We change the shape of the world

White Paper

NovaTec

Access Media Gateway

Version 1.0 vom 26. Oktober 2010

Änderungen vorbehalten

INHALT

1 Einleitung

Das vorliegende White Paper beschreibt die Eigenschaften, Konfiguration, Betrieb und Anbindung der NovaTec A-MGWs in einer VoIP-Infrastruktur oder im Zusammenspiel mit z. B. dem Cisco Unified Communications Manager über einen SIP-Trunk.

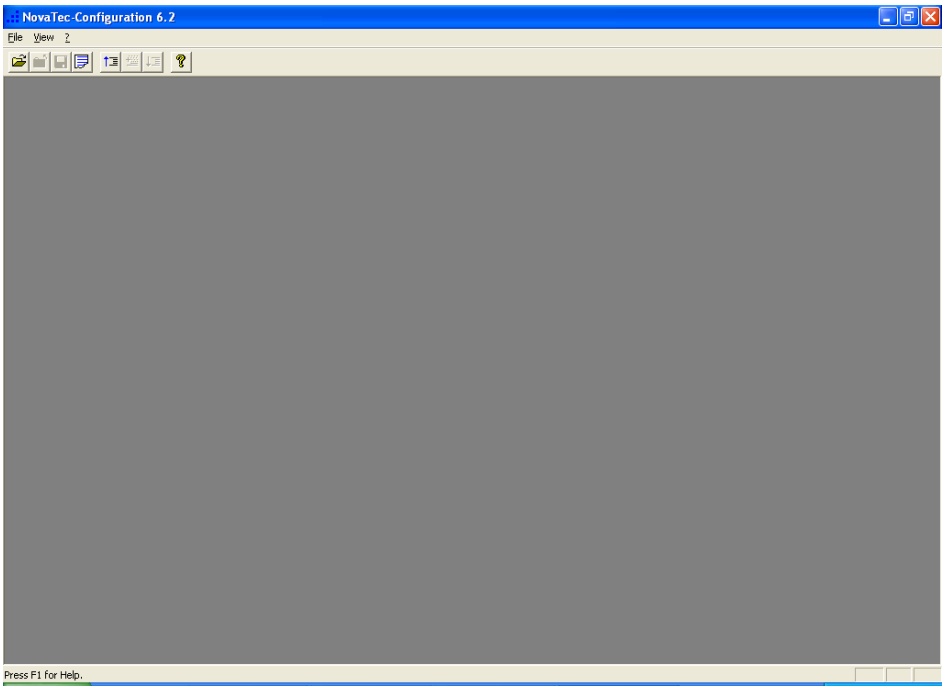
Die NovaTec A-MGWs stellen dabei alle herkömmlichen TDM basierten Schnittstellen (S_0, S_{2M}, U_{k0}, Analog, GSM) zur Verfügung. Die NovaTec Sx Modelle können z. B. als Third Party Device an Cisco Unified Communications Manager angebunden werden

Diese Dokument behandelt unter anderem die allgemeine Vorgehensweise für die TLS-Verschlüsselung, eine detaillierte Beschreibung wie TLS eingerichtet wird, wie DHCP einzurichten ist, wie die Sx Schritt für Schritt zu konfigurieren ist, wenn sie über einen SIP-Trunk angebunden wird, wie das NovaTec Management System installiert wird und wie es mit der Sx zusammenarbeitet.

2 Konfigurationsanweisung

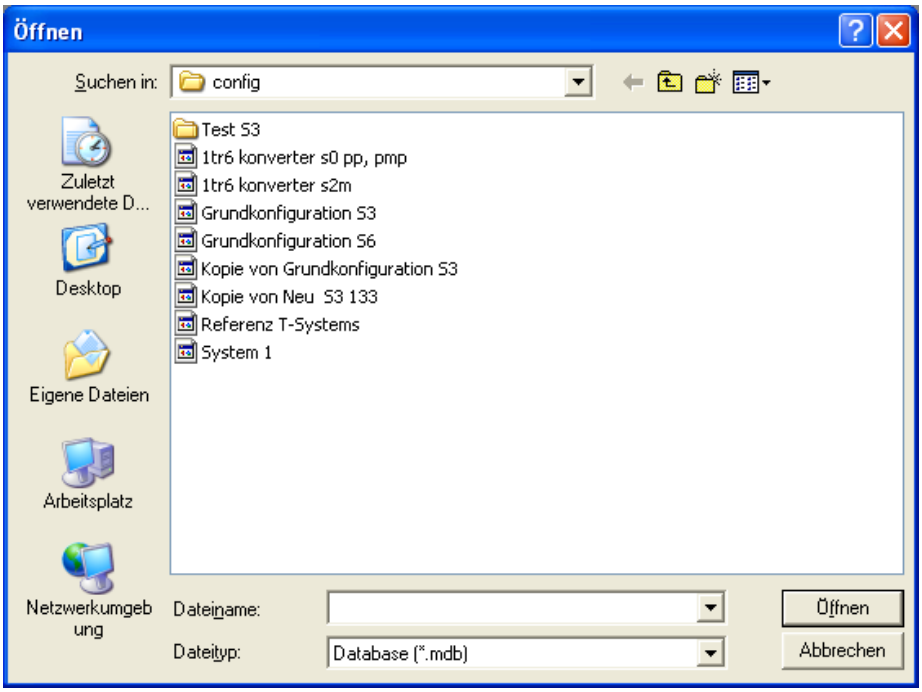
2.1 Konfigurationsoberfläche starten:

Starten Sie die Konfigurationsoberfläche über das Windows-Startmenü:
Startmenü → Programme → NovaTec → NMP 6.2 → NovaTec Configuration



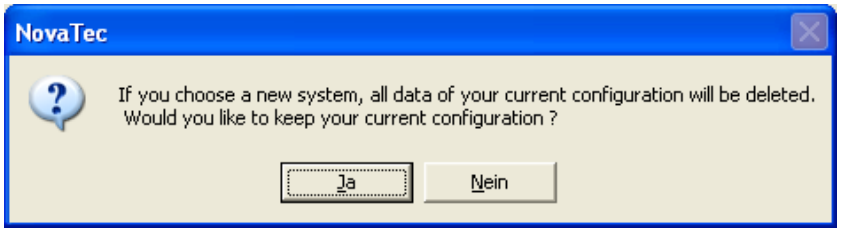
2.2 Die Datenbank öffnen

Wählen Sie in der Menüleiste den Punkt *„File/Open“* aus. Wählen Sie im Öffnen-Dialogfenster die zu öffnende Datei aus.



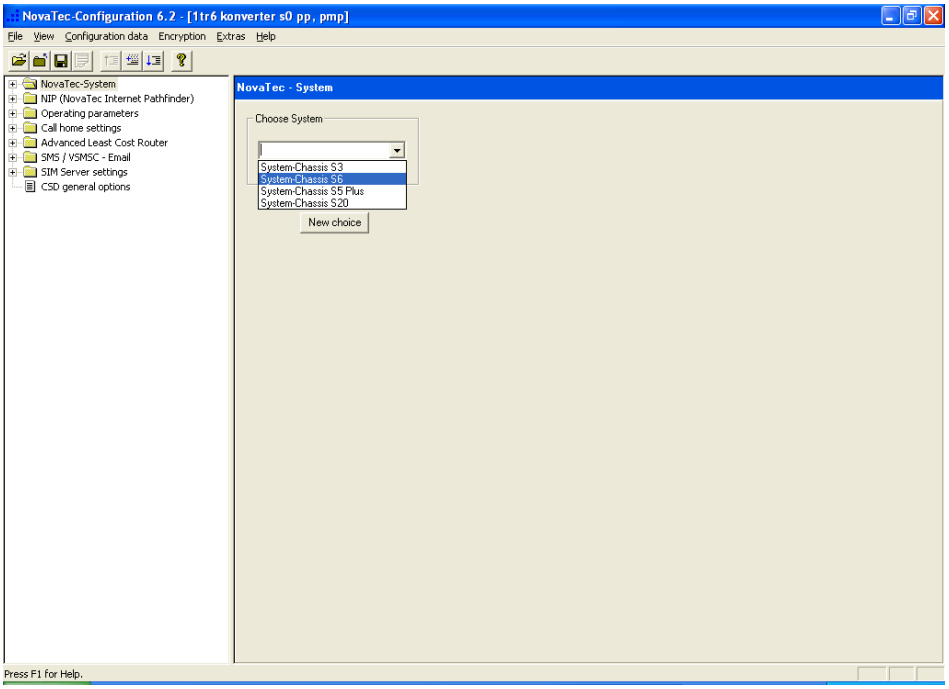
2.3 Chassis konfigurieren (S20, S6, S5+ oder S3)

Klicken Sie im linken Baum auf *„NovaTec-System“* und danach im rechten Fenster auf die Schaltfläche *„New choice“.*



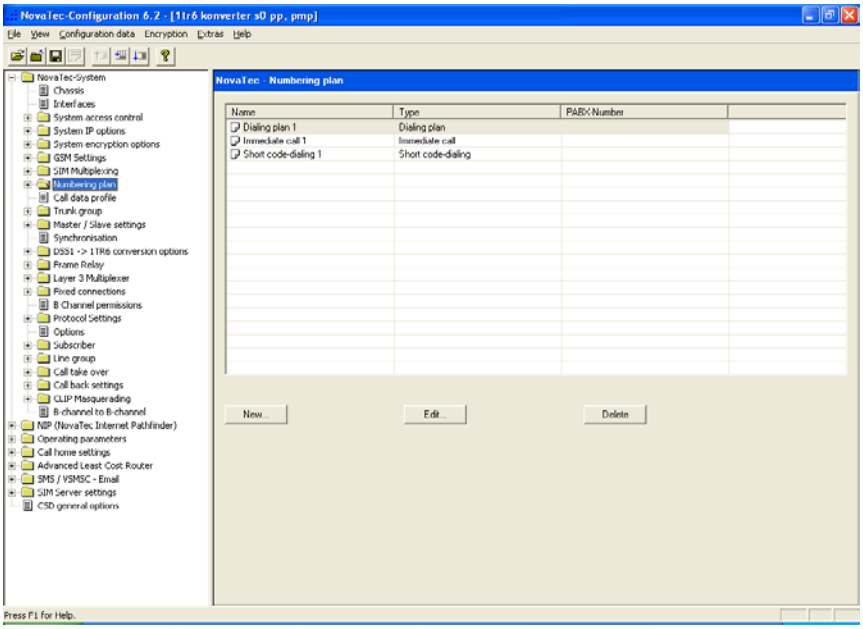
Bestätigen Sie den erscheinenden Dialog mit „*Nein*“. Dadurch werden schon vorhandene Einstellungen in der Datenbank verworfen. Sie erstellen damit eine neue Konfiguration.

Wählen Sie als Chassis z.B. „*System-Chassis S6*“ aus um eine NovaTec S6 zu konfigurieren.

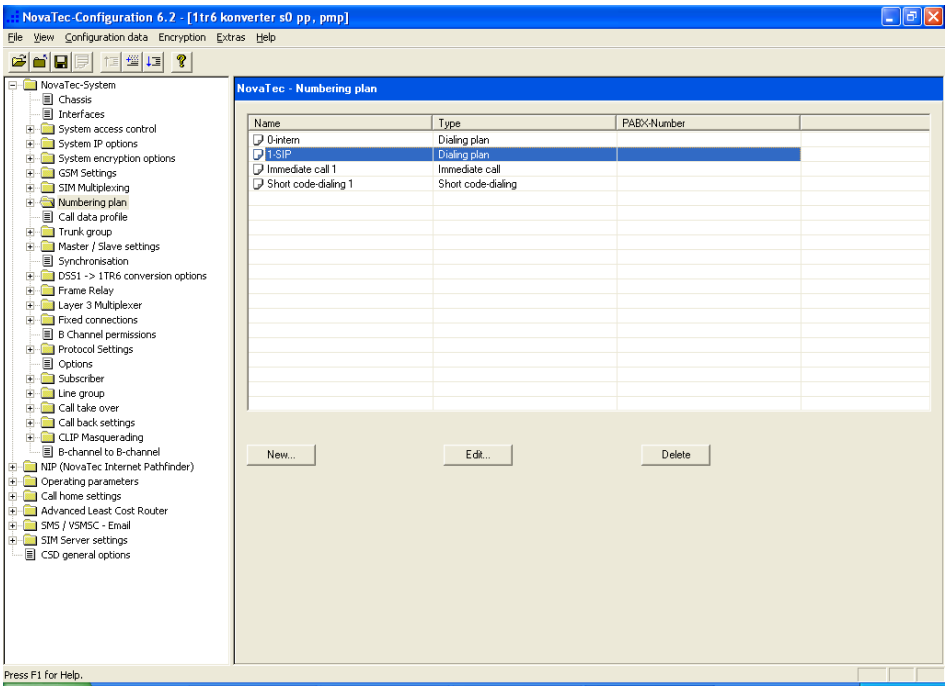


2.4 Numbering plan definieren

Gehen Sie im linken Baum auf „*NovaTec-System/Numbering plan*“ und klicken Sie im rechten Fenster auf die Schaltfläche „*New*“.

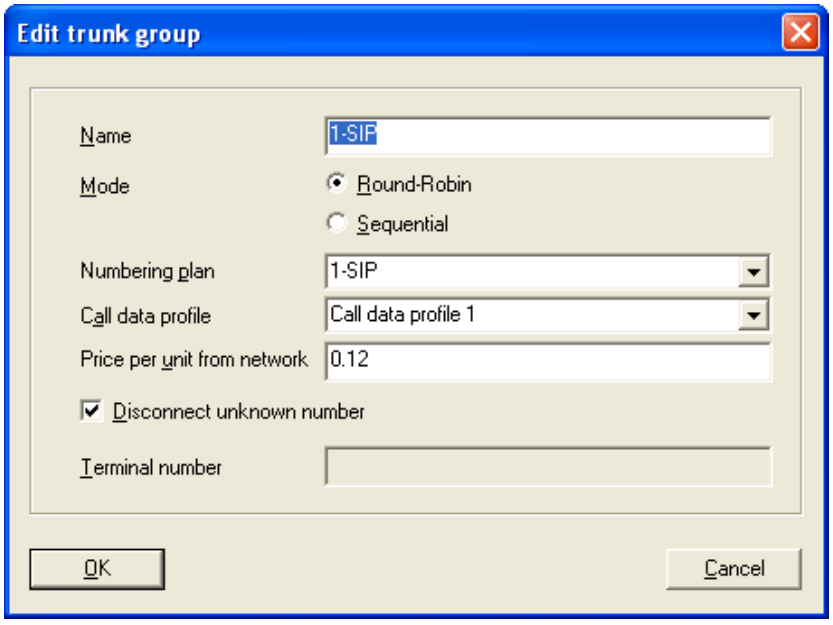


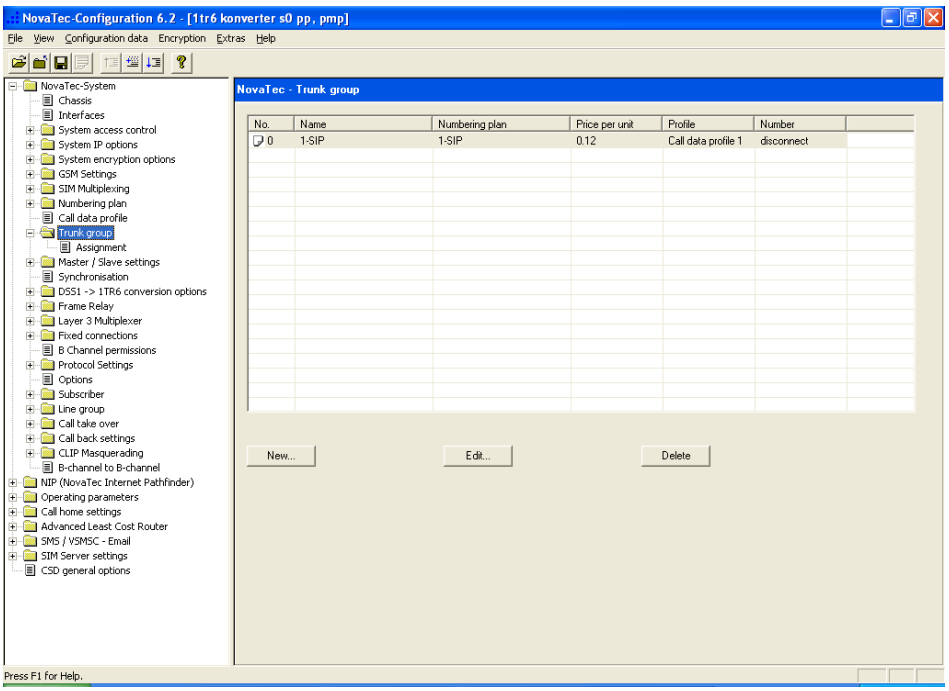
Im Fenster „New numbering plan“ geben Sie als „Name“ ***„0-intern“*** ein und wählen als *„Type“* *„Dialing plan“.* Das Feld *„PABX-Number“* bleibt leer. Bestätigen Sie mit *„OK“*. Wiederholen Sie den Vorgang und legen einen weiteren Rufnummernplan mit dem Namen ***„1-SIP“*** an. Wählen Sie die gleichen Einstellungen wie zuvor.



