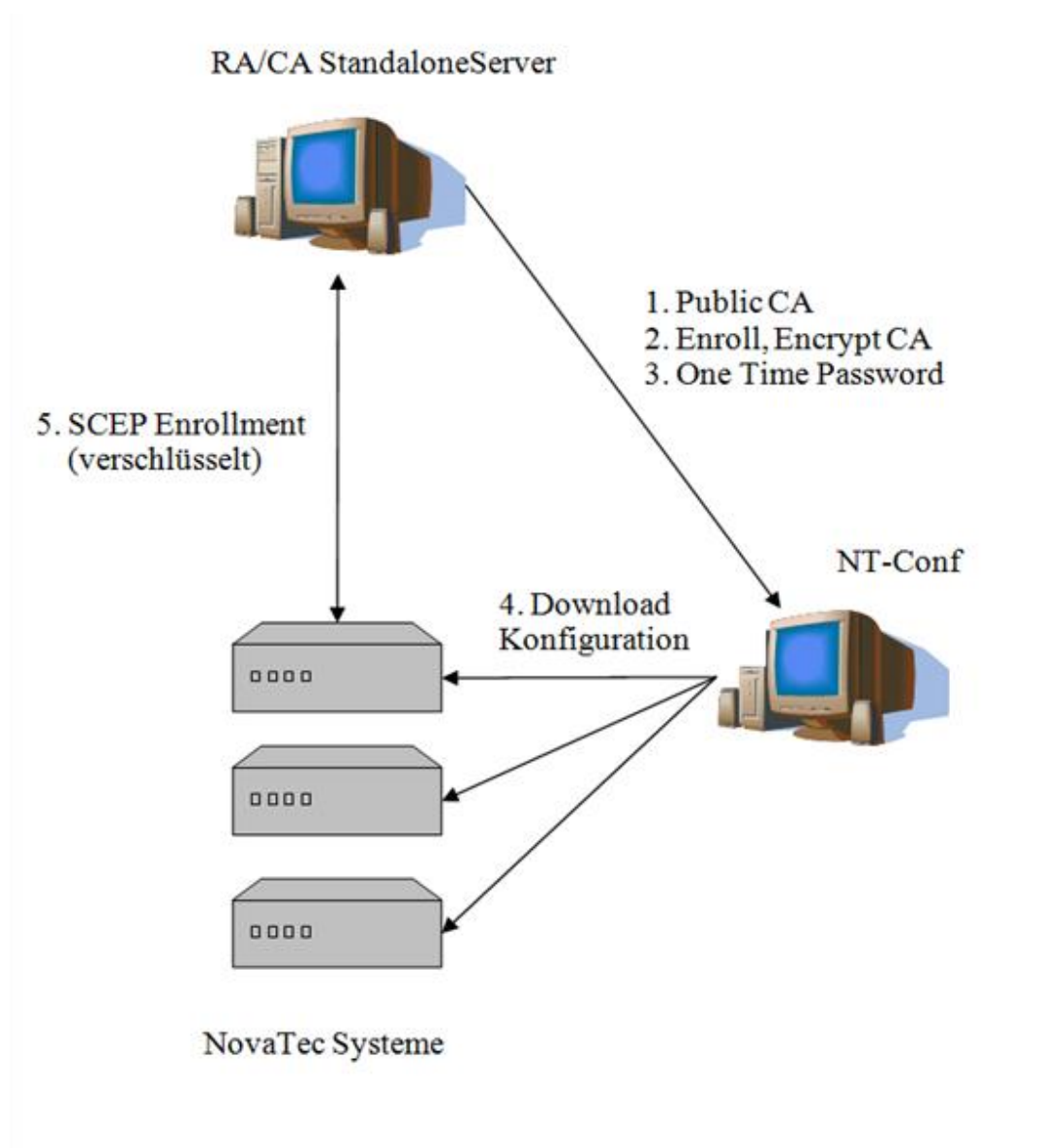
Note (1):

The serial number is saved in a file by the name serial.txt. If this file is not detectable in the entered path the application will create a new file with a default number. The user can determine the number himself by creating a file name serial.txt with a 16-digit hexadecimal number, e.g. 0123456789ABCDEF. The application will use the serial number currently given in the serial.txt file. After the current serial number has been used the application will count up the serial.txt file.

5.2 Signing process with SCEP

The following 8 steps are passed through during configuration of SCEP and signing with SCEP:

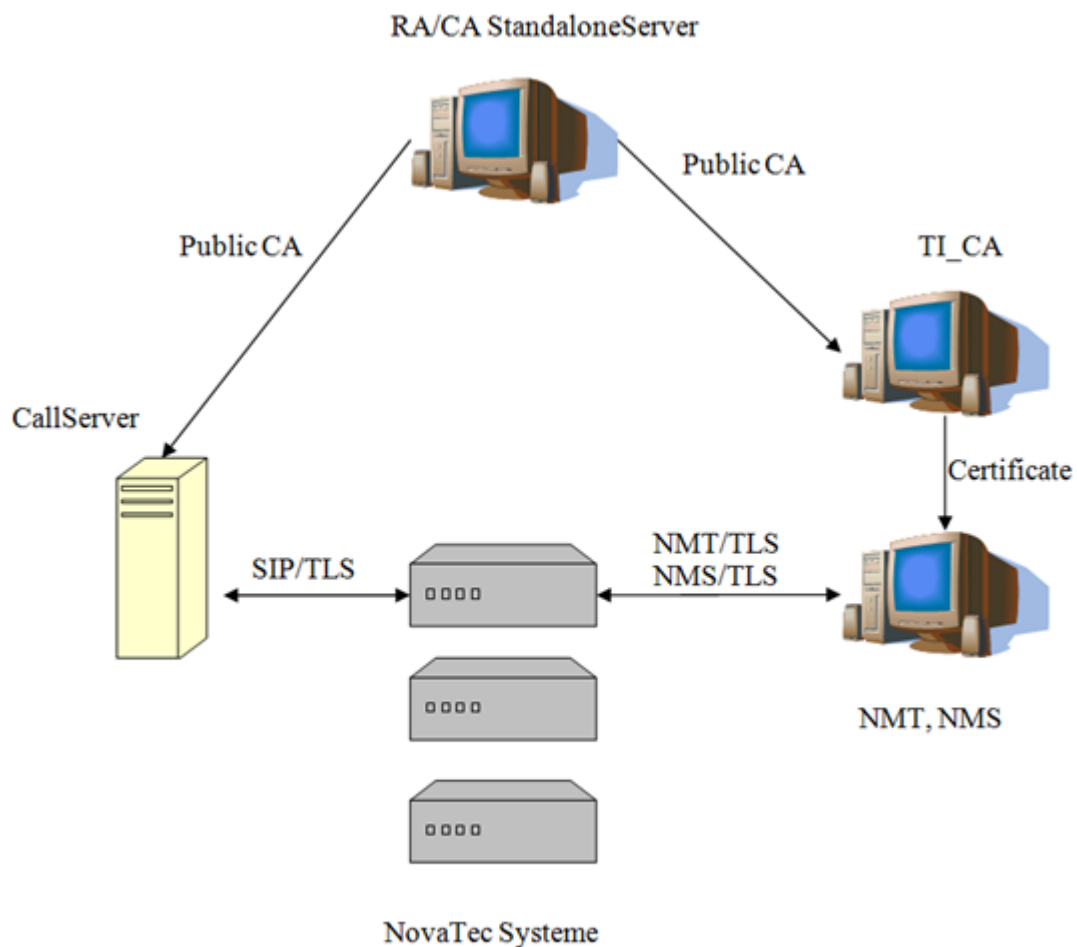
1. Step: Public certificate for all three instances are imported into the configuration.
2. Step: Enrollment and encryption certificates are imported into the configuration.
3. Step: (Optional) Import „One Time Password“ from web browser into the configuration.
4. Step: Upload the configuration onto the NovaTec systems with reset.
5. Step: SCEP Enrolment with automatical reset.



Picture 52 - SCEP Enrolment NovaTec Gateways

After the TLS certificates on the NovaTec gateways have been signed and the necessary certificates (here only the public CA) for the verification of the PKI chain have been imported to these, the CallServer and the workstation, with which the gateways are supervised, have to be equipped with the complete certificate chain. Apart of this the TLS certificate for NMT and NMS on the workstation is signed by TI-CA.

6. Step: Import the public CA certificate into the CallServer (e.g. CUCM, see chapter 6.3 Importing and exporting certificates).
7. Step: Create the NMT and NMS certificates with TI-CA out of the public CA certificate (see **Fehler! Verweisquelle konnte nicht gefunden werden.**).
8. Step: Performance test of NMT, NMS and SIP with TLS.



Picture 53 - SCEP Enrollment CallServer & NovaTec Management PC



5.3 Signing systems with NAMES

Carry out the configuration steps described in the NAMES user manual. After this NAMES can process the signing of the certificates automated. All three CSR files on the gateways are signed, which have previously been created if given by the systems configuration.



6 Configuring secured connections in the CUCM

In order to allow the establishment of TLS and sRTP secured connections between NovaTec gateways and the Cisco Call Manager, the Cisco Unified Communication Manager (CUCM) cluster security mode has to be set to "mixed mode". As precondition the Cisco CTL client has to be installed, which creates a list of certificates (Certificate Trust List) within the CUCM. Two Cisco security dongles/tokens and the corresponding passwords are required. Connect these dongles to a USB port only on explicit prompt.

For detailed information please check the CUCM help desk or pursue the short instruction in the next section.

6.1 Installing the CISCO CTL client

Please carry out the following steps in order to install the Cisco CTL client:

1. Open the Cisco Unified Communications Manager administration as described in the Cisco Unified Communications Manager administration guide on the Windows PC or the Windows server, on which you wish to install the client.
2. Select „Application > Plugins“ in the Cisco Unified Communications Manager Administration. The "Find and List" plugin is shown.
3. Please enter „Installation“ in the drop down menu of the plugin and click „Find“.
4. Localise the Cisco CTL client.
5. Press "Download" on the right side of the window on height of the Cisco CTL client plugin in order to download the file.
6. Choose „save“ and enter a path. Please remember the entered path.
7. Ensure that the security agent is turned off. E.g.: No enterprise security agent is running on this server.
8. To begin the installation double click "Cisco CTL Client" (icon or executable file, depending on where the download was saved). Note: You can also use the „Open“ button in the „Download completed“ prompt.
9. The version of the Cisco CTL Clients is shown; click button "next".
10. The installation agent is shown. Click button "next".
11. Accept license agreement and click „next“.
12. Select directory, in which you want to install the client. To change the default settings select "search". After choosing the place of installation press „next“.
13. Click „next“ to begin with the installation.
14. As soon as the installation is completed please press „Finish“.



Please check the following before beginning to connect the CTL client with the CUCM:

1. Go to Cisco Unified Serviceability → Tools → Service Activation and ensure the following services are active:
 - Cisco CTL Provider is ACTIVE
 - Cisco Certificate Authority Proxy Function is ACTIVE

Security Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco CTL Provider	Activated
<input checked="" type="checkbox"/>	Cisco Certificate Authority Proxy Function	Activated

Picture 54 - CTL Provider Activated

2. Go to CUCM Admin page → System → Service Parameter Configuration
 - Choose the fitting CUCM as server.
 - Wählen Sie als Service den „Cisco CTL Provider Service“.
 - Port number has to be 2444.