2.5 SIP Trunk Group konfigurieren

Gehen Sie im linken Baum auf *„NovaTec-System/Trunk group“* und klicken Sie im rechten Fenster auf *„Edit“*. Legen Sie ein Trunk Group mit dem Namen ***„1-SIP“*** und den unten gezeigten Einstellungen/Werten an. Bestätigen Sie mit *„OK“*.

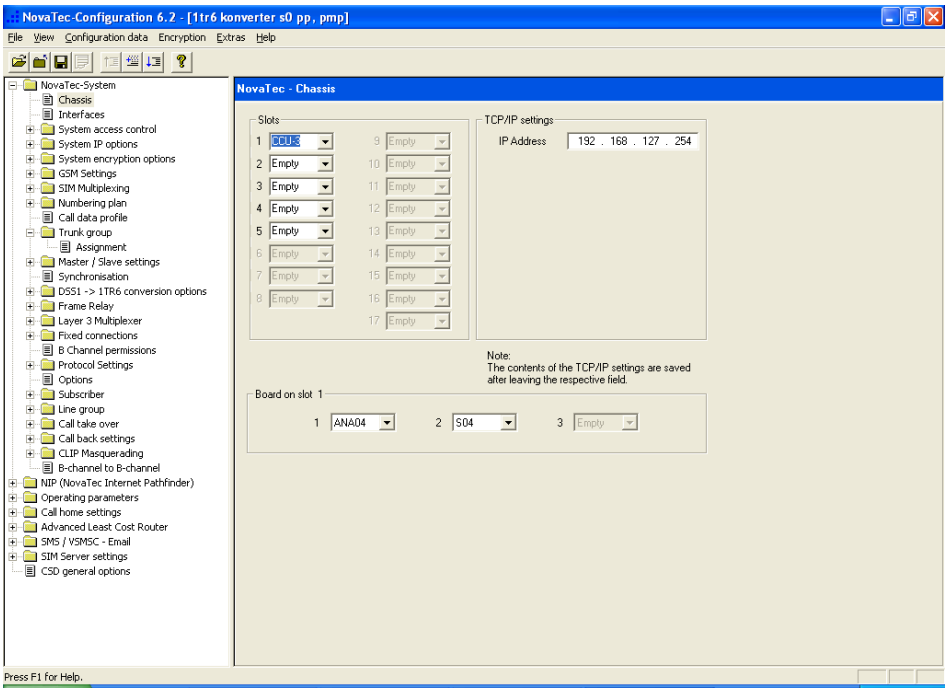



NovaTec-Configuration 6.2 - [1tr6 konverter s0 pp, pmp]
File View Configuration data Encryption Extras Help
NovaTec-System
Chassis
Interfaces
System access control
System IP options
System encryption options
GSM Settings
SIM Multiplexing
Numbering plan
Call data profile
Trunk group
Assignment
Master / Slave settings
Synchronisation
DSS1 -> 1TR6 conversion options
Frame Relay
Layer 3 Multiplexer
Fixed connections
B Channel permissions
Protocol Settings
Options
Subscriber
Line group
Call take over
Call back settings
CLIP Masquerading
B-channel to B-channel
NIP (NovaTec Internet Pathfinder)
Operating parameters
Call home settings
Advanced Least Cost Router
SMS / VSMSC - Email
SIM Server settings
CSD general options
NovaTec - Trunk group
No. Name Numbering plan Price per unit Profile Number
0 1-SIP 1-SIP 0.12 Call data profile 1 disconnect
New...
Edit...
Delete
Press F1 for Help.

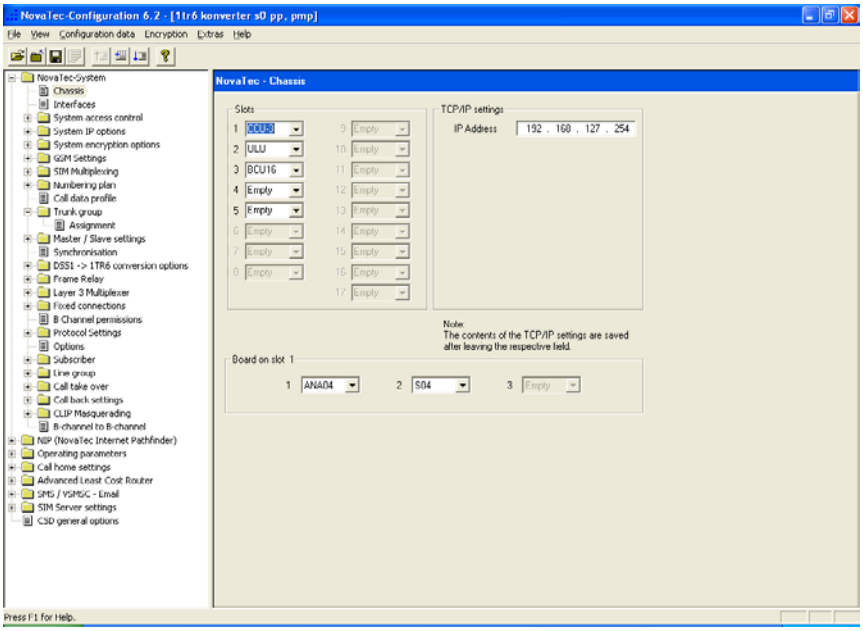
2.6 Module konfigurieren (z.B. Aufbau des S6)

In diesem Beispiel enthält die S6 folgende Hardwarekomponenten:
CCU mit einer analogen Aufsteckkarte ANA4 und einer ISDN-S_0-Karte S04,
ULU mit 4 Uk_0 Schnittstellen,
BCU 16 mit 16 VoIP-Kanälen

Gehen Sie im linken Baum unter *„NovaTec System/Chassis“*. Wählen Sie im rechten Fenster unter *„Slots“* für Slot 1 *„CCU-3“* aus. Im unteren Fensterbereich wählen Sie unter *„Board on slot 1“* für Aufsteckplatz 1 *„ANA04“* aus und für Aufsteckplatz 2 *„S04“.*



Wählen Sie für Slot 2 *„ULU“* aus und für Slot 3 *„BCU16“*. Da die beiden Boards keine Aufsteckplätze besitzen brauchen keine weiteren Einstellungen für Slot 2 und 3 vorgenommen werden.

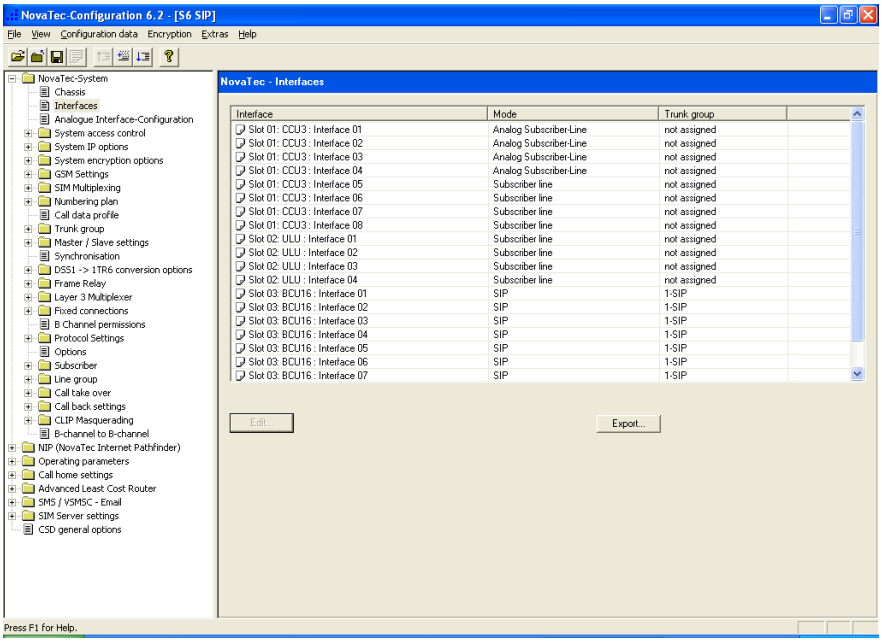


2.7 Interfaces definieren

Gehen Sie im linken Baum unter *„Novatec-System/Interfaces“.*
Selektieren Sie die jeweilige Schnittstelle und klicken dann auf „Edit“ Nehmen Sie für die verschiedenen Schnittstellentypen folgende Einstellungen vor:
Für S_0 und Uk_0-Schnittstellen wählen Sie den Modus „*Subscriber line*“. Die Einstellung „Trunk group“ lassen Sie auf „not assigned“ stehen.

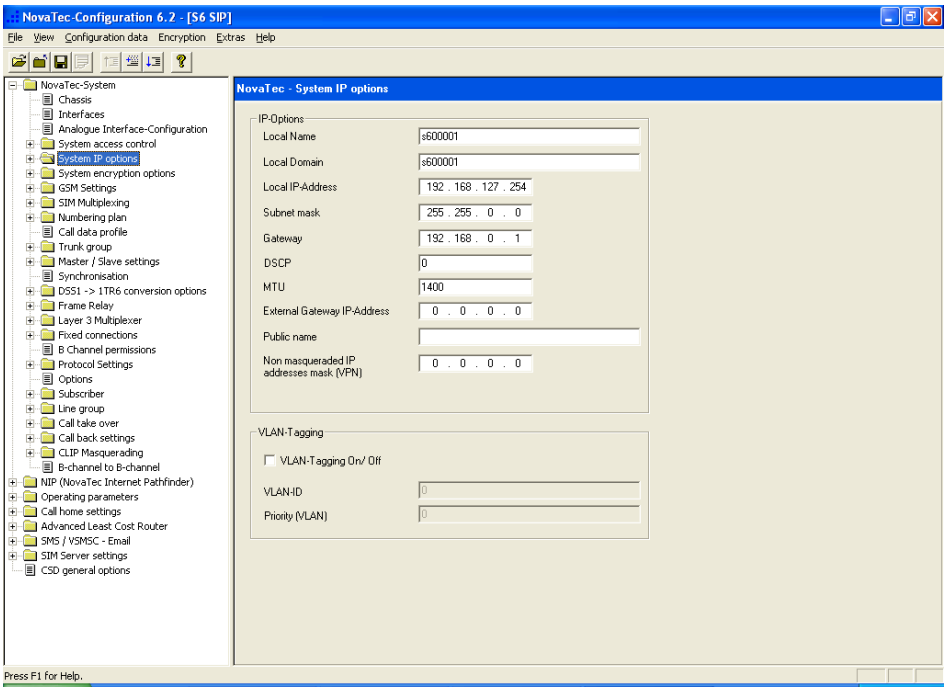
Für die analogen Schnittstellen (ANA4) wählen Sie den Modus „*Analog Subscriber line*“. Die Einstellung „Trunk group“ lassen Sie auf „not assigned“ stehen.

Für die VoIP-Schnittstellen (BCU16) wählen Sie den Modus „*SIP*“ und „*Trunk group*“ **„*1-SIP*“** aus.



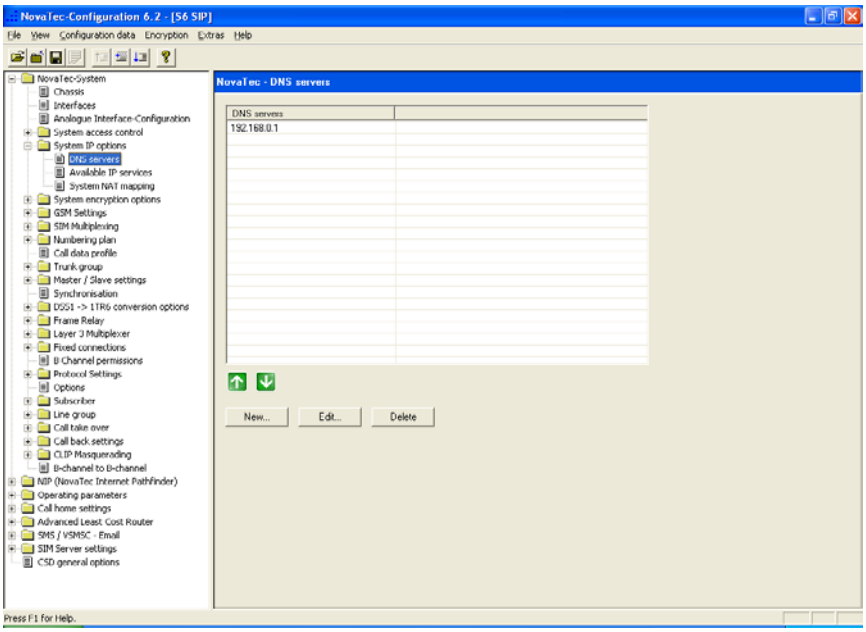
2.8 System IP options

Gehen Sie im linken Baum unter *„NovaTec-System/System IP options“*. Machen Sie die für Ihr Netzwerk und Ihre Installation passenden Eingaben.



Gehen Sie im linken Baum unter *„NovaTec-System/System IP options/DNS Server“*.

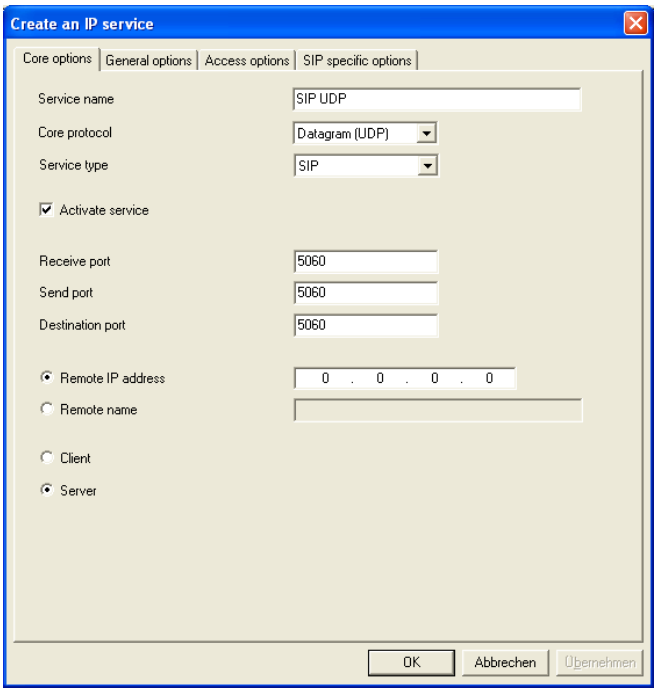
Klicken Sie auf *„New“* und tragen Sie die Adresse des DNS-Servers ein.