The screenshot shows the 'Service Parameter Configuration' page in Cisco Unified CM Administration. The page title is 'Cisco Unified CM Administration For Cisco Unified Communications Solutions'. The navigation bar includes 'System', 'Call Routing', 'Media Resources', 'Advanced Features', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The 'Service Parameter Configuration' section is active, showing 'Status: Ready'. Below this, the 'Select Server and Service' section has 'Server*' set to '192.168.131.1 (Active)' and 'Service*' set to 'Cisco CTL Provider (Active)'. A note states: 'All parameters apply only to the current server except parameters that are in the cluster-wide group(s)'. The 'Cisco CTL Provider (Active) Parameters on server 192.168.131.1 (Active)' section contains a table with one parameter:

Parameter Name	Parameter Value	Suggested Value
Port Number *	2444	2444

Buttons for 'Save' and 'Set to Default' are visible at the bottom of the configuration area.

Picture 55 - CTL Service Parameter

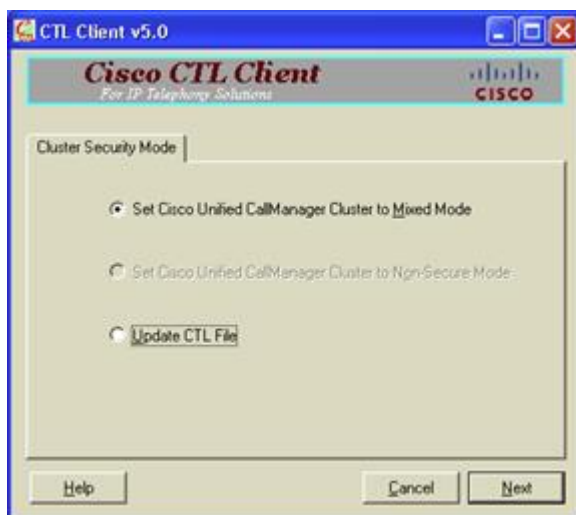
Adding security certificates to the CUCM and activating „Mixed Mode“

1. Start the CTL Client.



Picture 56 – CTL Client connect

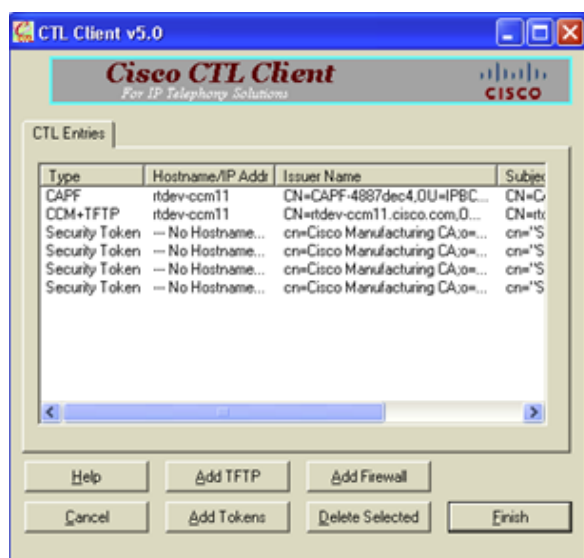
- Please do not use the DNS name of the CUCM, but solely its IP address.
 - The default port should be 2444.
 - Username and password are the username and password of the CUCM.
2. The CTL client will confirm the user and connect with the CUCM.
 3. The prompt given below is shown. Please select "Set Cisco Unified CallManger Cluster to Mixed Mode". Press button "Next".



Picture 57 - CTL Mixed Mode

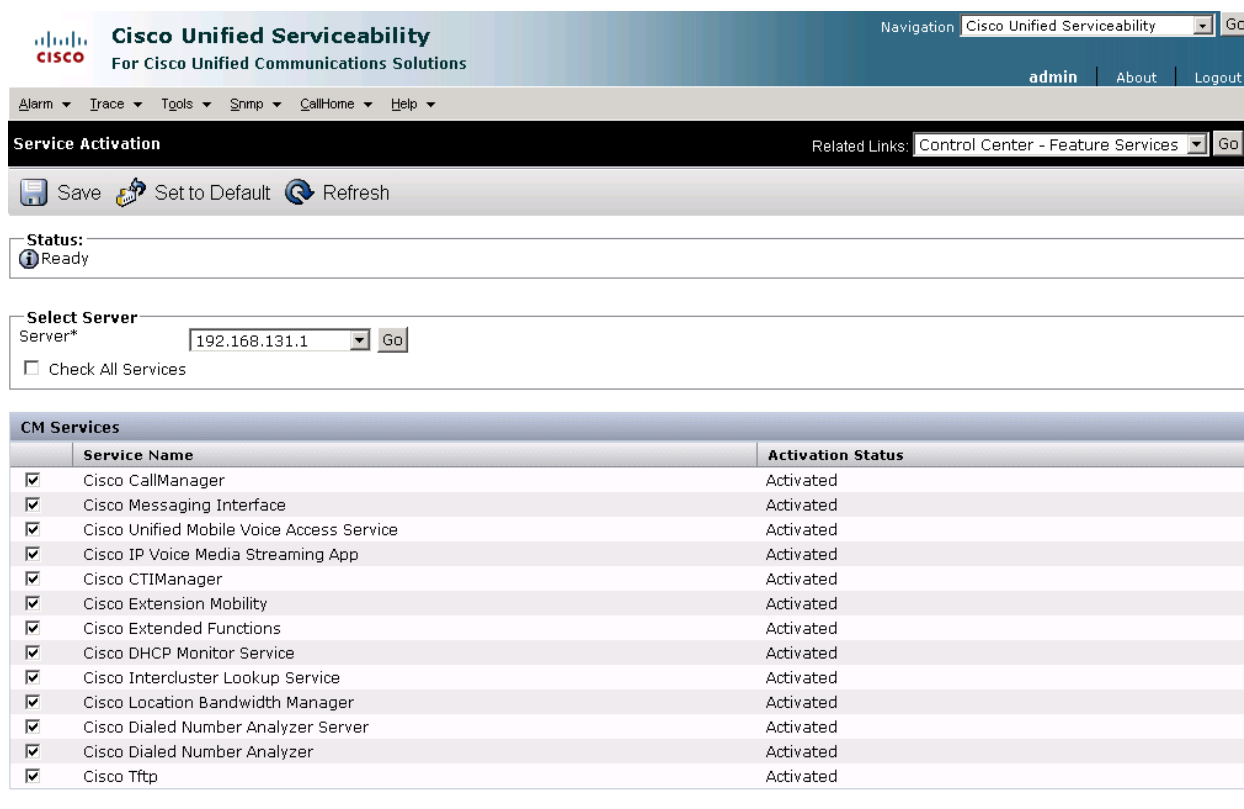
4. The CTL Client will ask you to add a proof of safety. Now please connect the dongle to the USB port of the PC/server, on which the CTL Client is installed.

5. The CTL Client will now query the password for the dongle. Use the password given on the sticker (e.g. "Cisco_xyz"). Please take special care when entering the password, as two wrong entries will disable the dongle.
6. When prompted to do so remove first dongle from the USB port and connect the second on demand.
7. At the end of the process a „Finish“ option is shown but also the possibility to add security tokens.
8. Repeat steps as above if adding further certificates and select „Finish“ or add even more.
9. After finalising this process you will see the corresponding number of security tokens next to the entries CAPF and CCM TFTP as also shown in the picture below. Attention: The picture shows four security tokens. Depending on how many tokens you have loaded the quantity will differ.



Picture 58 - CTL Entries

10. Remove all dongles from the USB ports and keep these safe.
11. Close the CTL Client.
12. Start the CUCM and TFTP service via the CUCM Administration page anew.



The screenshot shows the Cisco Unified Serviceability web interface. At the top, there is a navigation bar with the Cisco logo and the text "Cisco Unified Serviceability For Cisco Unified Communications Solutions". The user is logged in as "admin". Below the navigation bar, there are several tabs: "Alarm", "Trace", "Tools", "Snmp", "CallHome", and "Help". The main content area is titled "Service Activation" and includes a "Related Links" section with a dropdown menu set to "Control Center - Feature Services". Below this, there are buttons for "Save", "Set to Default", and "Refresh". The "Status" section shows "Ready". The "Select Server" section has a dropdown menu set to "192.168.131.1" and a "Go" button. Below this, there is a table titled "CM Services" with columns for "Service Name" and "Activation Status". All services listed are checked and show "Activated".

	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco CallManager	Activated
<input checked="" type="checkbox"/>	Cisco Messaging Interface	Activated
<input checked="" type="checkbox"/>	Cisco Unified Mobile Voice Access Service	Activated
<input checked="" type="checkbox"/>	Cisco IP Voice Media Streaming App	Activated
<input checked="" type="checkbox"/>	Cisco CTIManager	Activated
<input checked="" type="checkbox"/>	Cisco Extension Mobility	Activated
<input checked="" type="checkbox"/>	Cisco Extended Functions	Activated
<input checked="" type="checkbox"/>	Cisco DHCP Monitor Service	Activated
<input checked="" type="checkbox"/>	Cisco Intercluster Lookup Service	Activated
<input checked="" type="checkbox"/>	Cisco Location Bandwidth Manager	Activated
<input checked="" type="checkbox"/>	Cisco Dialed Number Analyzer Server	Activated
<input checked="" type="checkbox"/>	Cisco Dialed Number Analyzer	Activated
<input checked="" type="checkbox"/>	Cisco Tftp	Activated

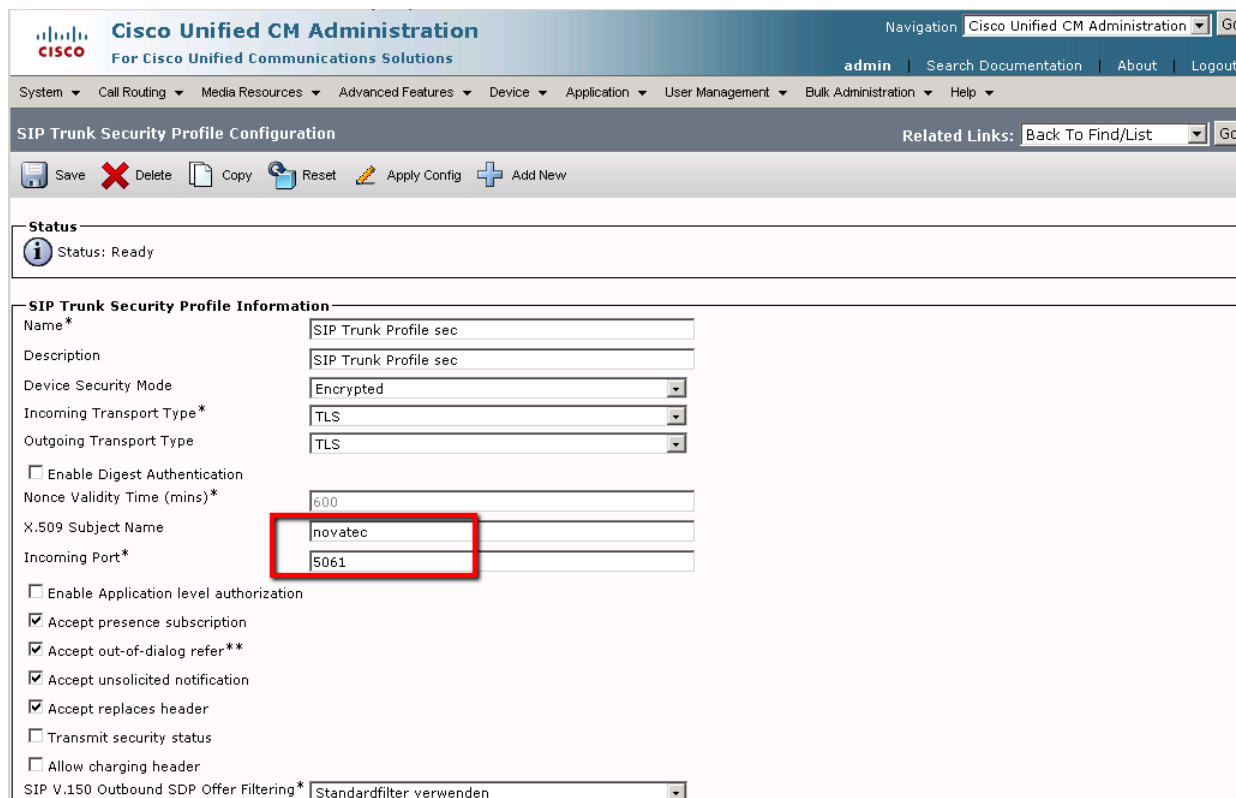
Picture 59 - CUCM Service activation

6.2 Activating in configuration

6.2.1 NovaTec on TRUNK connection

Please select → CM Administration → Security → Sip Trunk Security Profile

- The X.509 subject name has to be identical to the „Common Name“ as given in the configuration of the connected NovaTec gateway for its SIP-CSR.
- Set "Incoming Port:" to 5061.

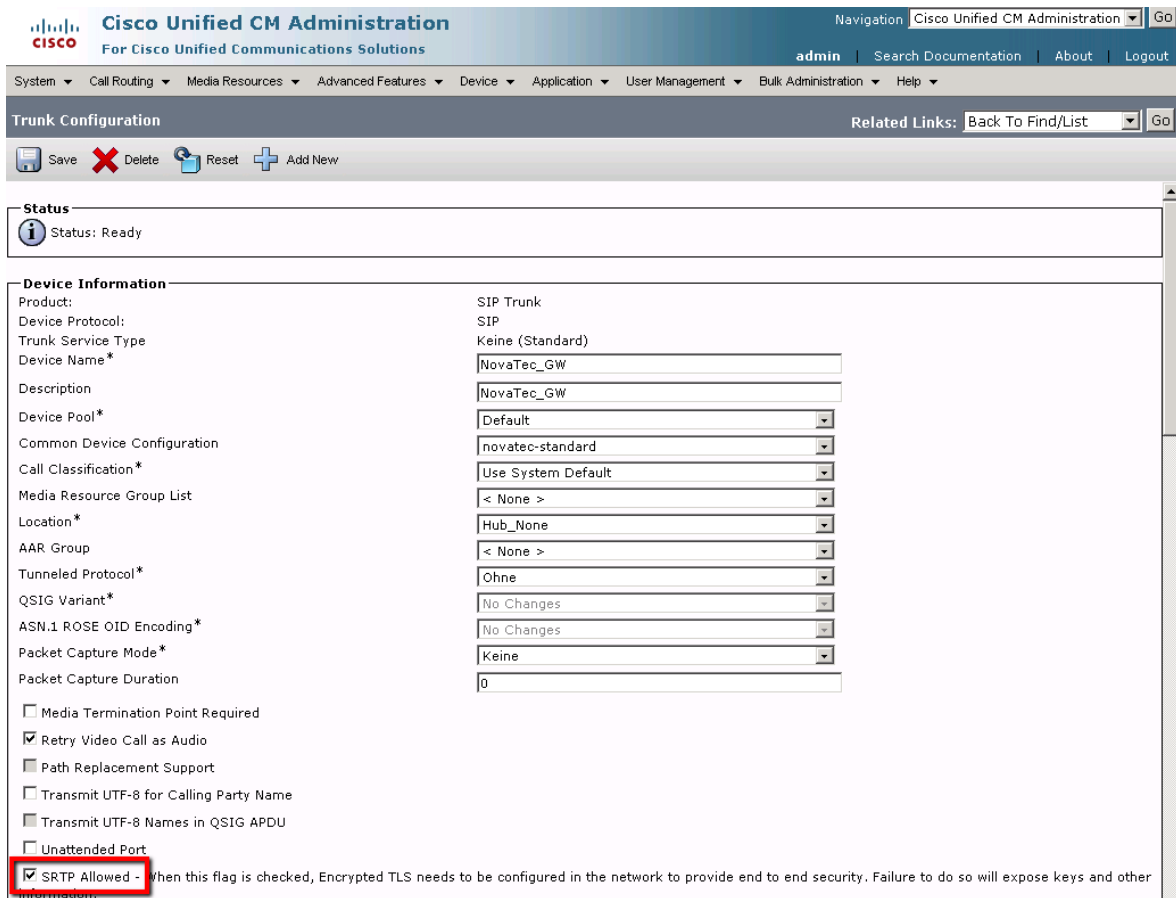


The screenshot shows the Cisco Unified CM Administration interface for configuring a SIP Trunk Security Profile. The page title is "SIP Trunk Security Profile Configuration". The status is "Ready". The configuration fields are as follows:

Field	Value
Name*	SIP Trunk Profile sec
Description	SIP Trunk Profile sec
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
Enable Digest Authentication	<input type="checkbox"/>
Nonce Validity Time (mins)*	600
X.509 Subject Name	novatec
Incoming Port*	5061
Enable Application level authorization	<input type="checkbox"/>
Accept presence subscription	<input checked="" type="checkbox"/>
Accept out-of-dialog refer**	<input checked="" type="checkbox"/>
Accept unsolicited notification	<input checked="" type="checkbox"/>
Accept replaces header	<input checked="" type="checkbox"/>
Transmit security status	<input type="checkbox"/>
Allow charging header	<input type="checkbox"/>
SIP V.150 Outbound SDP Offer Filtering*	Standardfilter verwenden

Picture 60 - CUCM Trunk Security Profile

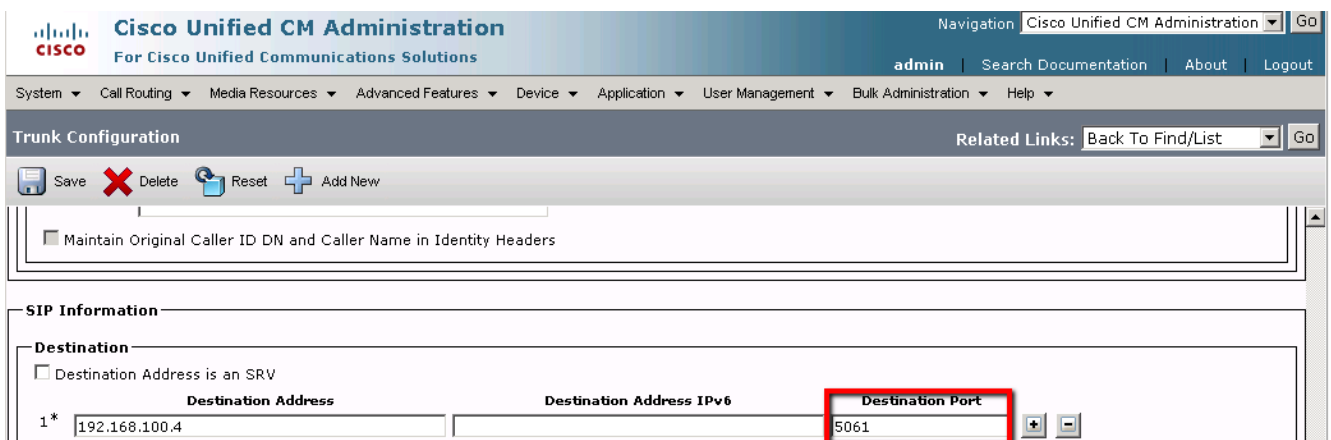
Set "Destination Port" to 5061 in the trunk configuration and select the corresponding trunk security profile.



Picture 61 - CUCM Trunk sRTP Allowed

„SRTP Allowed“ is set in the trunk configuration to enable the actual voice or data stream to be secured with sRTP next to the TLS secured connection establishment via SIP.

As „Destination Port“ 5061 is set for TLS.



Picture 62 - CUCM Trunk Port 5061

6.2.2 NovaTec on a phone connection

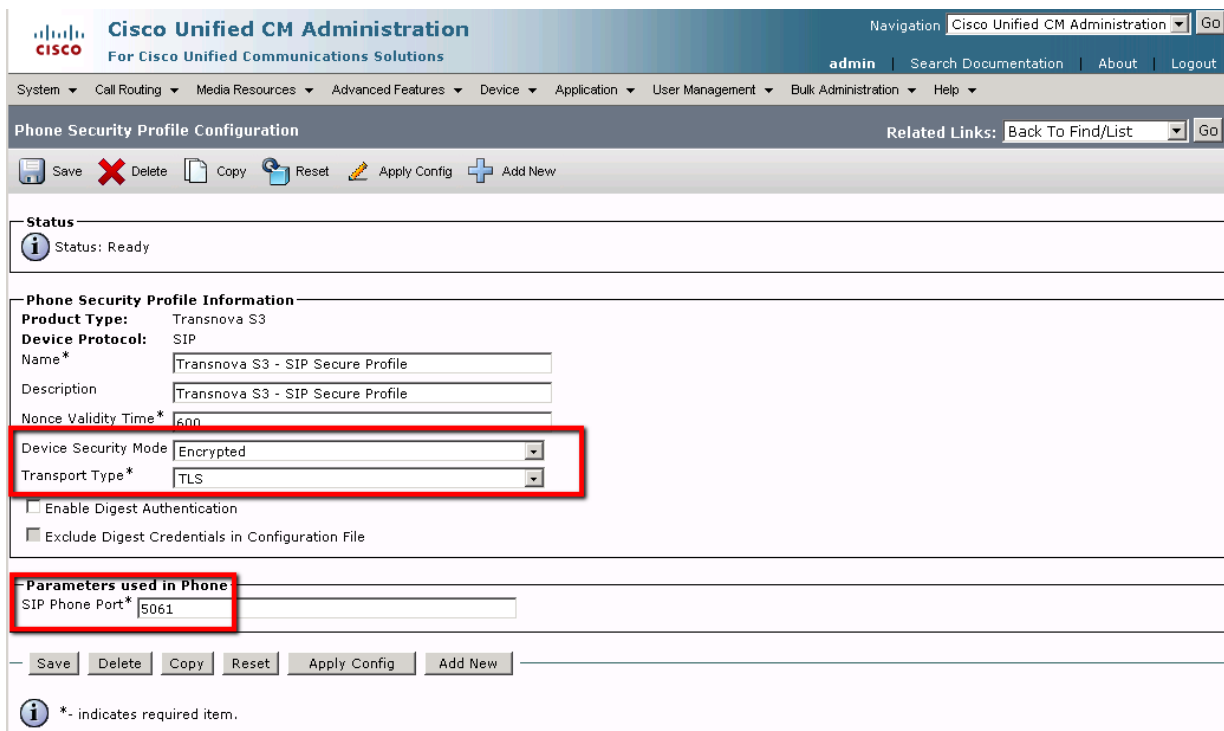
A NovaTec S3 can be connected to a phone line of the CUCM. To secure this connection with TLS and sRTP please proceed as follows.