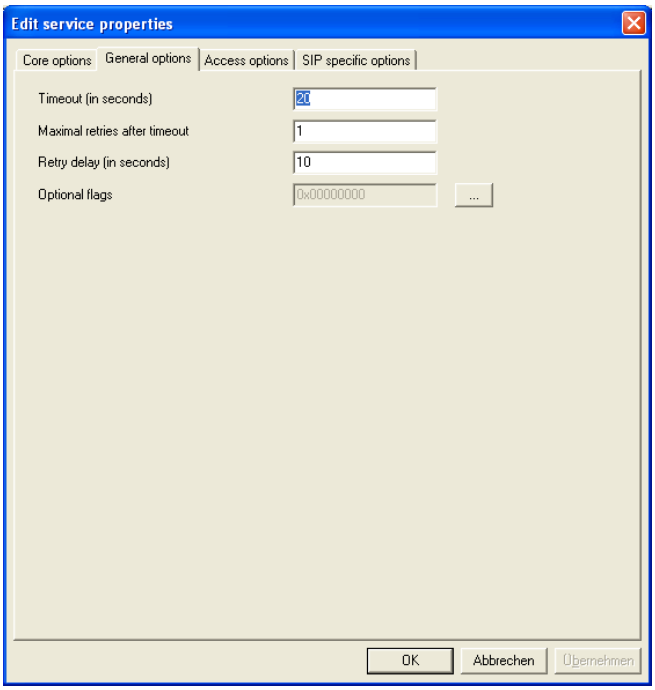


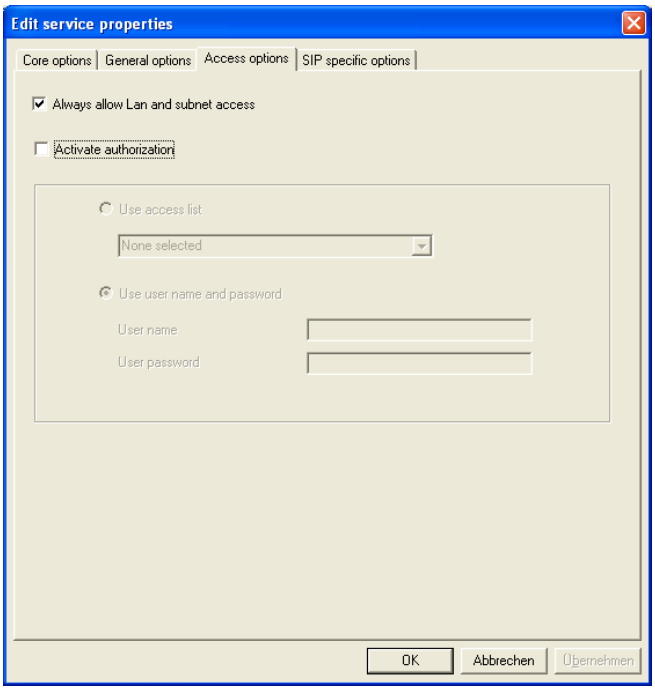
Gehen Sie im linken Baum unter *„NovaTec-System/System IP options/Availabe IP services“.*

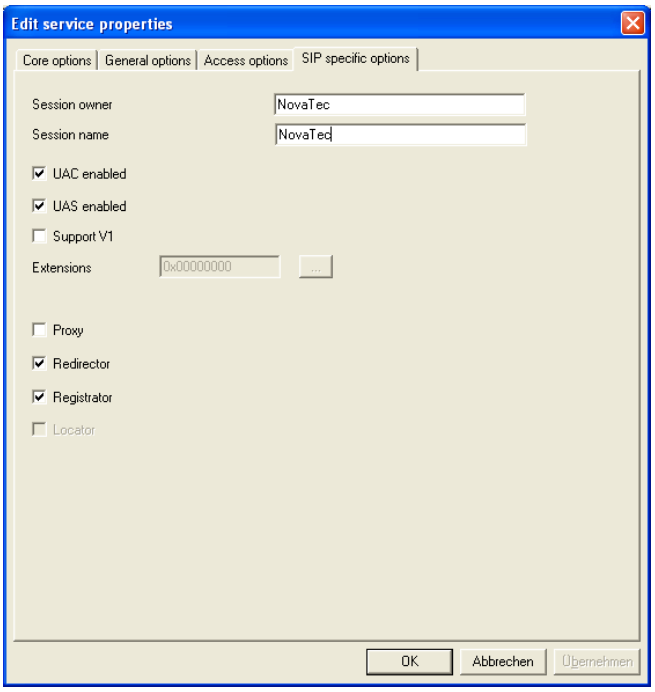
Klicken Sie auf *„New“* und führen Sie die in den nächsten vier Bildern dargestellten Einstellungen durch, um den Dienst SIP über UDP (über IP-Port 5060) zu aktivieren.

Bestätigen Sie mit *„OK“*.



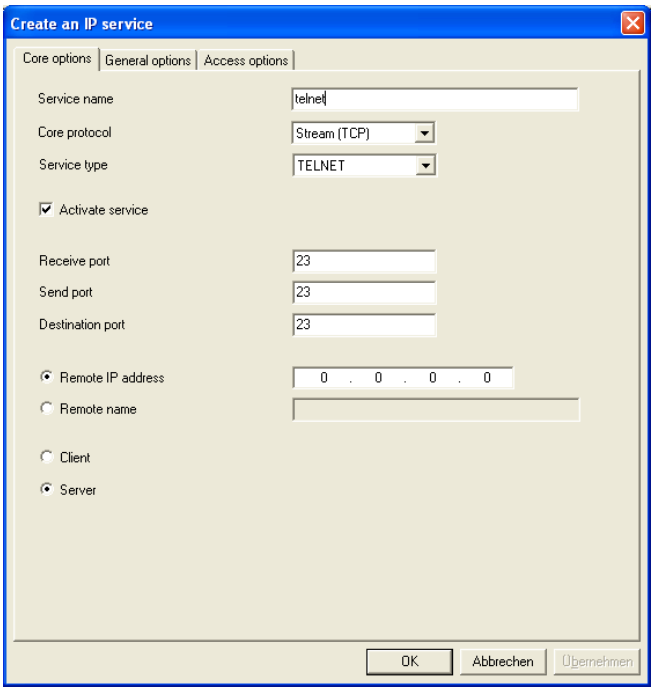


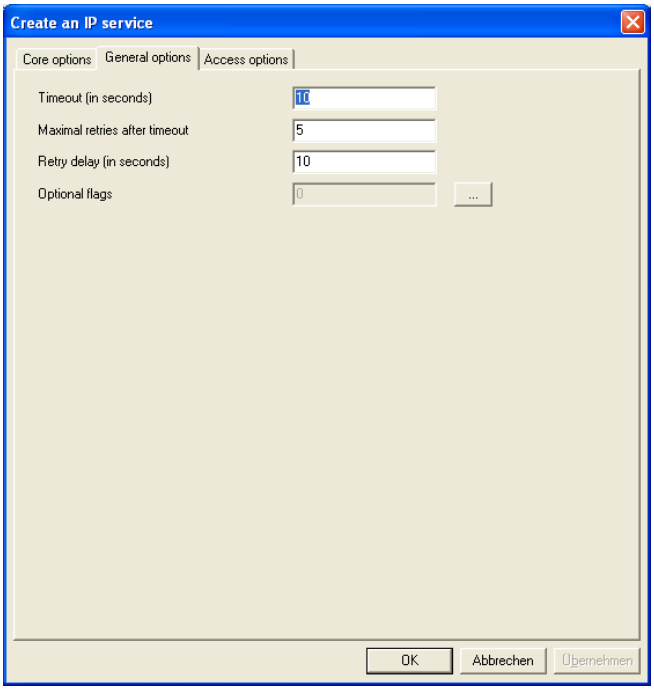


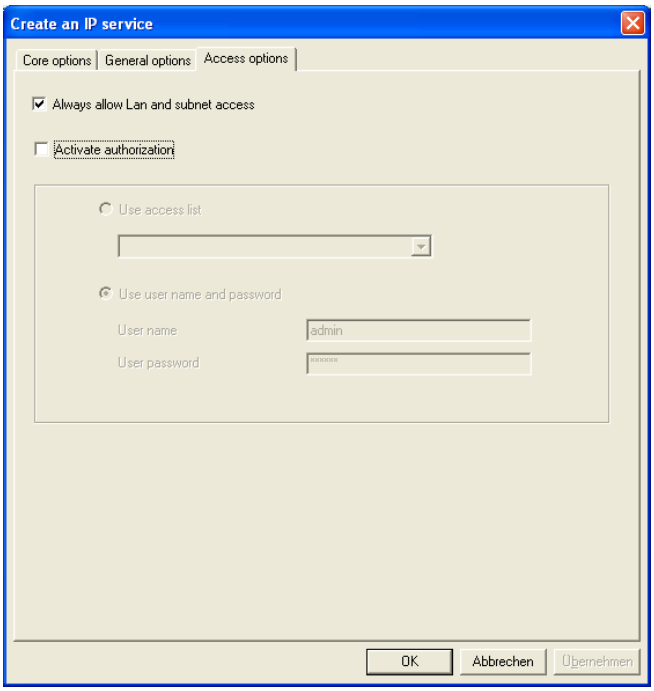


Klicken Sie erneut auf *„New“* und führen Sie die in den nächsten drei Bildern dargestellten Einstellungen durch, um den Dienst Telnet (über IP-Port 23) zu aktivieren.

Bestätigen Sie mit *„OK“*.

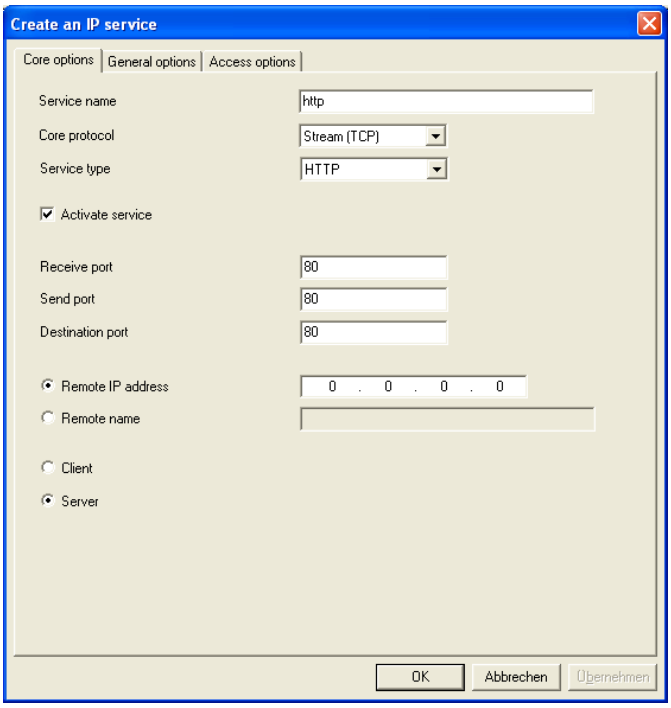

Create an IP service
Core options
General options
Access options
Service name
telnet
Core protocol
Stream (TCP)
Service type
TELNET
Activate service
Receive port
23
Send port
23
Destination port
23
Remote IP address
0 . 0 . 0 . 0
Remote name
Client
Server
OK
Abbrechen
Übernehmen

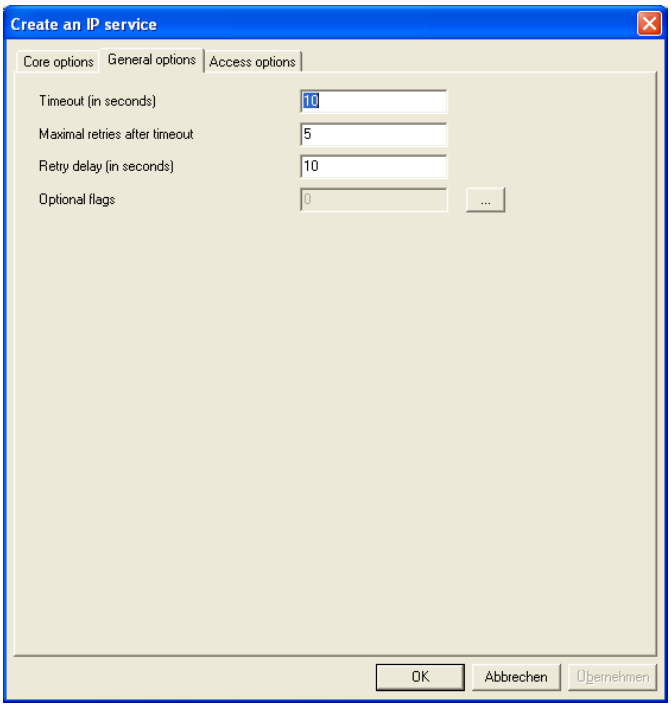

Create an IP service
Core options
General options
Access options
Timeout (in seconds)
10
Maximal retries after timeout
5
Retry delay (in seconds)
10
Optional flags
0
...
OK
Abbrechen
Übernehmen

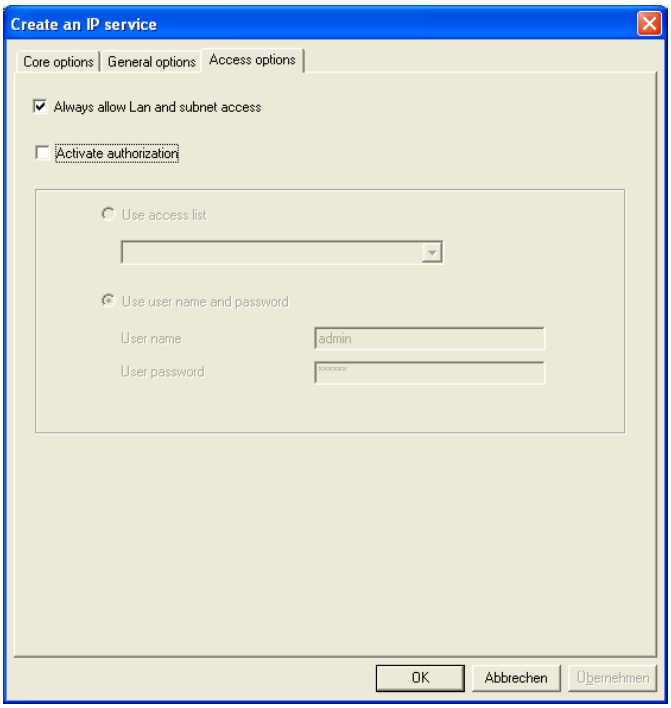


Klicken Sie nochmals auf *„New“* und führen Sie die in den nächsten drei Bildern dargestellten Einstellungen durch, um den Dienst HTTP (über IP-Port 80) zu aktivieren.