In cast no security profile exists such is created by copying a „Transnova S3 – Standard SIP Non-Secure Profile“ and saving it as „Transnova S3 – SIP Secure Profile“.

The following security adjustments are made in this profile.

Select → Device → Phone → Security Profile

- Set "Device Security Mode" to "Encrypted"
- As "Transport Type" choose "TLS"
- As „SIP Phone Port“ enter 5061



The screenshot shows the Cisco Unified CM Administration interface for configuring a Phone Security Profile. The page title is "Phone Security Profile Configuration" and the status is "Ready". The "Phone Security Profile Information" section includes the following fields:

- Product Type: Transnova S3
- Device Protocol: SIP
- Name*: Transnova S3 - SIP Secure Profile
- Description: Transnova S3 - SIP Secure Profile
- Nonce Validity Time*: 600
- Device Security Mode: Encrypted (highlighted with a red box)
- Transport Type*: TLS (highlighted with a red box)
- Enable Digest Authentication:
- Exclude Digest Credentials in Configuration File:

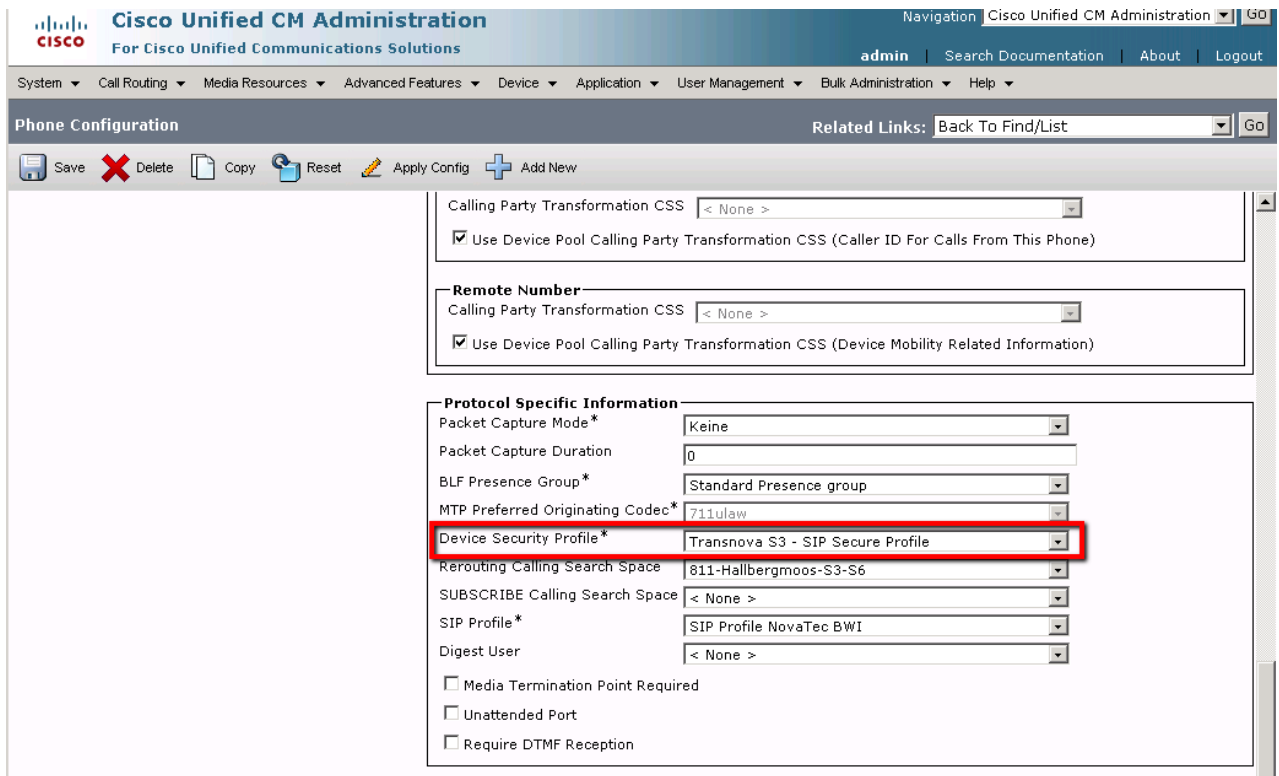
The "Parameters used in Phone" section includes:

- SIP Phone Port*: 5061 (highlighted with a red box)

At the bottom, there is a legend: ***** - indicates required item.

Picture 63 - Modify Transnova S3 - Non-Security Profile

The new „Transnova S3 – SIP Security Profile“ is now assigned to the "device Security Profile" in the „Phone Configuration“.



Picture 64 - Transnova S3 - Security Profile



6.3 Importing and exporting certificates

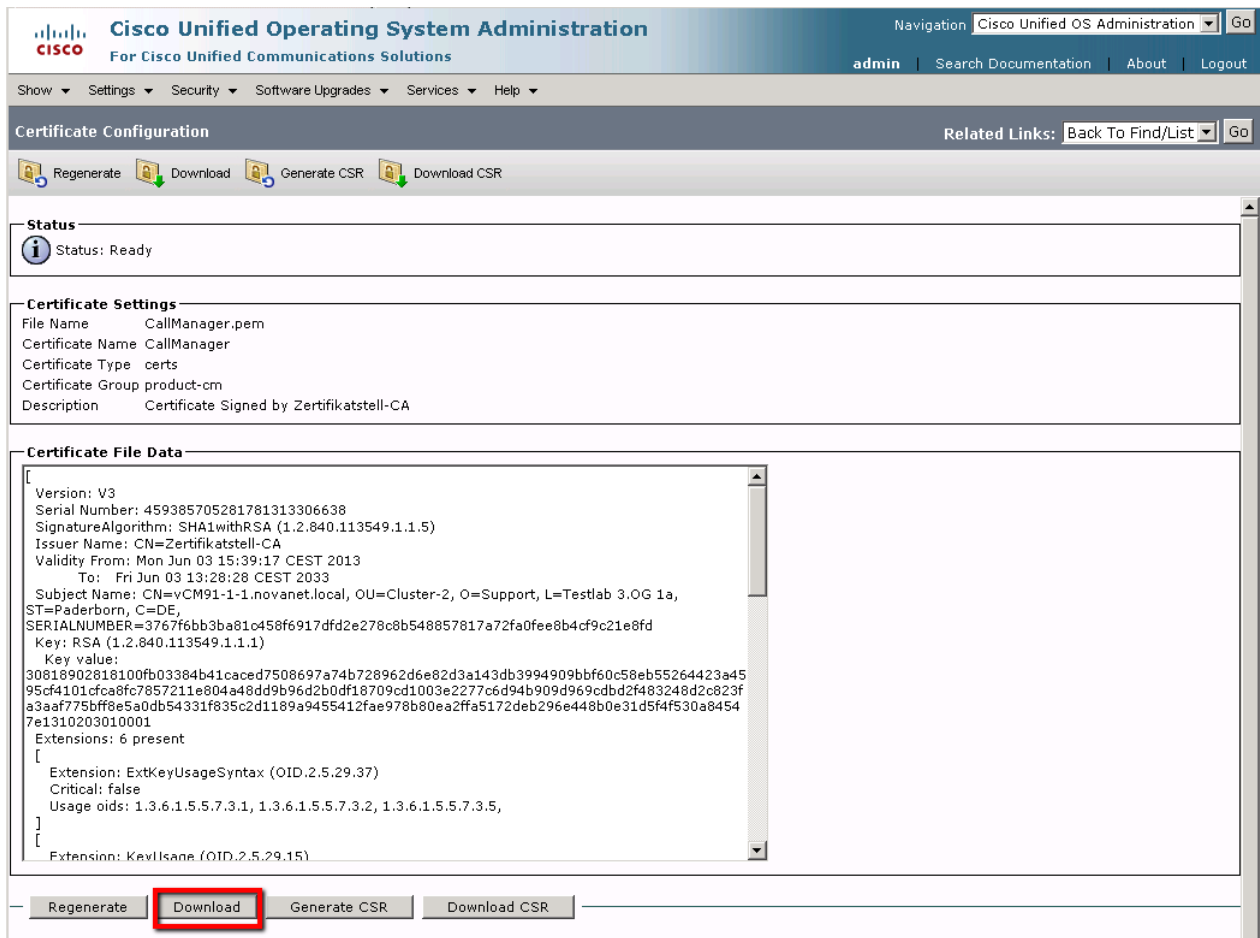
In case no common certification authority (CA) is available for a CUCM and a NovaTec gateway, a two-way exchange of the SIP-TLS-certificates is necessary. The CUCM for example might only have a self-signed certificate and the NovaTec gateway might be operated with a SIP-TLS-certificate, which was signed with TI-CA or an external CA. In this case both certificates have to be exported from the systems and imported into the opposite system.

6.3.1 Exporting CUCM certificates to a NovaTec system

6.3.1.1 Downloading a certificate from a CUCM

In order to download a certificate from the CUCM on to your PC please proceed as follows:

1. Go to OS-Administration → Security → Certificate Management in the CUCM. The list of certificates is shown.
2. You can use the search function to filter the certificate list.
3. Click onto the name of the certificate „CallManager.pem“. The certificate configuration is shown as window. Press button “Download”.
4. Open the download dialogue and save the exported file.
5. The CUCM certificates, which are saved on a PC, can be imported into the trust list of a NovaTec gateway as described in chapter 4.2.3 „ Loading the CA certificate into the trust list “.



Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified OS Administration | Go
admin | Search Documentation | About | Logout

Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾

Certificate Configuration Related Links: Back To Find/List ▾ Go

Regenerate Download Generate CSR Download CSR

Status
Status: Ready

Certificate Settings
File Name: CallManager.pem
Certificate Name: CallManager
Certificate Type: certs
Certificate Group: product-cm
Description: Certificate Signed by Zertifikatstell-CA

Certificate File Data

```
[
  Version: V3
  Serial Number: 459385705281781313306638
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: CN=Zertifikatstell-CA
  Validity From: Mon Jun 03 15:39:17 CEST 2013
  To: Fri Jun 03 13:28:28 CEST 2033
  Subject Name: CN=vCM91-1-1.novanet.local, OU=Cluster-2, O=Support, L=Testlab 3.0G 1a,
  ST=Paderborn, C=DE,
  SERIALNUMBER=3767f6bb3ba81c458f6917dfd2e278c8b548857817a72fa0fee8b4cf9c21e8fd
  Key: RSA (1.2.840.113549.1.1.1)
  Key value:
  30818902818100fb03384b41caced7508697a74b728962d6e82d3a143db3994909bbf60c58eb55264423a45
  95cf4101cfca8fc7857211e804a48dd9b96d2b0df18709cd1003e2277c6d94b909d969cddb2f483248d2c823f
  a3aaf775bff8e5a0db54331f835c2d1189a9455412fae978b80ea2ffa5172deb296e448b0e31d5f4f530a8454
  7e1310203010001
  Extensions: 6 present
  [
    Extension: ExtKeyUsageSyntax (OID.2.5.29.37)
    Critical: false
    Usage oids: 1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.5,
  ]
  [
    Extension: KeyUsage (OID.2.5.29.15)
  ]
]
```

Regenerate Download Generate CSR Download CSR

Picture 65 - Download CallManager certificate

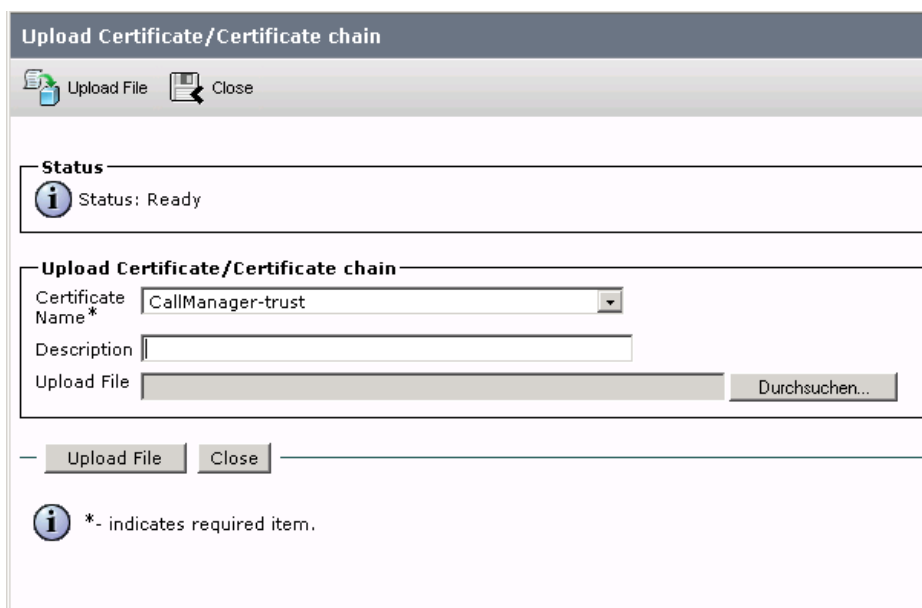
6.3.2 Importing a NovaTec certificate into the CUCM

To upload a certificate from your PC into the trust store of a CUCM please proceed as follows.

The CA certificate, with which the SIP-TLS-certificate of a NovaTec gateway has been signed, has to be uploaded into the CUCM trust store. Please also consider the security passage in the CUCM OS Admin Guide, in order to find out how a certificate can be loaded into the CUCM Trust Store.

- The CA certificate „xxxxx“ should be uploaded into the Call Manager and classified as trustworthy certificate.
- OS Administration → Security → Certificate Management → Upload Certificate
- Certificate name: Callmanager-trust
- Root Certificate (can be left empty)
- Upload File: E.g.: „siptcl_ca_cert.pem“

If multiple Call Managers are configured within a cluster „xxxxx“ has to be loaded onto all Call Managers within the cluster.



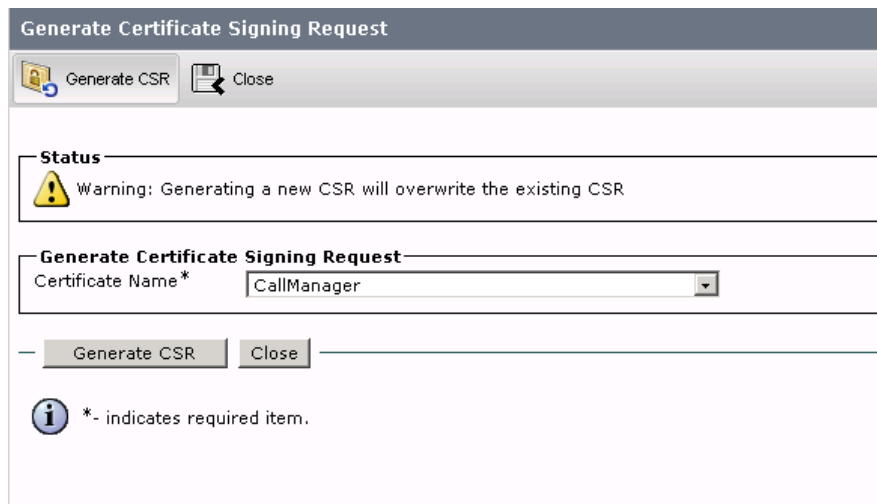
The screenshot shows a dialog box titled "Upload Certificate/Certificate chain". At the top, there are "Upload File" and "Close" buttons. Below that, a status box shows "Status: Ready". The main section is titled "Upload Certificate/Certificate chain" and contains a "Certificate Name*" dropdown menu with "CallManager-trust" selected, a "Description" text input field, and an "Upload File" field with a "Durchsuchen..." button. At the bottom, there are "Upload File" and "Close" buttons, and a note: "*- indicates required item."

Picture 66 - Upload CA certificate into CUCM trust list

6.4 External CA signs Call Manager

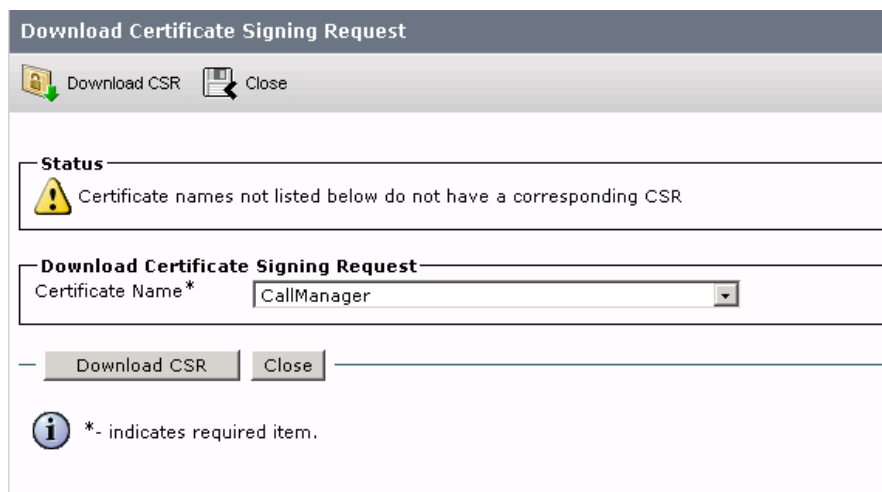
If the self-signed Call Manager certificate is not to be used but an external CA signs the Call Manager certificate, the following steps are necessary:

- The Call Manager places a certificate signing request (CSR).
- OS Administration → Security → Certificate List → button „Generate CSR“



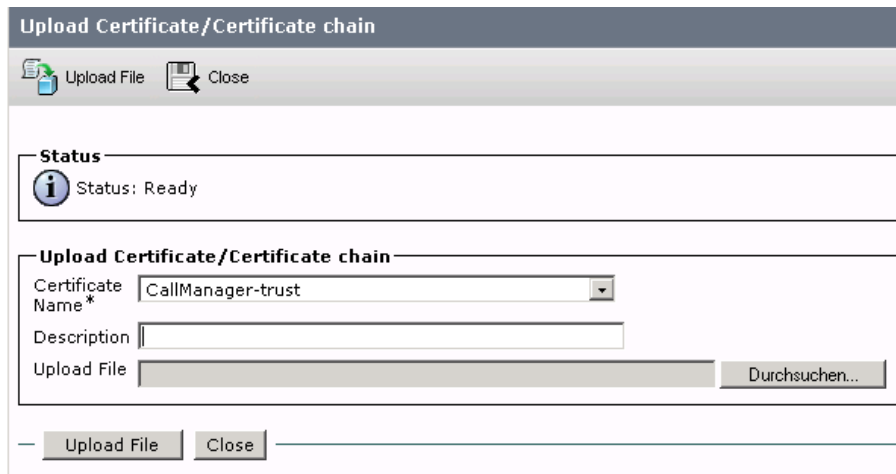
Picture 67 - Generate CSR

- The CSR is exported and sent to a CA for signing.
- OS Administration → Security → Certificate List → button „Download CSR“



Picture 68 - Download CSR

- The CA certificate of the external CA is loaded into the Call Manager.
- OS Administration → Security → Certificate List → button „Upload Certificate“
- As “Certificate Name” select “CallManager-trust”



Upload Certificate/Certificate chain

Upload File Close

Status
Status: Ready

Upload Certificate/Certificate chain

Certificate Name* CallManager-trust

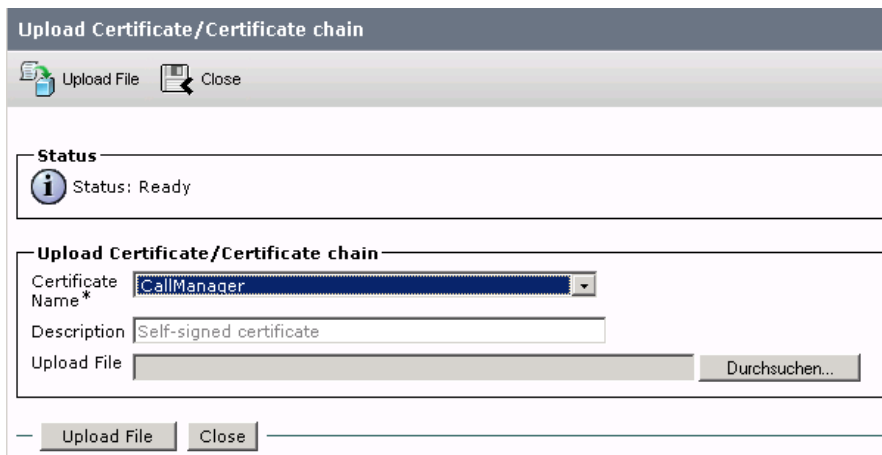
Description

Upload File

Upload File Close

Picture 69 – Loading the CA certificate into the trust list

- The signed certificate is loaded into the Call Manager.
- OS Administration → Security → Certificate List → button „Upload Certificate“
- As “Certificate Name” select “CallManager”



Upload Certificate/Certificate chain

Upload File Close

Status
Status: Ready

Upload Certificate/Certificate chain

Certificate Name* CallManager

Description Self-signed certificate

Upload File

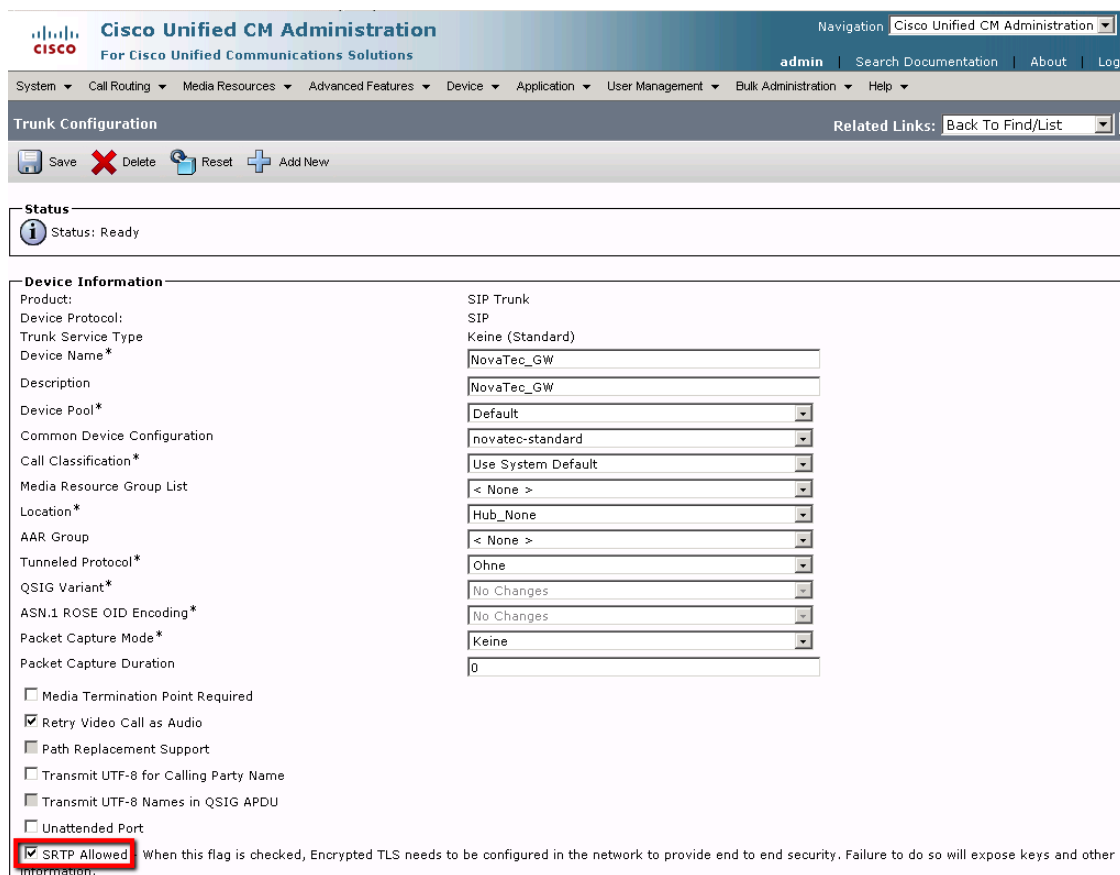
Upload File Close

Picture 70 – Loading New Call Manager certificate

6.5 Deactivating in the configuration

6.5.1 Deactivating TLS and sRTP for a CUCM trunk

- Delete the tick in the box „SRTP Allowed...” in the trunk configuration window. Set “Destination Port” to 5060 and select the favoured trunk „non-security” profile.

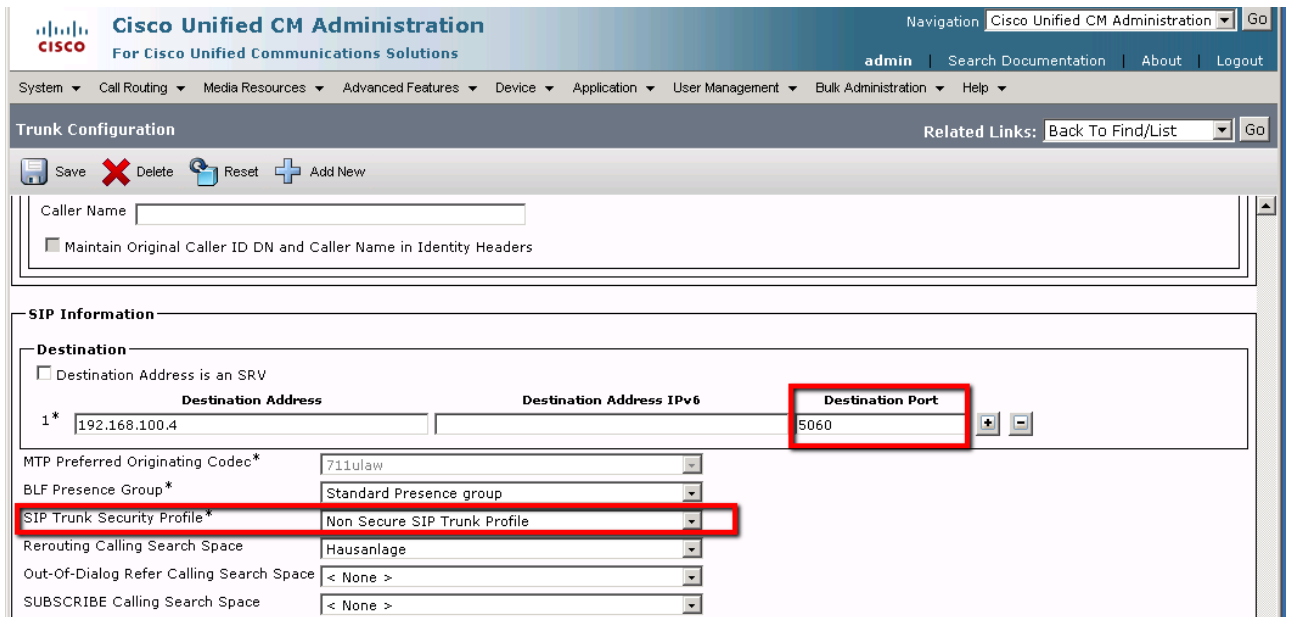


The screenshot shows the Cisco Unified CM Administration interface for configuring a SIP Trunk. The 'Device Information' section is expanded, showing various configuration options. The 'SRTP Allowed' checkbox is checked and highlighted with a red box. The text next to it reads: "When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information."

Field	Value
Product	SIP Trunk
Device Protocol	SIP
Trunk Service Type	Keine (Standard)
Device Name*	NovaTec_GW
Description	NovaTec_GW
Device Pool*	Default
Common Device Configuration	novatec-standard
Call Classification*	Use System Default
Media Resource Group List	< None >
Location*	Hub_None
AAR Group	< None >
Tunneled Protocol*	Ohne
QSIG Variant*	No Changes
ASN.1 ROSE OID Encoding*	No Changes
Packet Capture Mode*	Keine
Packet Capture Duration	0

Media Termination Point Required
 Retry Video Call as Audio
 Path Replacement Support
 Transmit UTF-8 for Calling Party Name
 Transmit UTF-8 Names in QSIG APDU
 Unattended Port
 SRTP Allowed When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.

Picture 71 - Trunk configuration – sRTP



Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation | Cisco Unified CM Administration | Go

admin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Trunk Configuration | Related Links: Back To Find/List | Go

Save | Delete | Reset | Add New

Caller Name:

Maintain Original Caller ID DN and Caller Name in Identity Headers

SIP Information

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	192.168.100.4		5060

MTP Preferred Originating Codec*: 711ulaw

BLF Presence Group*: Standard Presence group

SIP Trunk Security Profile*: Non Secure SIP Trunk Profile

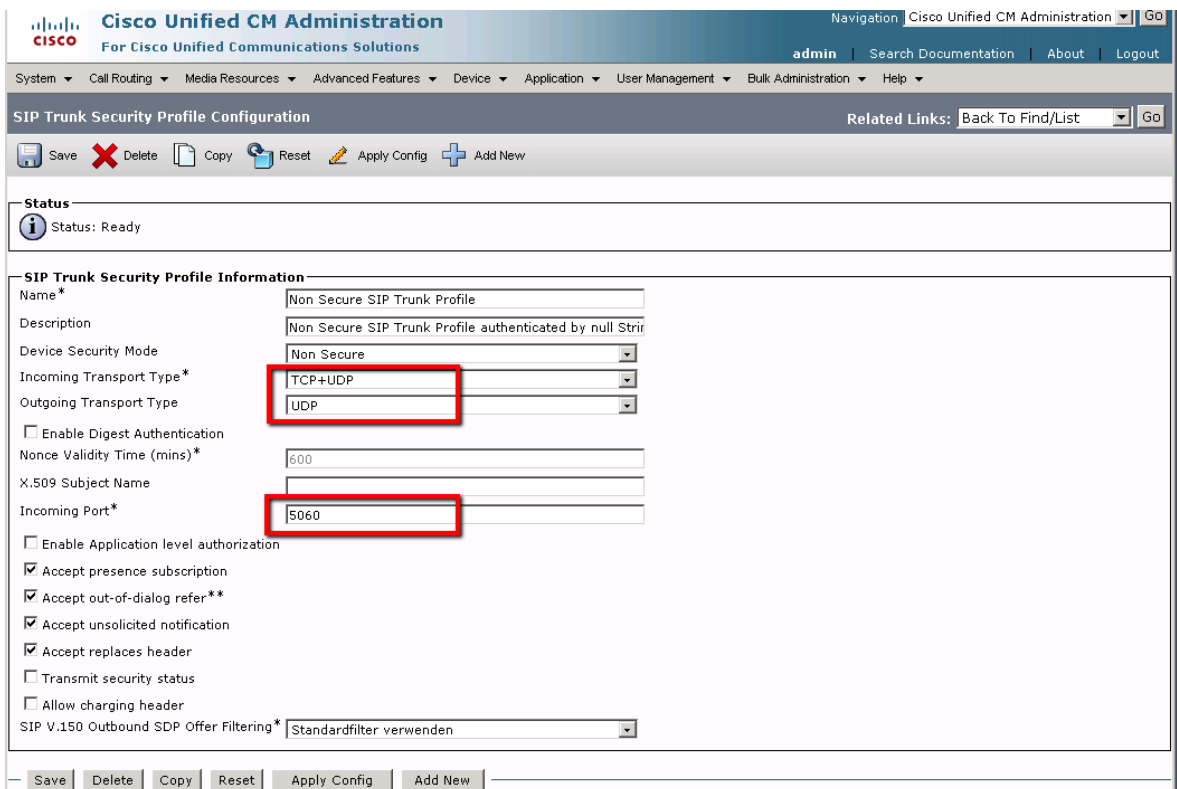
Rerouting Calling Search Space: Hausanlage

Out-Of-Dialog Refer Calling Search Space: < None >

SUBSCRIBE Calling Search Space: < None >

Picture 72 - Trunk configuration security profile

- The settings of the trunk "non-security" profile should look like those in the example below. "Incoming Port:" 5060.



Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation | Cisco Unified CM Administration | Go

admin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

SIP Trunk Security Profile Configuration | Related Links: Back To Find/List | Go

Save | Delete | Copy | Reset | Apply Config | Add New

Status

Status: Ready

SIP Trunk Security Profile Information

Name*: Non Secure SIP Trunk Profile

Description: Non Secure SIP Trunk Profile authenticated by null Stri

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

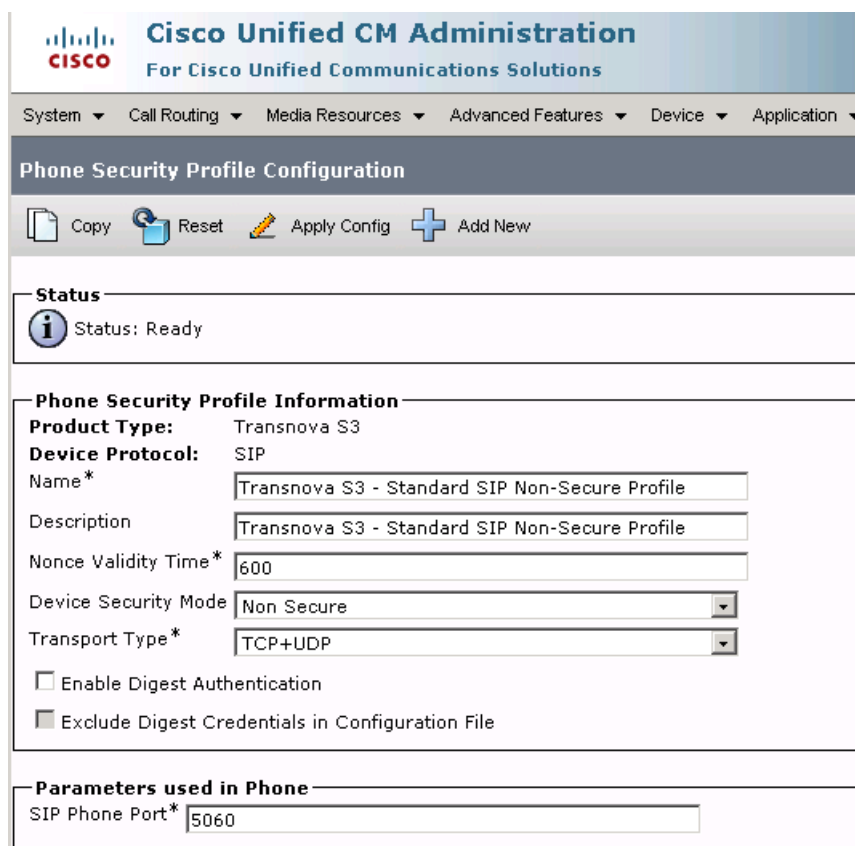
Allow charging header

SIP V.150 Outbound SDP Offer Filtering*: Standardfilter verwenden

Save | Delete | Copy | Reset | Apply Config | Add New

6.5.2 Deactivating TLS and sRTP for a CUCM line

- Change the profile from a "crypto security" profile to a „non-security phone" profile.
- The settings of the line device in "non-security" profile should be as follows: "Incoming Port:" 5060.



The screenshot displays the Cisco Unified CM Administration interface for configuring a Phone Security Profile. The page title is "Cisco Unified CM Administration For Cisco Unified Communications Solutions". The navigation menu includes System, Call Routing, Media Resources, Advanced Features, Device, and Application. The main heading is "Phone Security Profile Configuration". Below this, there are icons for Copy, Reset, Apply Config, and Add New. The "Status" section shows "Status: Ready". The "Phone Security Profile Information" section includes the following fields: Product Type (Transnova S3), Device Protocol (SIP), Name* (Transnova S3 - Standard SIP Non-Secure Profile), Description (Transnova S3 - Standard SIP Non-Secure Profile), Nonce Validity Time* (600), Device Security Mode (Non Secure), and Transport Type* (TCP+UDP). There are also checkboxes for "Enable Digest Authentication" (unchecked) and "Exclude Digest Credentials in Configuration File" (checked). The "Parameters used in Phone" section shows "SIP Phone Port*" set to 5060.

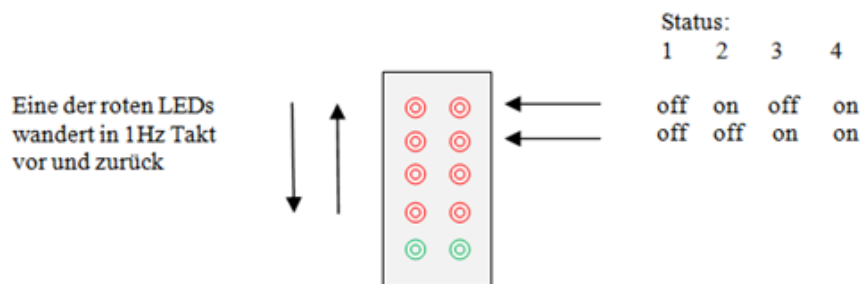
Picture 73 - CUCM Line disable security

7 Appendix

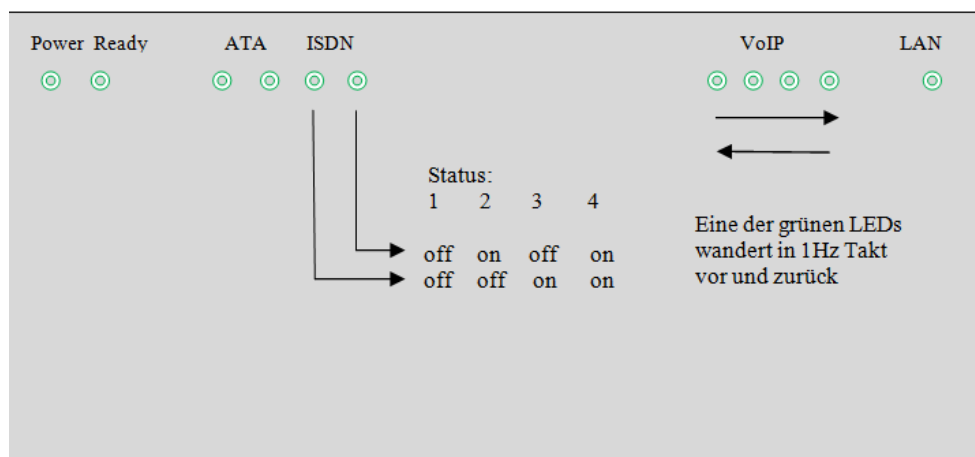
7.1 State of LED signals during the signing process

The LEDs on the control panel can signal the following states:

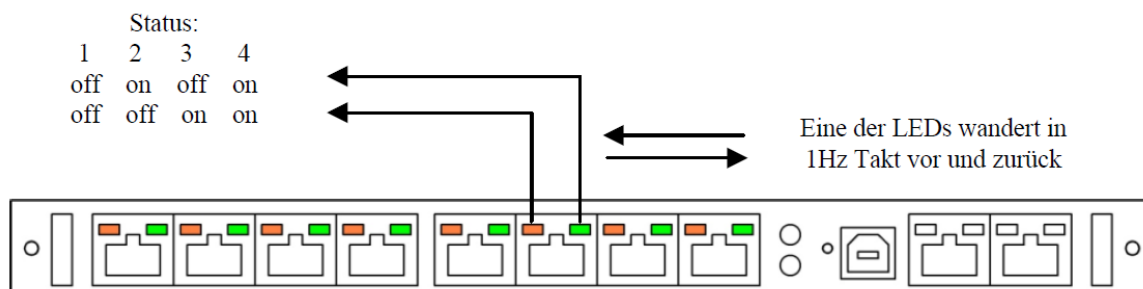
1. No meaning.
2. The system is generating a 1024/2048 key and will reboot subsequently.
3. SCEP mode: system is looking for the IP address of the CA server via DNS.
4. SCEP mode: CA server has been found. Enrolment is executed and system will reboot subsequently.



Picture 74 - LED area of the CCU3



Picture 75 - LED area of the S3



Picture 76 - LED area of the CCU4

7.2 Changeover between 1024/2048 bit RSA key

In the Trace Info Client under „System-Security“ the length of the current private RSA key is shown.

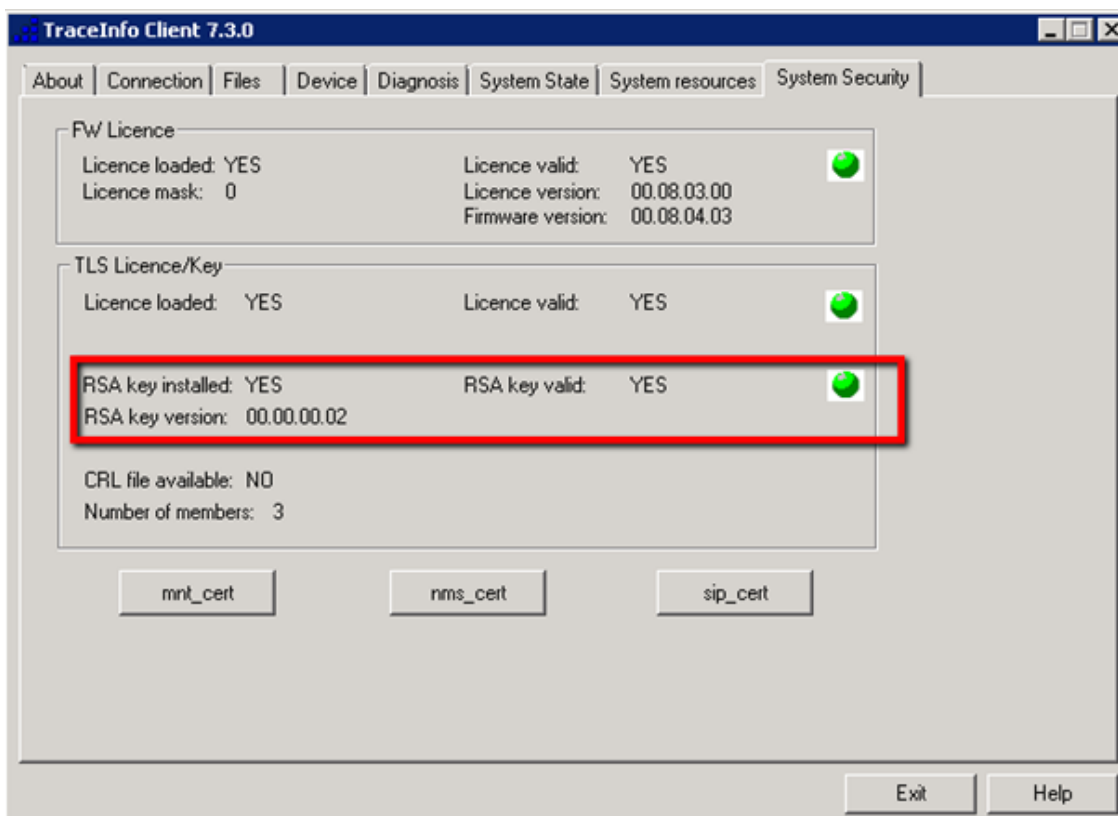
RSA key version: 00.00.00.01 → 1024 bit key

00.00.00.02 → 2048 bit key

A new key is only generated if the key length is changed. A new key with the same length as the key already existing in the system cannot be generated.

If a 1024 bit key was stored before the exchange of the key, with the next reboot a 2048 bit key will be generated and vice versa. This private RSA key is secured and stored within the gateway and cannot be read out.

The LEDs on the front plate show the creation of a new key (see section 7.1). The process may take a few minutes (CCU3/S3: 4min/1024bit, 10min/2048bit – CCU4: 0,5min/1024bit, 1min/2048bit). The end of the key creation is marked by a system reset.