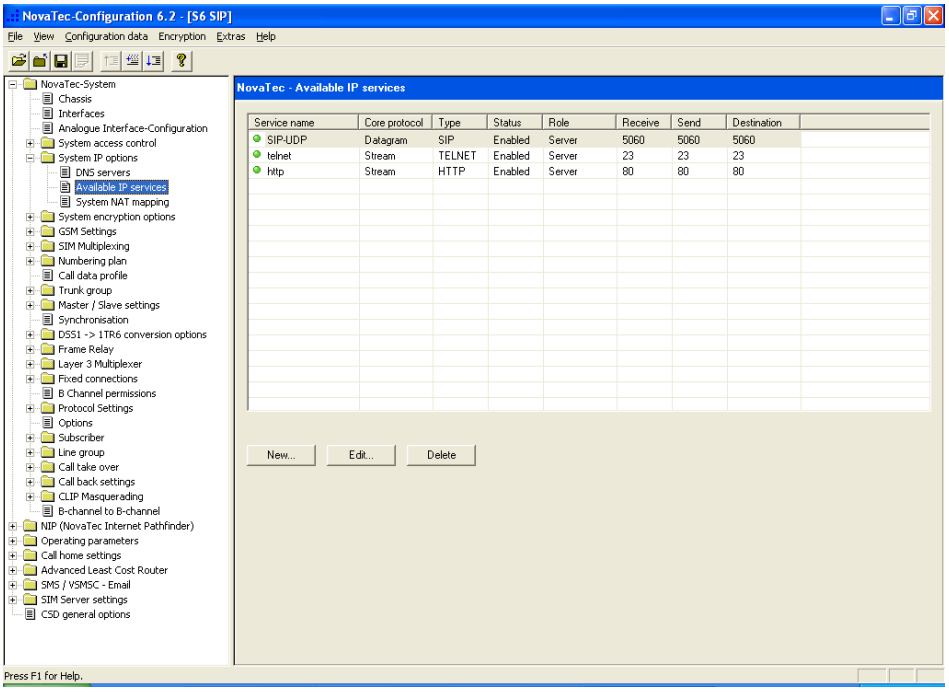
Bestätigen Sie mit *„OK“*.







Wenn Sie alle Dienste wie oben beschrieben aktiviert haben, dann müsste die Übersicht jetzt wie im Bild unten dargestellt aussehen.

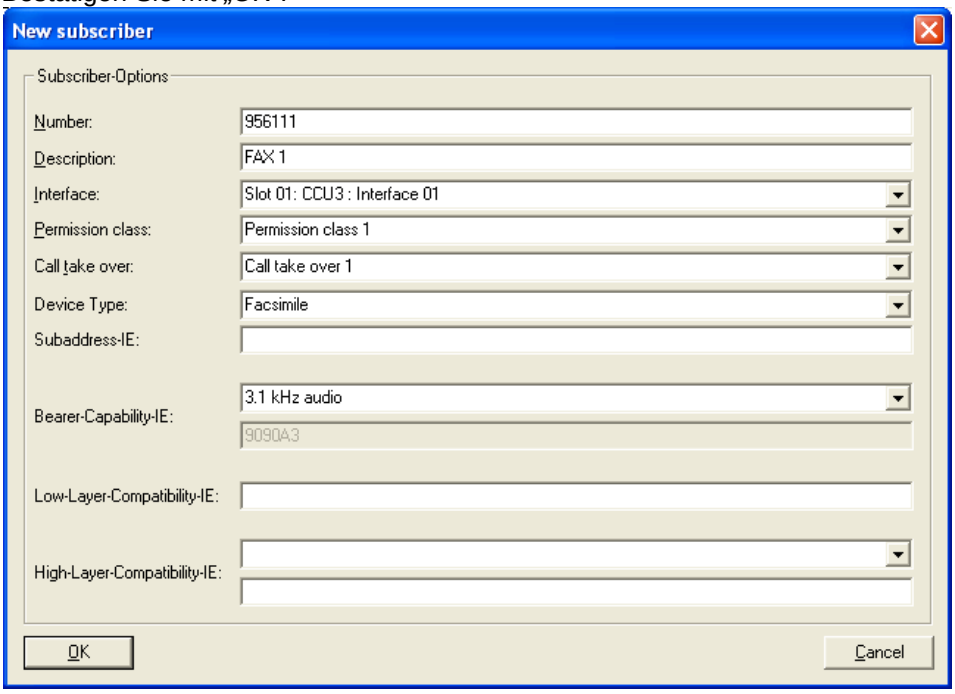


2.9 Subscriber und Permission Class konfigurieren

Gehen Sie im linken Baum unter *„NovaTec-System/Subscriber“* und klicken Sie auf *„New“.*

Nehmen Sie die unten dargestellten Einstellungen vor, um an der 1. analogen Schnittstelle ein Faxgerät mit der Nummer „956111“ zu konfigurieren.

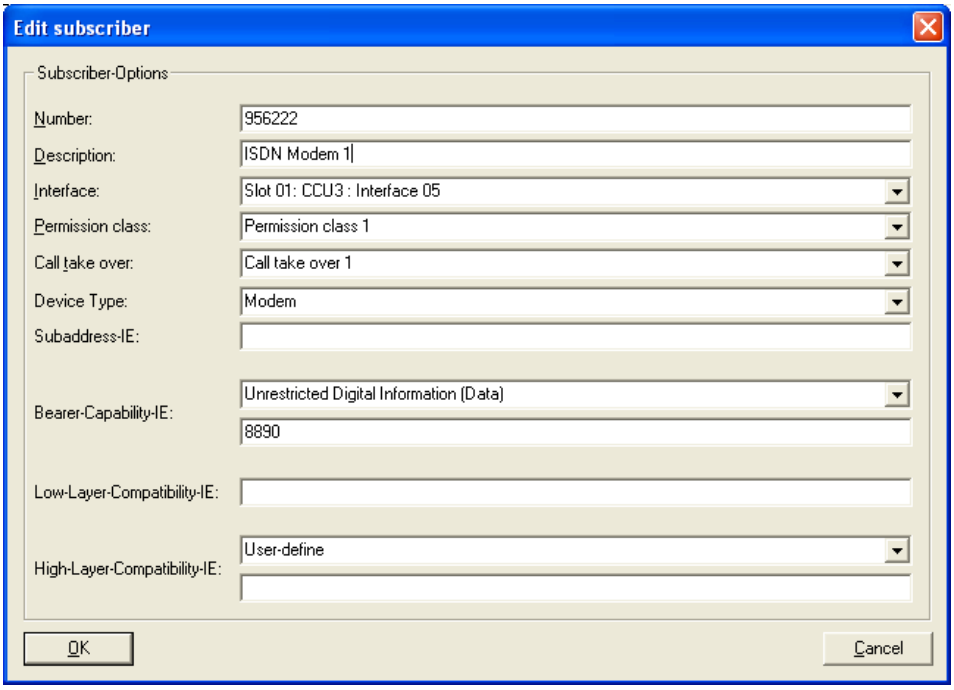
Bestätigen Sie mit *„OK“*.



Klicken Sie erneut auf *„New“.*

Nehmen Sie die unten dargestellten Einstellungen vor, um an der 1. ISDN Schnittstelle ein Modem mit der Nummer „956222“ zu konfigurieren.

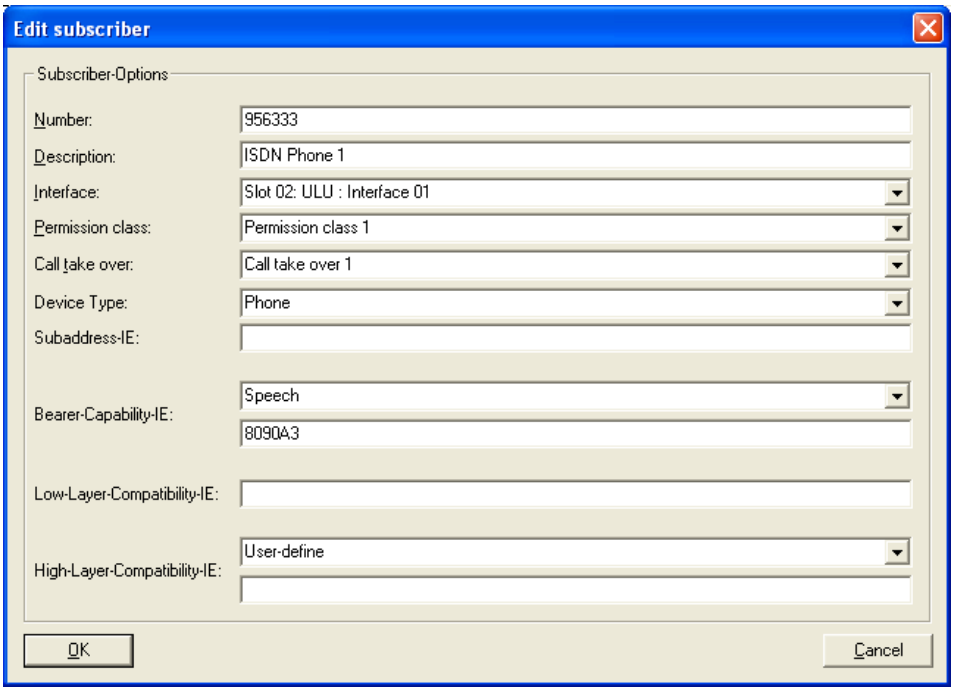
Bestätigen Sie mit *„OK“*.



Klicken Sie erneut auf *„New“.*

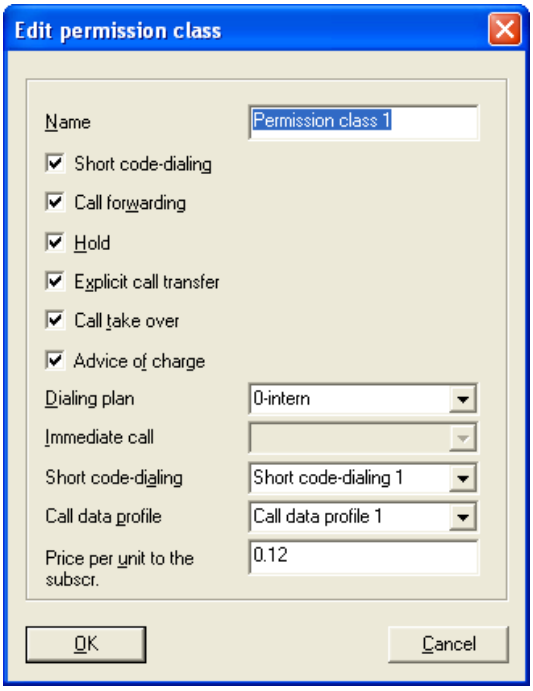
Nehmen Sie die unten dargestellten Einstellungen vor, um an der 1. U_{K0} Schnittstelle ein Modem mit der Nummer „956333“ zu konfigurieren.

Bestätigen Sie mit *„OK“*.



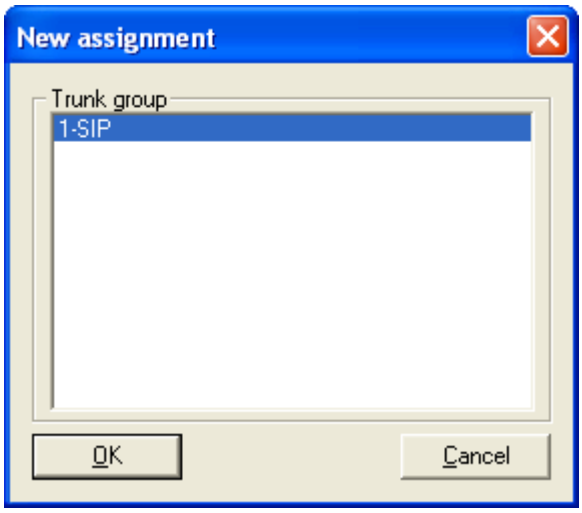
Gehen Sie im linken Baum unter *„NovaTec-System/Subscriber/Permission class“*. Selektieren Sie *„Permission class 1“* und klicken Sie auf *„Edit“*.

Führen Sie die unten dargestellten Einstellungen durch und bestätigen Sie mit *„OK“*.

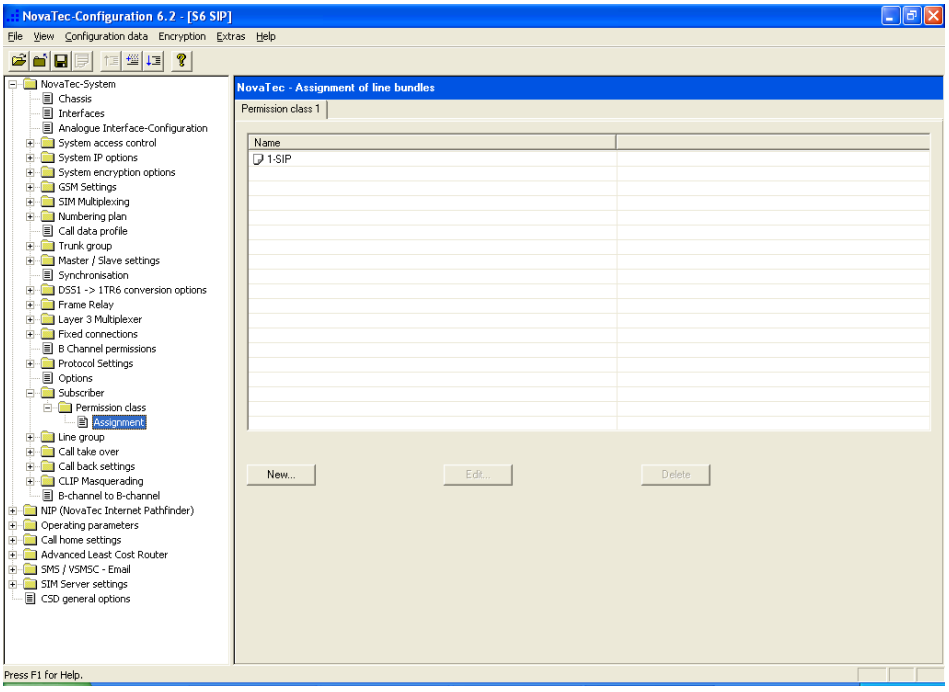


Gehen Sie im linken Baum unter „*NovaTec-System*/*Subscriber*/*Permission class*/*Assignment*“ und klicken Sie auf „*New*“.

Wählen Sie wie unten dargestellt die Trunk Group ***„1-SIP“*** aus und bestätigen Sie mit „*OK*“.



Unten sehen Sie die aktuelle Fensteranzeige nachdem die Trunk Group „*1-SIP*“ zur „*Permission class 1*“ hinzugefügt wurde.

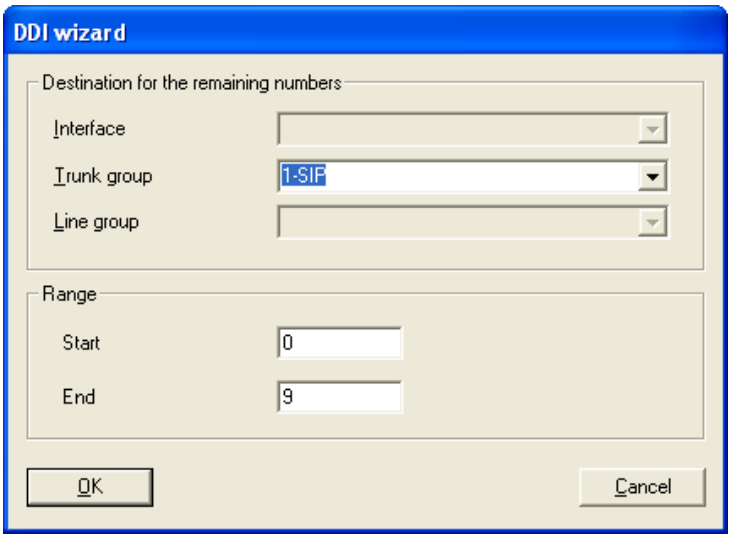


2.10 Rufnummernpläne konfigurieren

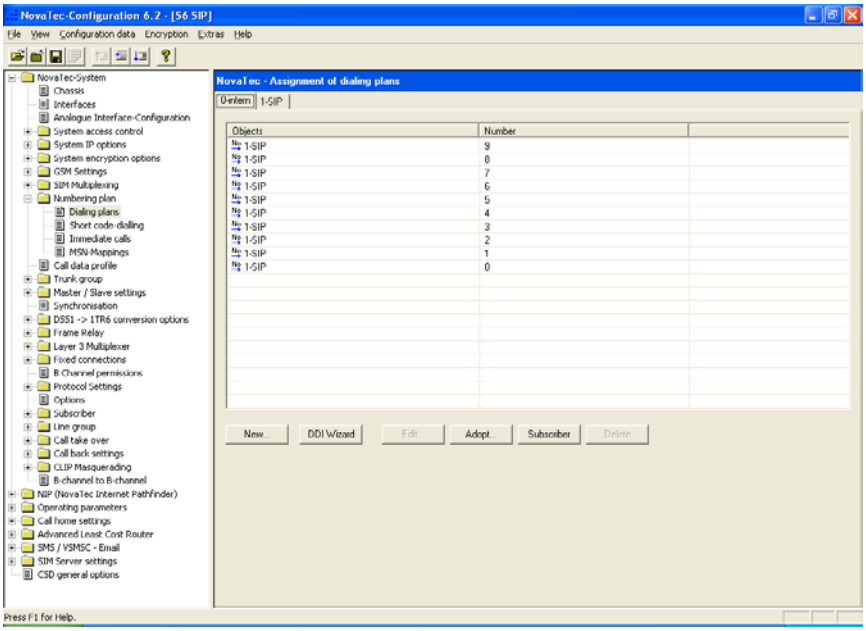
Es sind zwei Rufnummernpläne zu konfigurieren.