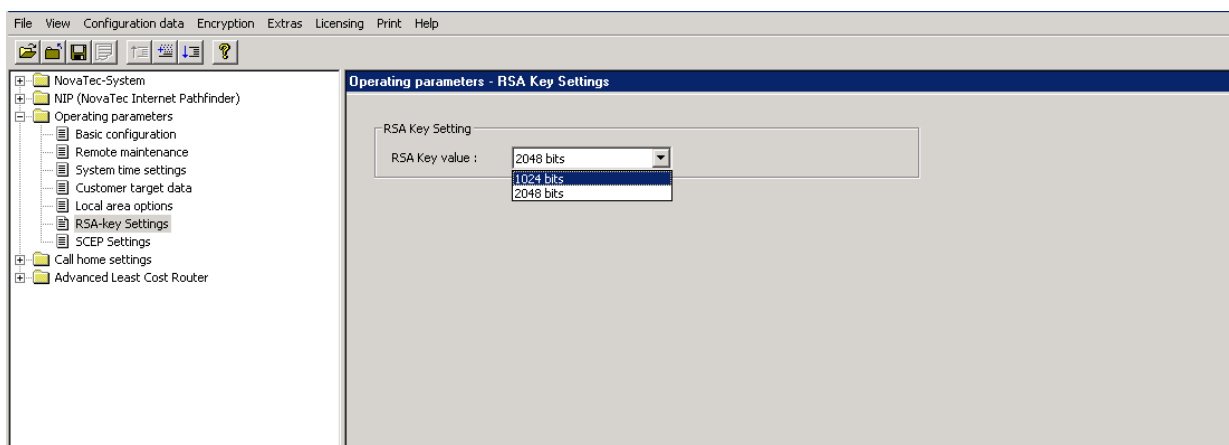


Picture 77 – Display of the current key length

In order to change the key length in the system the following steps are run:

1. The required modification license, a special firmware license, is available from NovaTec. It is loaded into the system like a normal firmware license.
2. Apart of this the new key length is specified in the configuration under „Operating parameters“ → „RSA-key Settings“.

3. Load the configuration into the system.
4. The system generates a new key with changed length.
5. Please load the original NovaTec firmware license into the system anew now and activate it by rebooting the gateway.



Picture 78 – Configuration of key length



7.3 SCEP application

7.3.1 NovaTec SCEP implementation

The protocol was designed in accordance with the so to speak norm of the internet engineering task force "Cisco Systems Simple Certificate Enrollment Protocol draft-nourse-scep-20":

The so to speak norm describes 4 functions

1. Get CA/RA certificate (Demand of public certificate chain and enrol certificate)
2. Enroll certificate (signing of the certificate request)
3. Query certificate (Demand of a signed certificate)
4. Query CRL (Loading of the "Certificate Revocation List".)

Function 1:

The function „Get CA/RA certificate“ doesn't fit into today's configuration concept as the public certificates or certificate chains are provided with the configuration of the NovaTec systems. The unsecured access to the certificate server is security relevant issue. As a rule it is demanded, that the fingerprint of the certificate is manually surveyed by the operator for plausibility.

Function 2:

„Enroll certificate“ describes the actual „Signing of the certificate request“. For this the client (NovaTec system) has to enter its IP address into the „X.509v3 extensions“ in the request:

Example:

```
[x509v3_IPAddr]
```

```
subjectAltName=critical,IP: "192.168.1.1"
```

If the server is capable of automatic enrolment, the certificate request has to be secured with a password additionally:

Example:

```
[ req_attributes ]
```

```
challengePassword          = "A challenge password"
```

```
challengePassword_min = 4
```

```
challengePassword_max    = 20
```



Function 3:

„Query certificate“ allows requesting a signed certificate. Is not used at the moment as optional and dependant on the used PKI.

Function 4:

„Query CRL“ loads and surveys the CRL list (“certificate revocation list”). Is not used at the moment as optional and dependant on the used PKI.



7.3.2 SCEP trace output

The module „SCEPD“ of the firmware conducts trace output in plaintext.

Example:

```
TI: 2011-03-01 11:38:51 0000050.483 EVENT SCEPD Starting SSCEP Version: 20081211
TI: 2011-03-01 11:38:51 0000050.575 EVENT SCEPD New transaction
TI: 2011-03-01 11:38:51 0000050.577 EVENT SCEPD SCEPD: transaction id:
08F1B9E9ACC468335ECECAE4D8BF9A90
TI: 2011-03-01 11:38:51 0000050.577 EVENT SCEPD Generating selfsigned certificate
TI: 2011-03-01 11:38:57 0000057.069 EVENT SCEPD SCEP_OPERATION_ENROLL
TI: 2011-03-01 11:38:57 0000057.070 EVENT SCEPD Sending certificate request
TI: 2011-03-01 11:39:05 0000064.492 EVENT SCEPD Server returned status code 200
TI: 2011-03-01 11:39:05 0000064.493 EVENT SCEPD Valid response from server
TI: 2011-03-01 11:39:05 0000064.548 EVENT SCEPD pkistatus: SUCCESS
TI: 2011-03-01 11:39:11 0000070.569 EVENT SCEPD Write_local_cert
TI: 2011-03-01 11:39:11 0000070.569 EVENT SCEPD Found certificate with
TI: 2011-03-01 11:39:11 0000070.569 EVENT SCEPD subject:
'/C=DE/ST=NRW/L=Paderborn/O=NovaTec/OU=Support/CN=novatec/emailAddress=support@novatec.de'
TI: 2011-03-01 11:39:11 0000070.569 EVENT SCEPD issuer: /DC=NET/DC=DE/CN=caserver1
TI: 2011-03-01 11:39:11 0000070.570 EVENT SCEPD request_subject:
'/C=DE/ST=NRW/L=Paderborn/O=NovaTec/OU=Support/CN=novatec/emailAddress=support@novatec.de'
TI: 2011-03-01 11:39:11 0000070.570 EVENT SCEPD CN's of request and certificate matched!
TI: 2011-03-01 11:39:11 0000070.585 EVENT SCEPD Certificate written
```



7.4 List of abbreviations

Abbreviation	Meaning
CA	Certificate Authority
CCU3	Central Control Unit Model 3
CCU4	Central Control Unit Model 4
CRT	Certificate
CSR	Certificate Signing Request
CTL	Certificate Trust List / CUCM
CUCM	Cisco Unified Communications Manager
DHCP	Dynamic Host Configuration Protocol
FW	Firmware
IP	Internet Protocol
MNT	Maintenance Task in den NovaTec
NAMES	NovaTec Administration & Management Element Server
NMS	NovaTec Management Server
PKI	Public Key Infrastructure
Root-CA	Root Certification Authority
Root-CRT	Root-Certificate / CA-Certificate
RSA	Rivest, Shamir & Adleman
RTP	Real-Time Transport Protocol
S3	SIP Gateway Model 3
SCEP	Simple Certificate Enrollment Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
sRTP	Secure Real-Time Transport Protocol
TI	Trace-Info
TI-CA	Trace-Info Certificate Authority
TLS	Transport Layer Security
Trust List	List of trustworthy CAs
VoIP	Voice over IP



7.5 List of illustrations

Picture 1 - Server- / Client-Authentication	7
Picture 2- Explanation of abridgment diagrams	8
Picture 3 – Creation of a TLS certificate of a gateway	9
Picture 4 – TLS connection establishment and one CA	10
Picture 5 - TLS connection establishment with two CAs.....	11
Picture 6 – loading the firmware license.....	12
Picture 7 - TLS license is loaded	13
Picture 8 - TLS Security is licensed	14
Picture 9 – Configuring TI-CA authorizations	15
Picture 10 – Creating a CSR	16
Picture 11 – Signing the CSR your self	17
Picture 12 – Signing CSR externally	18
Picture 13 - Creating a certificate with or without plain text	19
Picture 14 - sRTP encryption profile.....	23
Picture 15 – Assigning sRTP to SIP	24
Picture 16 - SIP – enable security	25
Picture 17 - SIP-CSR Common Name	26
Picture 18 - Trust List – Loading a CA certificate.....	27
Picture 19 - Trust List – Showing certificates	28
Picture 20 - SIP-TLS User Mapping	29
Picture 21 - SIP-TLS Local Mapping	30
Picture 22 - SIP-TLS Optional Flags 2	31
Picture 23 - SCEP Server URL.....	32
Picture 24 - Export of the two enrolment certificates	33
Picture 25 – Export data format	33
Picture 26 - SCEP CA export.....	34
Picture 27 - SCEP CA import.....	34



Picture 28 – Copying the challenge password	35
Picture 29 – Inserting the challenge password	36
Picture 30 - NAMES architecture	37
Picture 31 – Creating MNT & NMS CSR	41
Picture 32 - TI-CA signs MNT- & NMS-CSR	42
Picture 33 – Configuring CSR for MNT	43
Picture 34 – Configuring CSR for NMS	44
Picture 35 - MNT- / NMS-CSR form	44
Picture 36 - Input: TI-CA signs MNT- / NMS-CSR on the gateway	46
Picture 37 - Output: TI-CA signs MNT- / NMS-CSR on the gateway	47
Picture 38 – Activating TLS for MNT	48
Picture 39 – Loading TLS certificate for MNT	49
Picture 40 – Deactivating TLS in the configuration	50
Picture 41 – Checking the unsecured IP service	51
Picture 42 – Setting up UDP service for SIP	52
Picture 43 - Access Options	52
Picture 44 - SIP Session Owner	53
Picture 45 – Deactivating user mapping sRTP	54
Picture 46 - Local mapping	54
Picture 47 - TI-CA was started without dongle	55
Picture 48 – Addressing the target system	56
Picture 49 - TI-CA “Sign Certificate Requests” PC-to-PC	57
Picture 50 - TI-CA “Sign Certificate Requests” PC-to-Target	59
Picture 51 - TI-CA Sign Certificate Requests PC-to-Target	61
Picture 52 - SCEP Enrolment NovaTec Gateways	63
Picture 53 - SCEP Enrollment CallServer & NovaTec Management PC	64
Picture 54 - CTL Provider Activated	67
Picture 55 - CTL Service Parameter	67



Picture 56 – CTL Client connect.....	68
Picture 57 - CTL Mixed Mode.....	68
Picture 58 - CTL Entries	69
Picture 59 - CUCM Service activation	70
Picture 60 - CUCM Trunk Security Profile	71
Picture 61 - CUCM Trunk sRTP Allowed.....	72
Picture 62 - CUCM Trunk Port 5061	72
Picture 63 - Modify Transnova S3 - Non-Security Profile.....	73
Picture 64 - Transnova S3 - Security Profile.....	74
Picture 65 - Download CallManager certificate	76
Picture 66 - Upload CA certificate into CUCM trust list.....	77
Picture 67 - Generate CSR	78
Picture 68 - Download CSR	78
Picture 69 – Loading the CA certificate into the trust list	79
Picture 70 – Loading New Call Manager certificate.....	79
Picture 71 - Trunk configuration – sRTP.....	80
Picture 72 - Trunk configuration security profile	81
Picture 73 - CUCM Line disable security	82
Picture 74 - LED area of the CCU3.....	83
Picture 75 - LED area of the S3	83
Picture 76 - LED area of the CCU4.....	84
Picture 77 – Display of the current key length	85
Picture 78 – Configuration of key length	86