Der interne Rufnummernplan (Name: „0-intern“) wird von allen Teilnehmer (Endgeräten) des Systems benutzt.

Gehen Sie im linken Baum auf „*NovaTec-System/Numbering plan/Dialing plans.* Klicken Sie auf den Reiter ***„0-intern“***. *Klicken Sie auf die Schaltfläche „DDI Wizard“*. Nehmen Sie die unten dargestellten Einstellungen vor und bestätigen Sie mit *„OK“*.



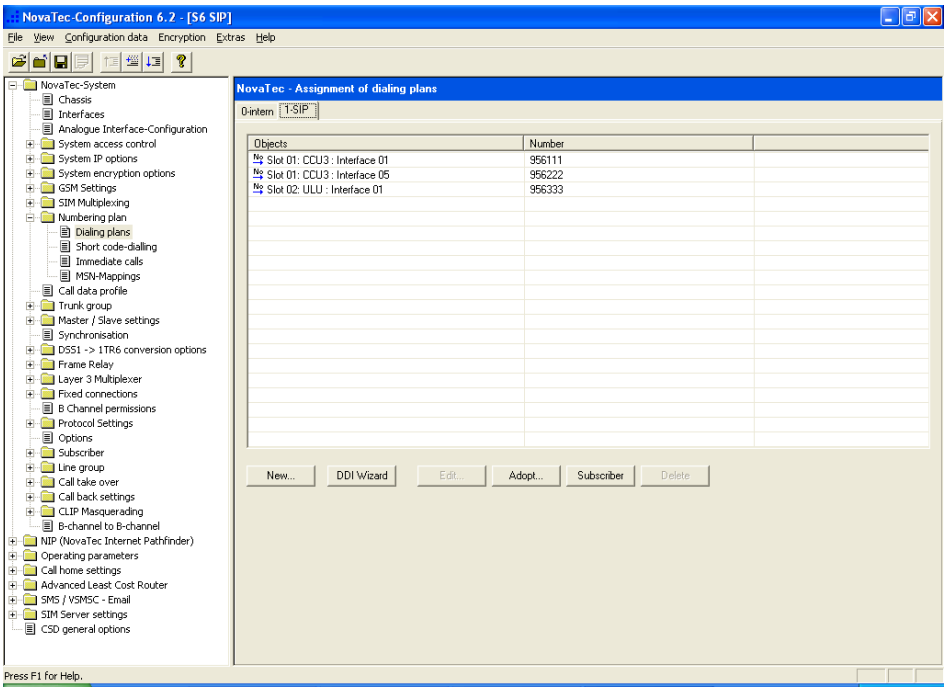
Das untere Bild zeigt die Einstellungen für den Rufnummernplan ***„0-intern“***. Alle Rufe werden zur Trunk Group *„1-SIP“* geroutet.



In den SIP-Rufnummernplan werden die Rufe der Endgeräte eingetragen.

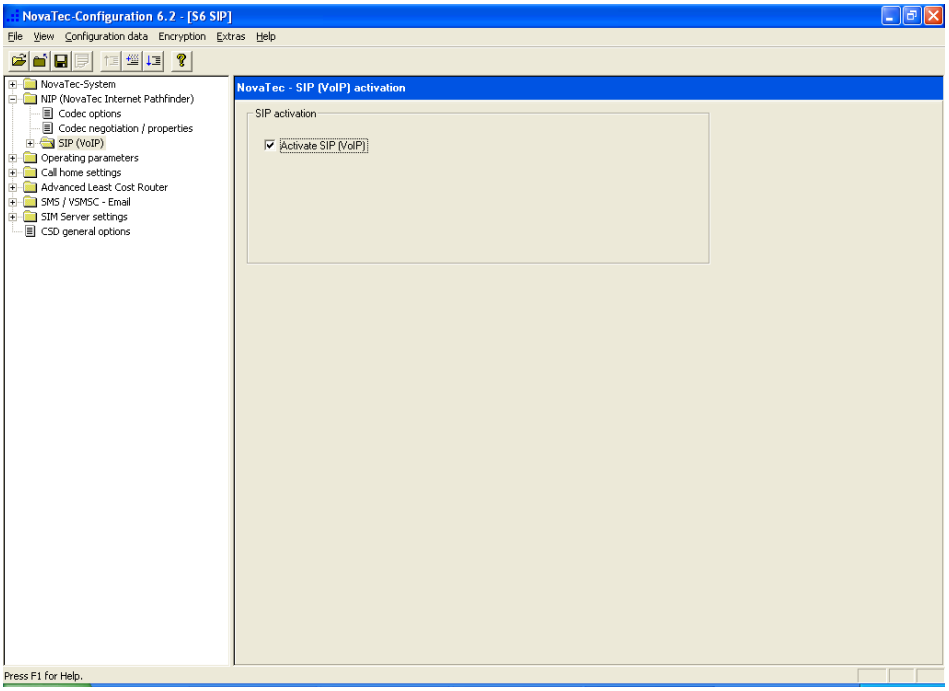
Gehen Sie im linken Baum auf *"NovaTec-Systems/Numbering plan/Dialing plans"*.

Klicken Sie auf den Reiter ***„1-SIP"*** und danach auf die Schaltfläche „*Subscriber"*. Hierdurch werden alle konfigurierten Subscriber in den Rufnummernplan eingetragen (siehe unten).



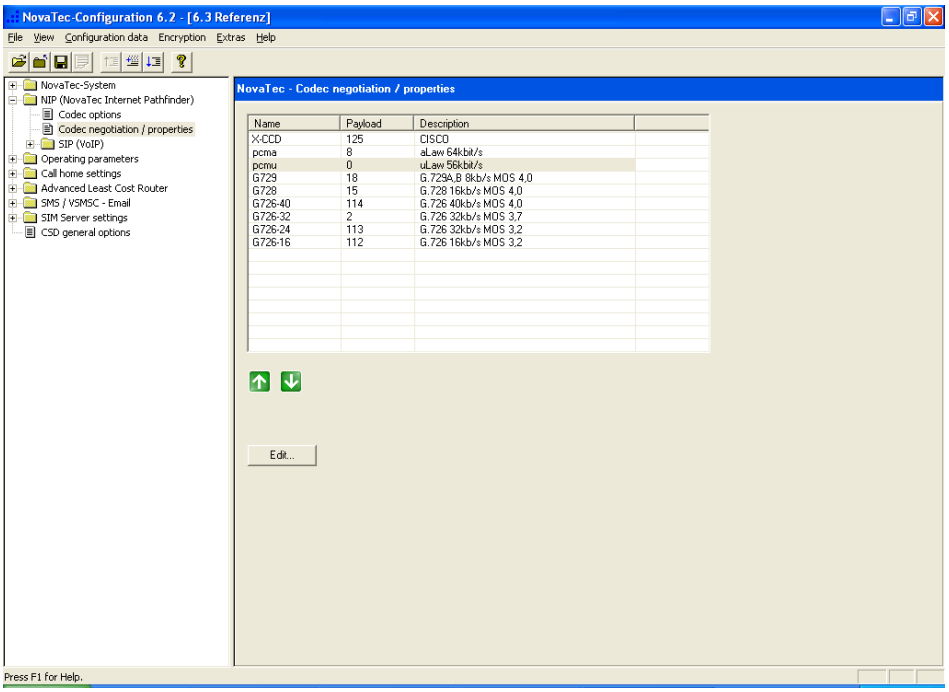
2.11 SIP aktivieren

Gehen Sie im linken Baum unter *„NIP/SIP“* und aktivieren Sie die Option *“Activate SIP“*.



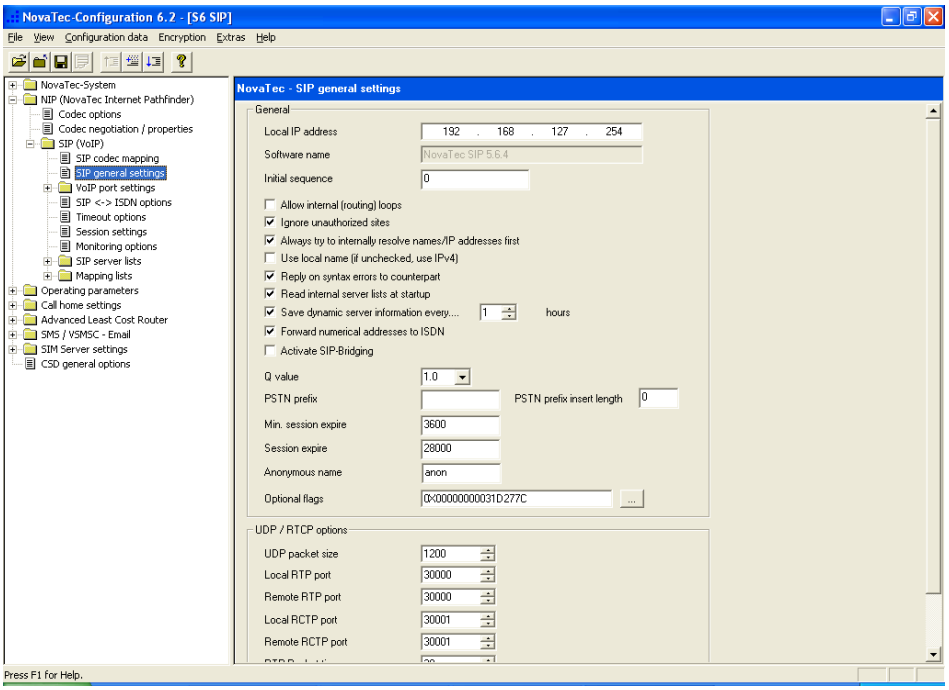
2.12 Codec Prioritäten definieren

Gehen Sie im linken Baum auf *„NIP/Codec negotiation“*. Selektieren Sie einen Codec und benutzen Sie die Schaltflächen mit den Pfeilen um die Priorität des Codecs zu ändern. Der Codec ganz oben in der Liste hat die höchste Priorität. Das Bild unten zeigt eine typische Codecpriorität. Der Codec X-CCD (Cisco Clear Channel Codec) sollte immer die höchste Priorität haben, also ganz oben in der Liste stehen.



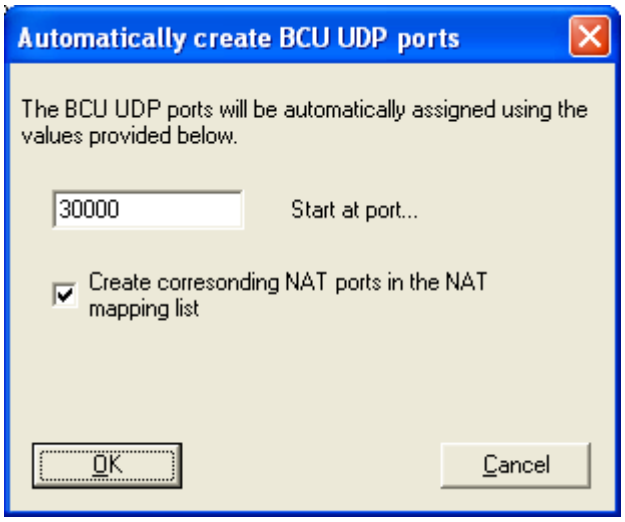
2.13 SIP General Settings kontrollieren

Gehen Sie im linken Baum unter *„NIP/SIP/SIP general settings“*. Die Einstellungen sollten sein wie unten dargestellt.

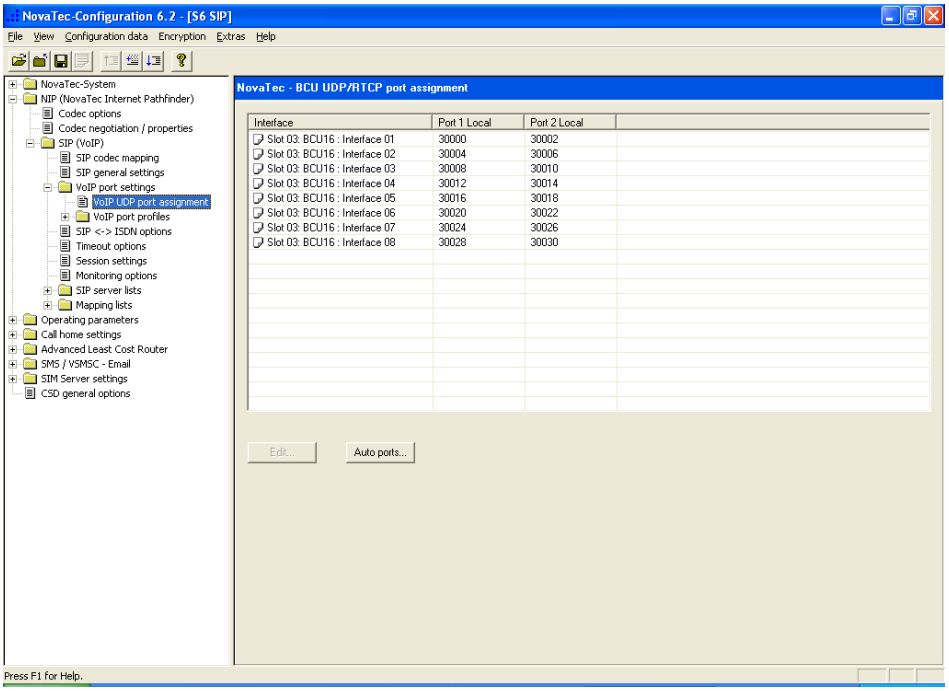


2.14 UDP Ports bestimmen

Gehen Sie im linken Baum unter *„NIP/SIP/VOIP port settings/VOIP UDP port assignment“* und klicken Sie auf die Schaltfläche *„Auto ports…“*. Wählen Sie die für RTP zu verwendenden IP-Ports aus, indem Sie eingeben welches der erste IP-Port für RTP ist (siehe unten).

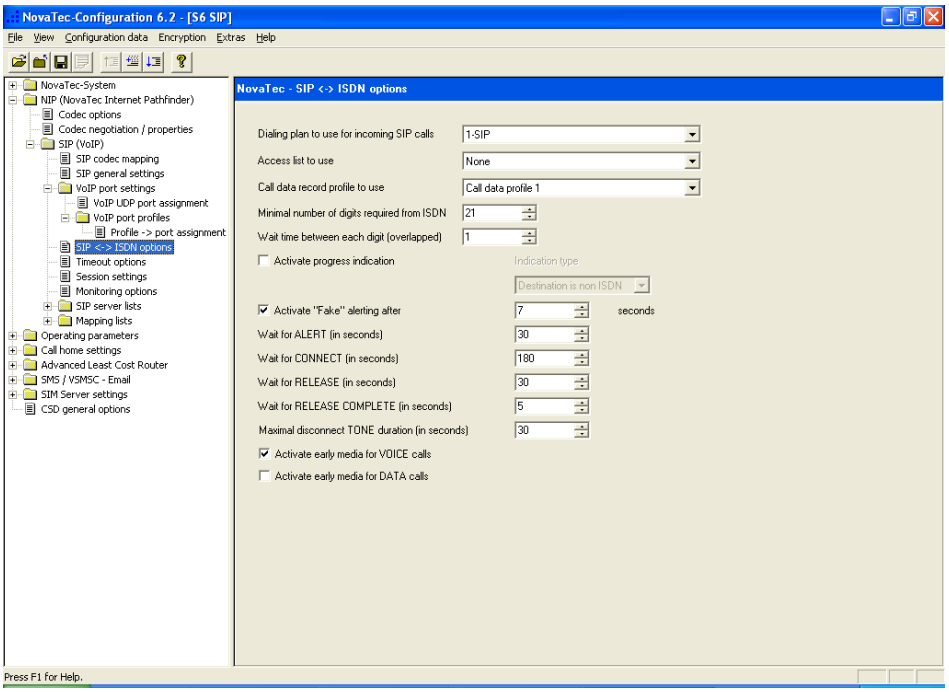


Die Konfigurationsoberfläche vergibt dann für jede VoIP-Schnittstelle zwei IP-Ports. Einen für RTP und den nächst höheren für RTCP.



2.15 SIP ISDN Options

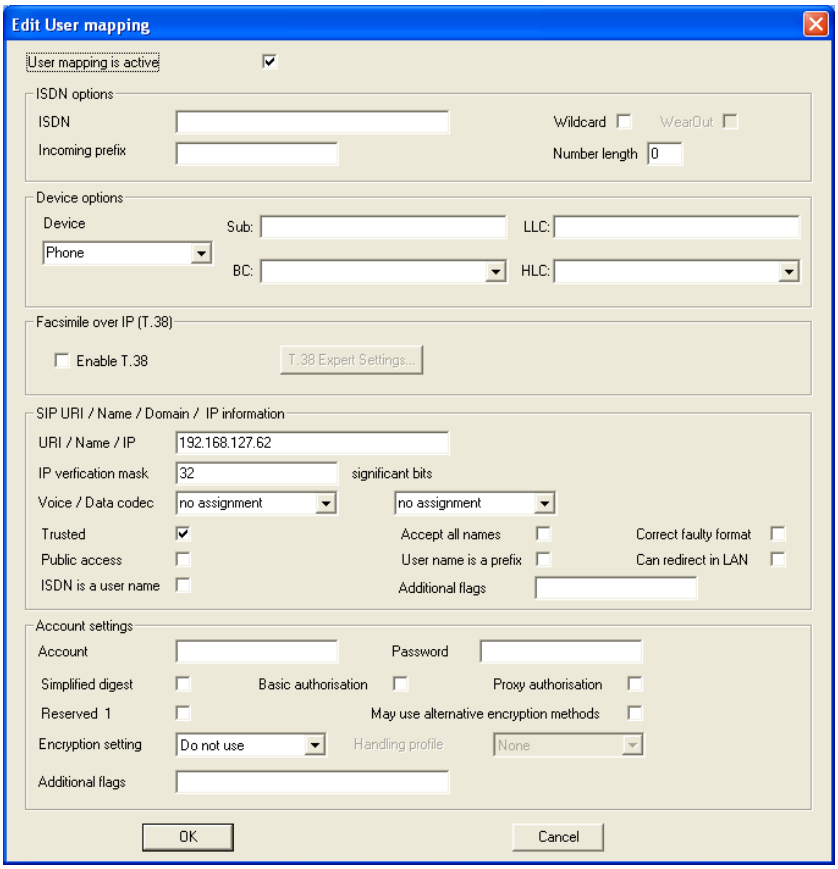
Gehen Sie im linken Baum unter *„NIP/SIP/SIP <-> ISDN options“* und nehmen Sie die unten dargestellten Einstellungen vor.

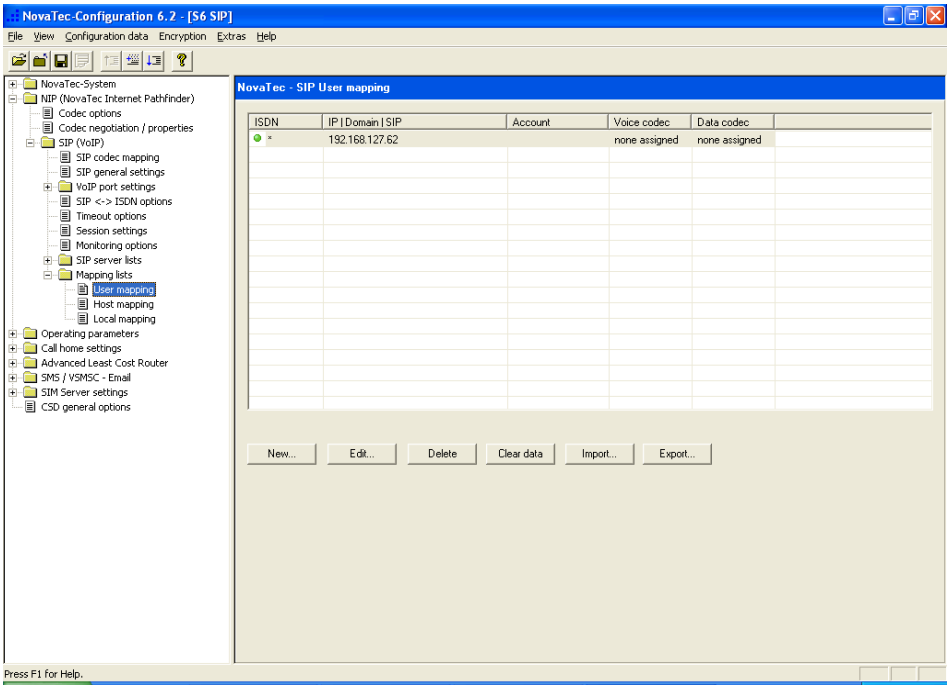


2.16 Mapping Lists

Gehen Sie im linken Baum unter *„NIP/SIP/Mapping lists/User mapping“* und klicken Sie auf *„New“*.

Nehmen Sie die unten dargestellten Einstellungen vor. Unter „URI / Name / IP“ geben Sie die IP-Adresse des Cisco Unified Communication Managers ein.

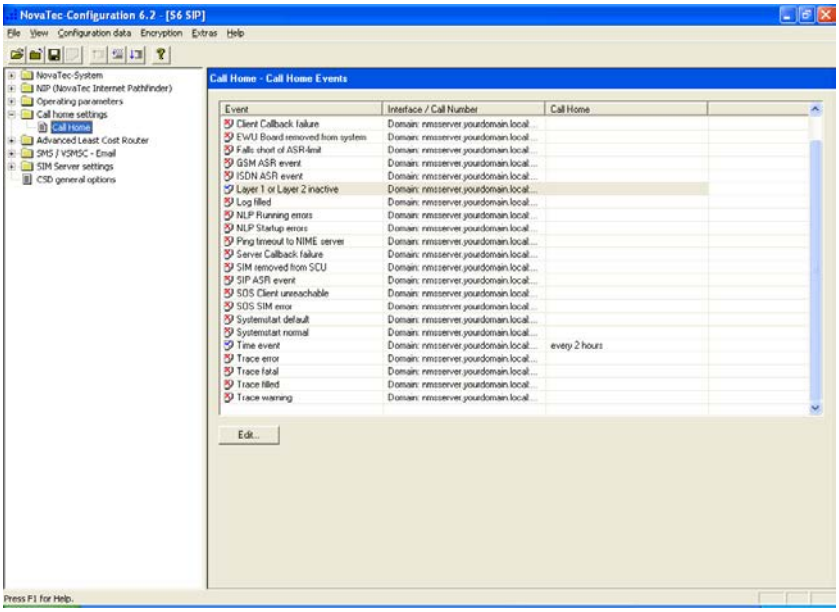




Nachdem Sie mit „OK“ bestätigt haben sehen Sie in der Übersicht noch mal die IP-Adresse des Cisco Unified Communication Managers.

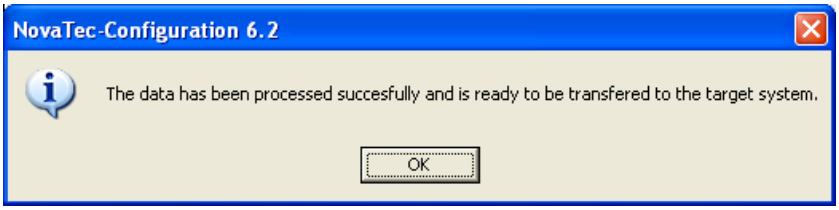
2.17 Call Home Settings

Gehen Sie im linken Baum unter *„Call Home settings“* und aktivieren Sie die gewünschten Call-Home-Events die an das NovaTec Netzwerk Management-System gemeldet werden sollen.



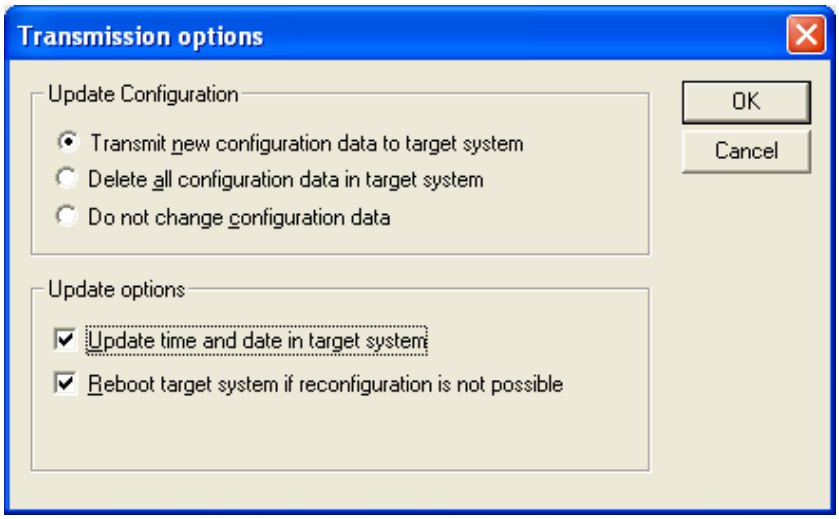
2.18 Datenbank aufbereiten und auf das System aufspielen

Wählen Sie den Punkt *„Configuration data/Process“* in der Menüleiste aus. Wenn keine groben Fehler oder Inkonsistenzen in den Konfigurationseinstellungen vorhanden sind, erhalten Sie folgende Meldung:



Bestätigen Sie mit *„OK“*. Sollten Sie eine Fehlermeldung bekommen, so kontrollieren Sie bitte Ihre Einstellungen.

Wählen Sie aus dem Menü den Punkt *„Configuration data/Transmit to target system“* aus.



Nehmen Sie die oben dargestellten Einstellungen vor und bestätigen Sie mit *„OK“*.

2.19 SRTP aktivieren

Gehen Sie im linken Baum auf „*Encryption/Enter serial number…“*.

Die Daten für Encryption werden von NovaTec GmbH erstellt und an den Kunden in folgender Form geliefert:

User name: *xxxxxxxxxxx (z.B. Name des Kunden)*

Backplane ID: *000006767676*

Serial number:
FB11 - EF76 - CA90 - EC73 - EF00
BF12 - AE30 - CC47 - FC46 - AD47

Nachdem die Encryption Daten eingetragen wurden, schließen Sie die Datenbank und öffnen Sie sie danach wieder.

Folgende weitere Schritte sind notwendig:

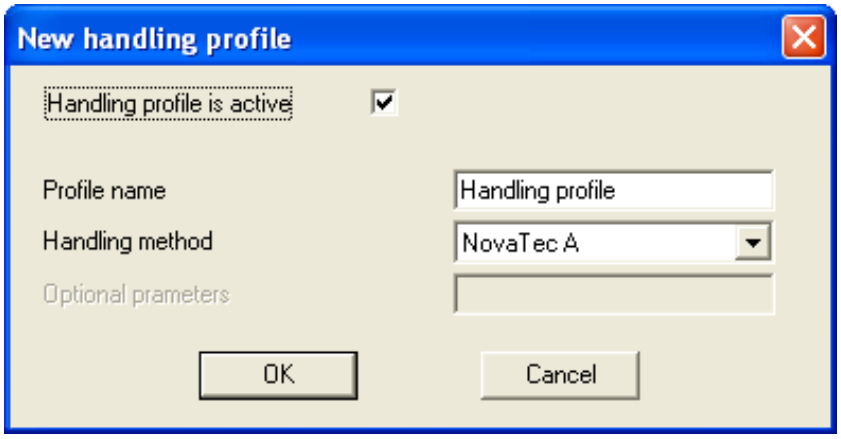
Gehen Sie im linken Baum auf *„NovaTec-System/System encryption options/Encryption profiles“* und klicken Sie auf „New“.

Wählen Sie die gewünschten Verschlüsselungsoptionen aus (siehe unten).

Bestätigen Sie mit *„OK“*.

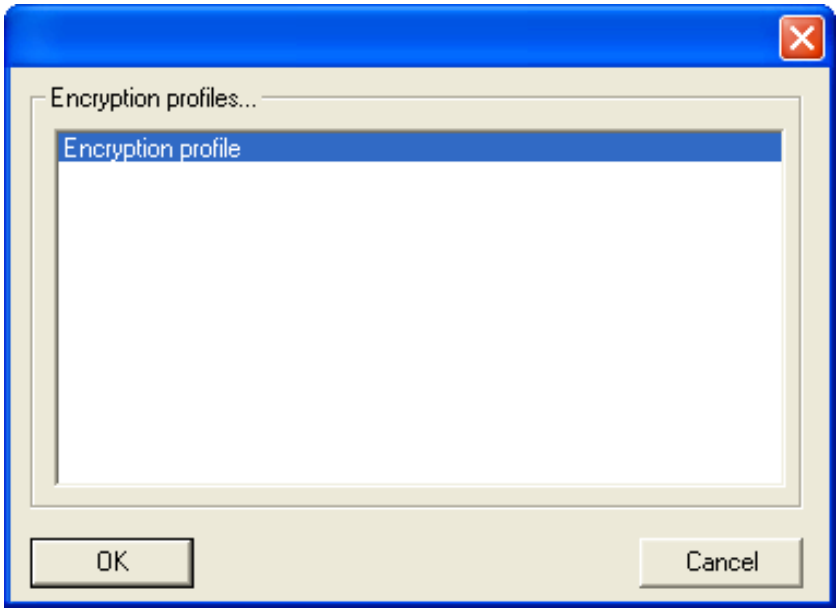
Gehen Sie im linken Baum auf *„NovaTec-System/System encryption options/Encryption handling profiles“* und klicken Sie auf *„New“.*

Nehmen Sie die unten dargestellten Einstellungen vor und klicken Sie auf *„OK“.*



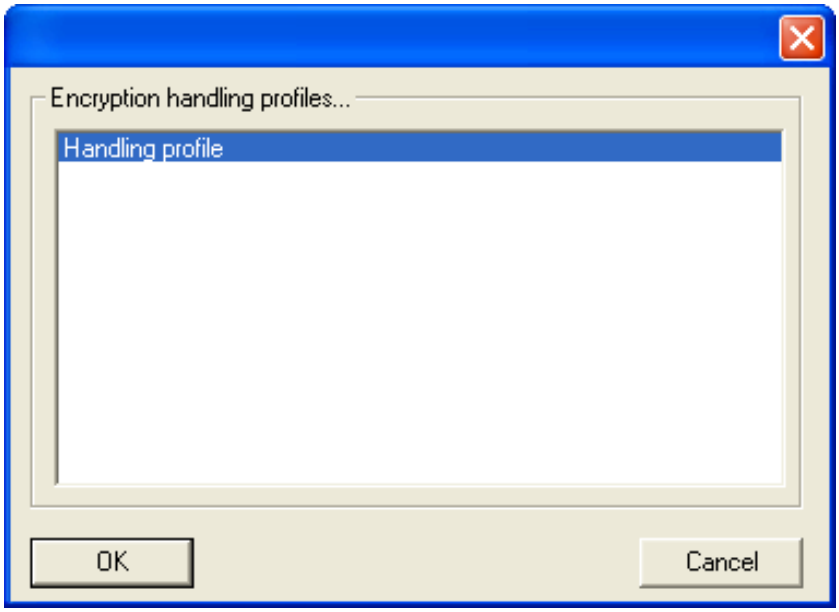
Gehen Sie im linken Baum auf *“NovaTec-System/System encryption options/Encryption handling/profiles/Encryption ->Handling assignment“* und klicken Sie auf *„New”*.

Wählen Sie *„Encryption profile“* aus und bestätigen Sie mit *„OK“*.

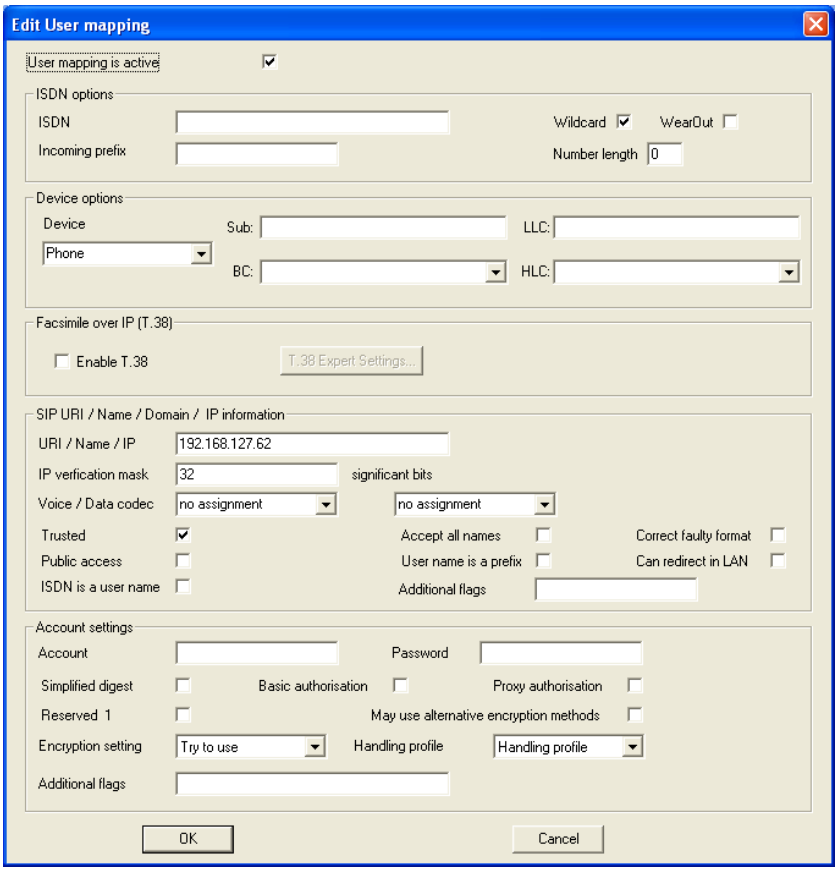


Gehen Sie im linken Baum auf *“NovaTec-System/System encryption options/System module / interface settings/Module assignment“* und klicken Sie auf *„New“*.

Wählen Sie *„Handling profile“* aus und bestätigen Sie mit *„OK“*.



Gehen Sie im linken Baum unter *„NIP/SIP/Mapping lists/User mapping“* und klicken Sie auf *„Edit“*. Wählen Sie für *„Encryption setting“ „Try to use“* aus und für *„Handling profile“ „Handling profile“*.



Bestätigen Sie mit *„OK“*.

Wiederholen ab 2.17. Call Home Settings.

3 DCHP aktivieren

Durch Auswahl des Menüpunktes „System-IP-Options“ im linken Teilfenster der Applikation „NTConf“ erscheint im rechten Teilfenster folgender Dialog.

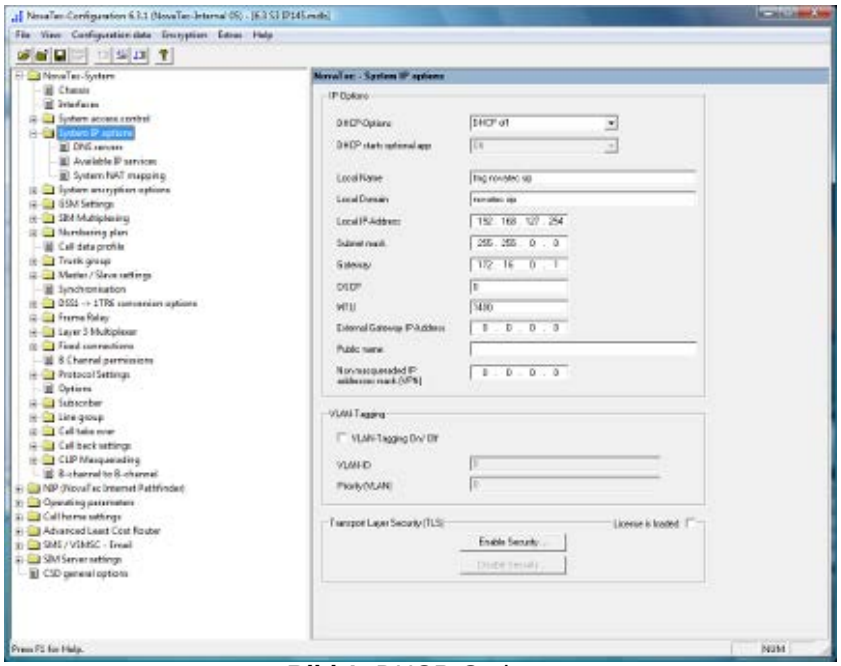


Bild 1: DHCP-Options

DHCP-Optionen lassen sich nun durch Auswahl der entsprechenden Punkte in den beiden Combo-Boxen (Auswahl-Boxen) definieren.

Falls DHCP aktiviert wird, werden nicht benötigte Eingabe-Felder „ausgegraut“, d.h. deaktiviert.

4 Allgemeine Vorgehensweise TLS

Die nachfolgende Vorgehensweise wird allen Kunden zur sicheren Handhabung der Verschlüsselung (TLS/SRTP) zwischen den NovaTec-Systemen bzw. mit dem Service-PC empfohlen.

4.1 Erstellen eines "Root Certification Authority Certificate"

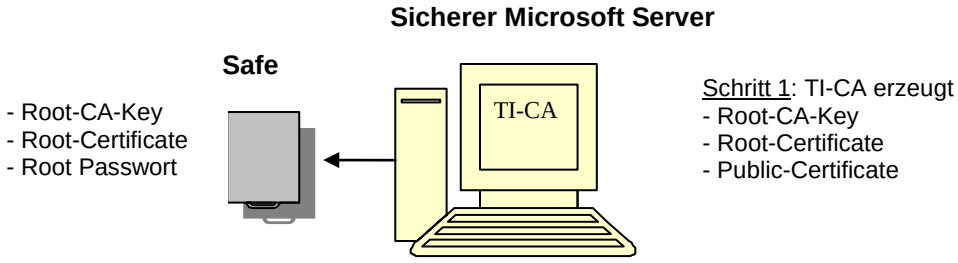


Bild 1: Root-CA erstellen

Der erste Schritt im Vorfeld besteht für den Kunden aus dem einmaligen Generieren eines „Root Certification Authority Certificate" (Root-CA). Sollte der Kunde bereits ein Zertifikat von einer Zertifizierungsstelle haben, so kann dieser Schritt übersprungen werden.
Das Erzeugen einer Root-CA muss mit dem NovaTec Tool „Trace Info Client" (TI-CA) vorgenommen werden. Die Applikation soll auf einem „zugriffsicheren Microsoft Server" installiert werden. Zugriffsicher bedeutet, dass der Server sich in einem verschlossenen Raum ohne LAN-Anschluss befindet.
Über das „Graphical User Interface" der TI-CA Applikation wird nun ein verschlüsselter Root-CA-Key (cakey.pem), ein Root-Certificate (cacert.pem) und ein Public-Certificate (cacert.crt) erstellt.

Der Root-CA Key (cakey.pem) und das Passwort dieses Schlüssels sind die sensibelsten Teile einer CA-Infrastruktur und müssen zusammen mit dem Root-Certificate (cacert.pem) im Safe des Kunden aufbewahrt werden.

Zum Transport in den Safe, kann man dem TI als Speichermedium für die Ausgabedateien zum Beispiel einen USB-Stick angeben und diesen im Safe lagern.

Das so gesicherte „Root-CA" dient ausschließlich dem Signieren anderer Zertifikate (siehe Punkt 5).

Das Public-Certificate (cacert.crt) wird allen an dieser CA-Infrastruktur beteiligten Maschinen zur Verfügung gestellt (siehe Punkt 3).

4.2 Maschinen-Freischalt-Code beziehen

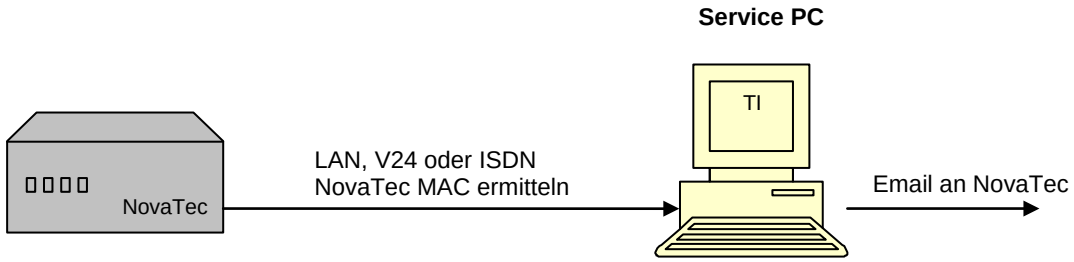


Bild 2: TLS Lizenz beziehen

Im Schritt 2 muss der Kunde mittels „TI“ Applikation die MAC-Adresse der entsprechenden Maschine (S3, S5, S6 oder S20) auslesen und an NovaTec-Support per Email senden.

NovaTec bestimmt einen individuellen Freischalt-Code für dieses System und übermittelt diesen dem Kunden via Email.

4.3 Verschlüsselung konfigurieren

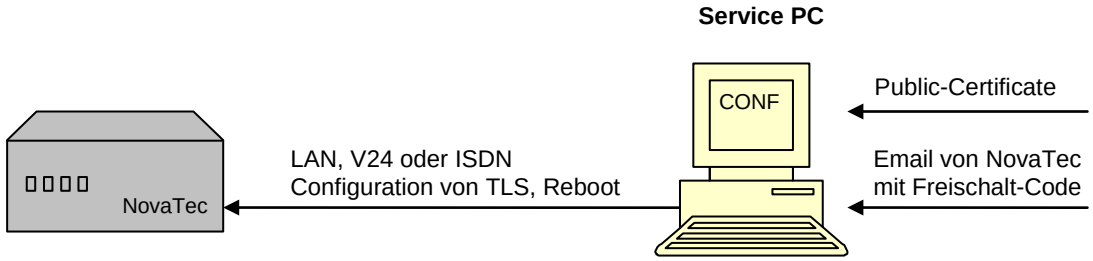


Bild 3: TLS für NovaTec System konfigurieren

Per Novatec Konfigurationsprogramm „NtConf“ kann in diesem Schritt nur das System mit der entsprechenden MAC-Adresse konfiguriert bzw. für TLS frei geschaltet werden.

Hierzu gibt es in der Konfigurationsoberfläche drei Kategorien: NMS, SIP und Maintenance.
Wobei Maintenance folgende Applikationen „TI, NtConf und Callserver“ beinhaltet.

Nach der Eingabe des „Freischalt-Codes“ (Schritt 2) können die drei aufgeführten Kategorien für TLS/SRTP eingeschaltet und konfiguriert werden. Je nach Sicherheitsgrad sind die in der Tabelle 1 aufgeführten Modi möglich. Zum Beispiel, importieren des „Public Certificate“
(cacert.crt) aus Punkt 1

Der ungeschützte Zugriff auf die Maschinen vor Ort ist nach der Aktivierung von TLS nicht mehr möglich. Alle Zugriffe über V24/USB, ISDN und IP wie HTTP und TELNET werden nicht angenommen.

4.4 Privaten Schlüssel in dem System erzeugen

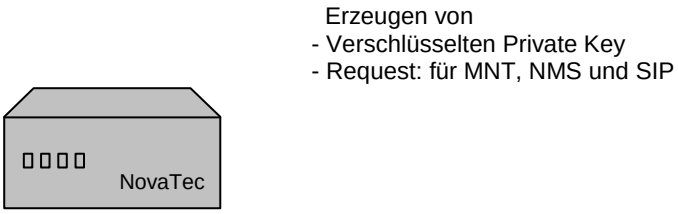


Bild 4: NovaTec System erzeugt private Key und Requests

Dieser Schritt funktioniert nur, wenn die Konfiguration im vorherigen Schritt vollständig und fehlerfrei durchgeführt worden ist. Dieser Schritt geschieht automatisch beim Reboot und dauert zwischen 20-30 Sekunden plus normale Reboot-Zeit.

Beginnend mit dem Übertragen der Konfigurationsdaten auf die Hardware überprüft diese nach dem erforderlichen „Reboot“ den Freischalt-Code auf Gültigkeit. Ist die Überprüfung positiv, so akzeptiert die NovaTec Hardware die neue Konfiguration mit Verschlüsselung.

Zusätzlich bewirkt dieser „Reboot“ nach der erfolgreichen Konfiguration folgende maschineninterne Aktionen:

- Hardware Private Key erzeugen

Erzeugen eines verschlüsselten privaten RSA-Key, welcher in einem nichtflüchtigen Speicher der Hardware gehalten wird. Es sind keinerlei Zugriffe auf diese Speicher von außen möglich.
Der Schlüssel bleibt in der Hardware und kann weder gelesen, überschrieben noch gelöscht werden. Das Passwort für den Schlüssel wird nicht gespeichert sondern zur Laufzeit Hardware individuell dynamisch generiert. Für jede Maschine wird so ein anderes Passwort erzeugt.

- Hardware Certificate Signing Request erzeugen

Nach dem Erzeugen des privaten Schlüssels generiert jede der drei konfigurierten Kategorien (Punkt 3) einen entsprechenden „Certification Signing Request“:

Maintenance, NMS und SIP erzeugen mit der Hilfe des „Private Key“ die Files mtn_req.csr , nms_req.csr und sip_req.csr und speichern sie freizugänglich im Flash-Dateisystem.

Achtung: Die Request-Files werden nach dem ersten erfolgreichen Öffnen des entsprechenden Zertifikats automatisch gelöscht.

4.5 Signieren der „Hardware Certificate Signing Request“

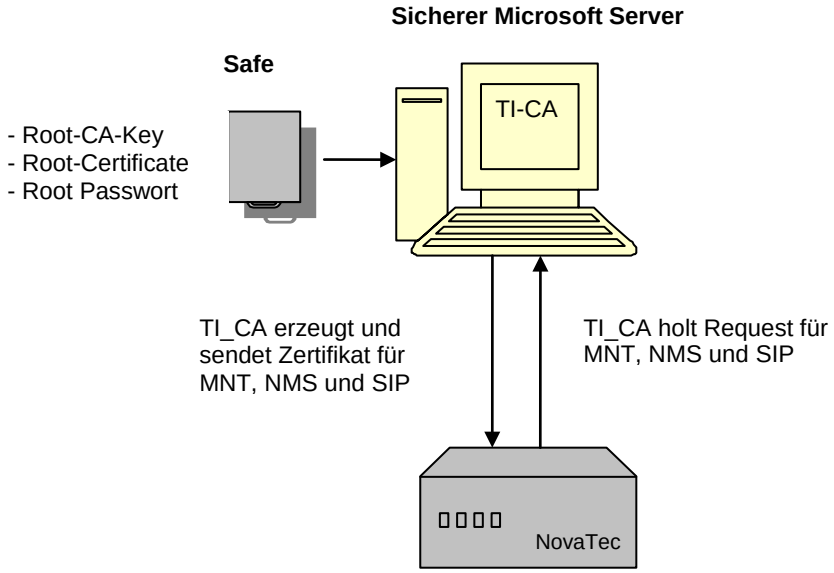


Bild 5: NovaTec System wird signiert lokal vom Server

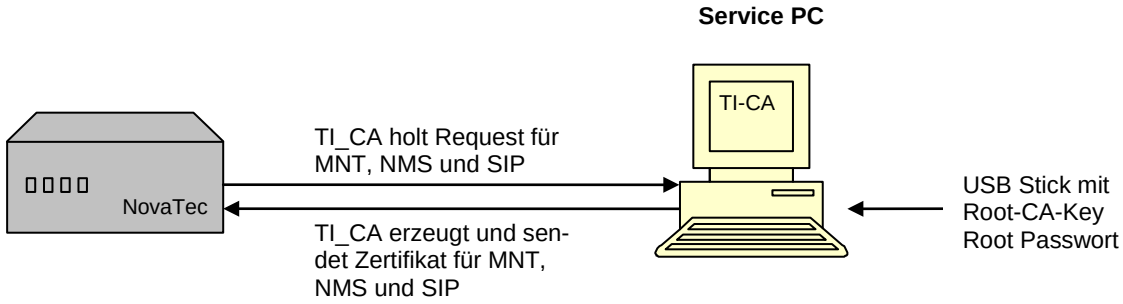


Bild 6: NovaTec System wird signiert vom Service PC

Die im Punkt 4 durch die Hardware erzeugten drei „Certification Signing Request“ müssen durch die „Root-CA“ (bzw. übergeordneten CA’s siehe Punkt 1) signiert werden.

Bei dieser Aktion erhält man entsprechende Zertifikate (Dateien) für die Hardware: mtn_cert.crt , nms_cert.crt und sip_cert.crt.

Die Durchführung dieses 5. Schritts ist wieder sicherheitsproblematisch, da hierzu der verschlüsselte Root-CA-Key (cakey.pem von Punkt 1) und das Passwort benötigt werden.

Der Transport des Schlüssels vom Safe zum sicheren Server (Punkt 1) lässt sich wieder mittels USB-Stick bewerkstelligen. Der TI-CA kann die Datei (cakey.pem) direkt vom USB-Stick importieren.

Achtung: ist das Zertifikat ungültig, so ist das System blockiert und muss vor Ort in den Zustand “Default“ gebracht werden. In diesem Zustand kann das System im Netz nicht betrieben werden und braucht wieder eine passende Konfiguration. Hierzu kann mit Hilfe von NovaTec Tools die neue Konfiguration auf

das Gerät aufgespielt werden oder mit Hilfe von z.B. „Telnet“ die IP Einstellungen des Gerätes so zu verändern, dass das Gerät in die Lage versetzt wird, sich die Konfiguration von dem NMS herunter zu laden.

4.6 Erzeugen der PC Schlüssel und Zertifikate

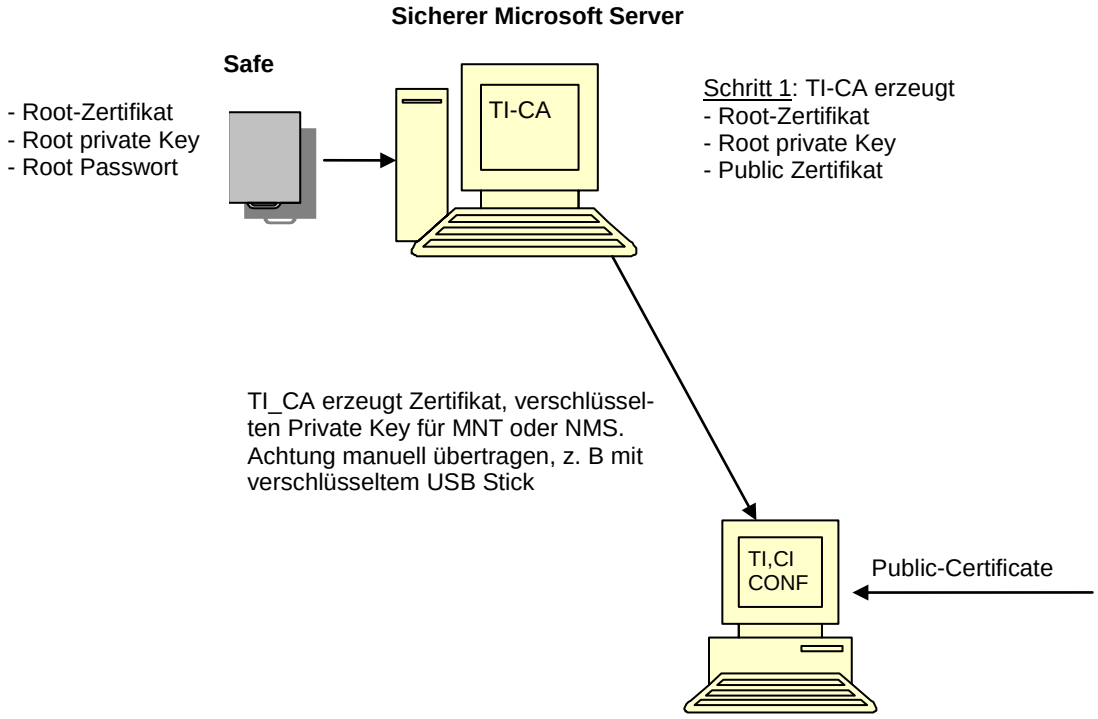


Bild 7: TI-CA signiert die NovaTec PC-Tools MNT und NMS

Damit der Service PC mit der NovaTec Hardware mit TLS kommunizieren kann, müssen auch die PC-Applikationen in die CA-Infrastruktur aufgenommen werden. Der TI-CA erzeugt hierzu einen verschlüsselten private Key und ein von der CA signiertes Zertifikat. Diese Dateien müssen zusammen mit dem public Certificate der CA auf den Service PC gespeichert und bei TI, CI, CONF und NMS importiert werden. Natürlich muss auch das Passwort des private Key importieren werden (z. B. mit verschlüsseltem USB-Stick).

Nach diesem Schritt sind alle Aktionen abgeschlossen und der Service PC kann TLS verschlüsselt mit dem NovaTec System kommunizieren

Dieser Schritt ist nicht bei SIP Verbindungen zwischen NovaTec Systemen notwendig.

4.7 Erläuterungen zu den Hardware TLS1.0 Modi laut RFC4346

Server-Modi für die Applikationen Maintenance (TI, NtConf, Callserver) und SIP

Mode	Server-Key	Server-Cert	CA-Cert	Bemerkungen
0	-	-	-	Unverschlüsselt
1	mandatory	-	-	Anonymous Mode Wird nicht unterstützt
2	mandatory	mandatory	-	Optional: Keine Client Überprüfung Sicherheit: mittel
3	mandatory	mandatory	mandatory	Volle Überprüfung: Sicherheit hoch
4-8	-	-	-	Bei TLS nicht erlaubt

Client-Modi für die Applikationen NMS und SIP

Mode	Client-Key	Client-Cert	CA-Cert	Bemerkungen
1	mandatory	-	-	Anonymous Mode Wird nicht unterstützt
2	mandatory	-	mandatory	Optional: Keine Client Überprüfung Sicherheit: mittel
3	mandatory	mandatory	mandatory	Volle Überprüfung: Sicherheit hoch
4-8	-	-	-	Bei TLS nicht erlaubt

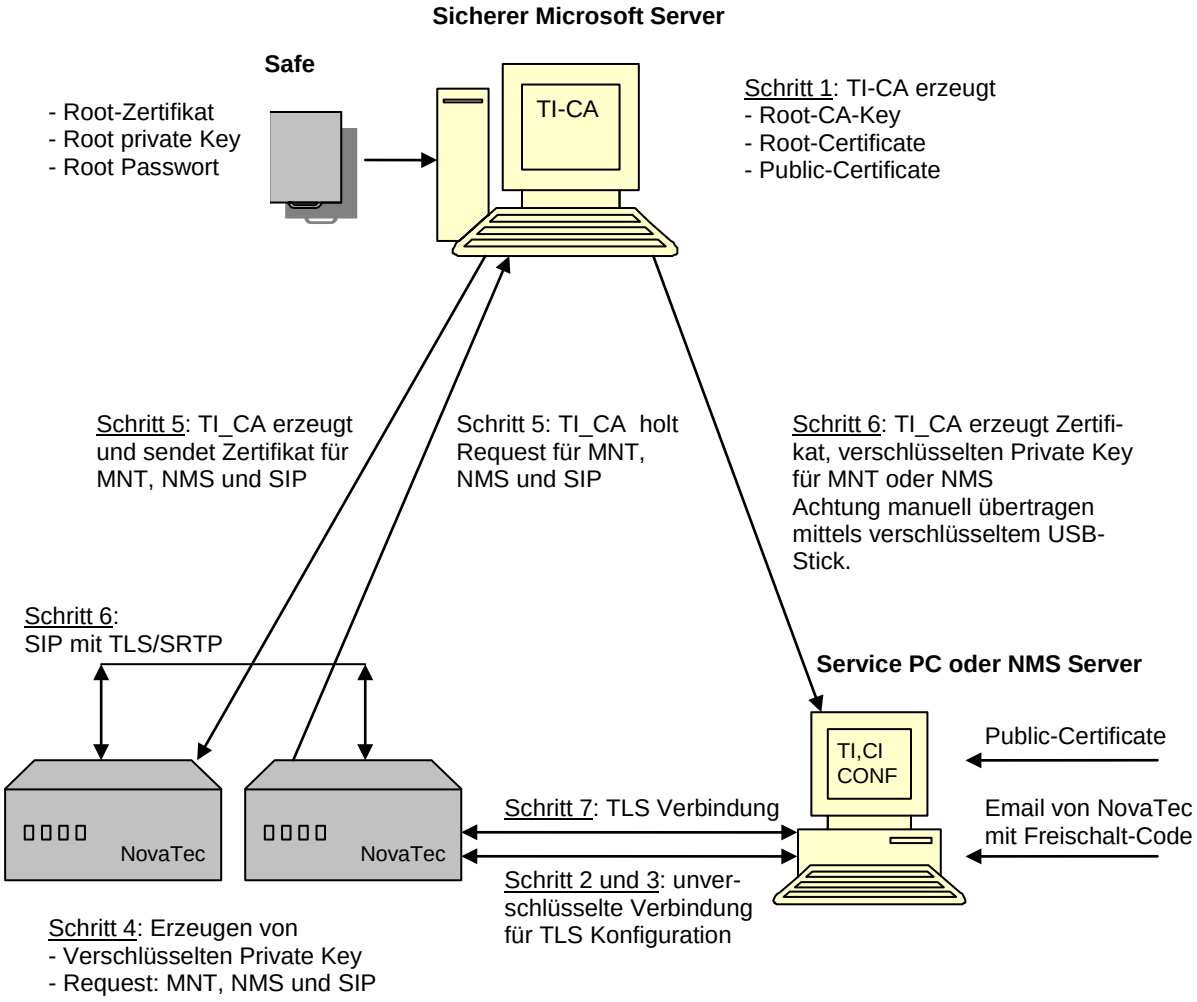


Bild 8: CA-Infrastruktur

Anmerkungen zu Schritt 5:

Die Kommunikation zwischen TI-CA und dem NovaTec System erfolgt zur Zeit manuell mittels des eigenen MMX-Protokolls. Hat der Kunde einen eigenen CA-Server, so kann im zweiten Schritt das Protokoll „SCEP“ („Simple Certificate Enrollment Protocol“) für einen automatischen verschlüsselten Datenaustausch sorgen (SCEP ist zurzeit nicht im Liferumfang).

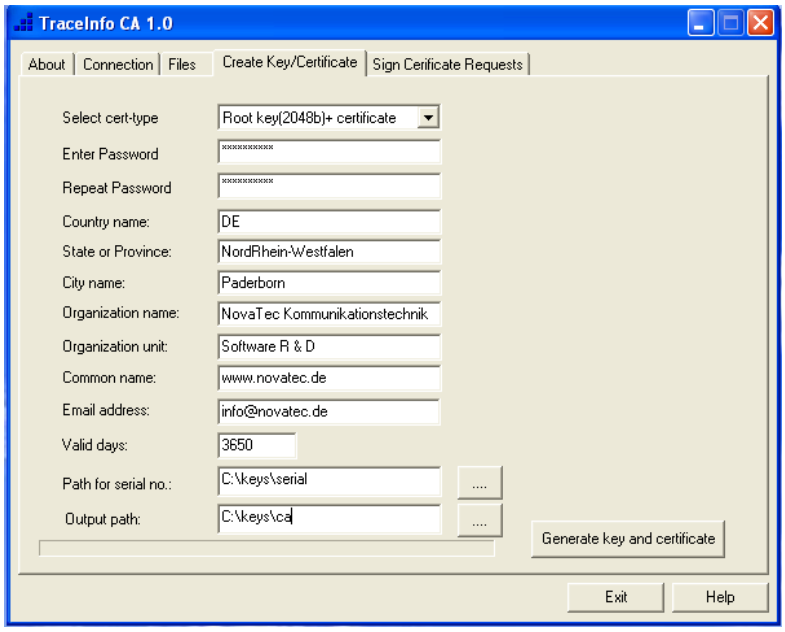
5 TLS

5.1 Erstellen einer Root-CA

DE_TICA_CREATECERT

Mit der Applikation TI-CA kann ein Anwender folgendes erzeugen:

CA privater Schlüssel und Root Zertifikat
Certificate-Request für Client oder Server

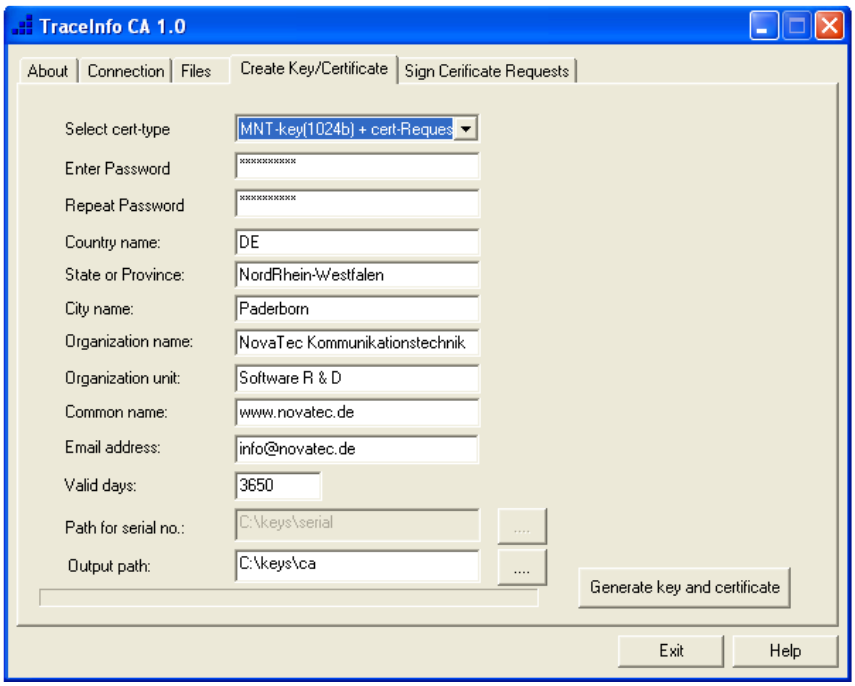


a) CA privater Schlüssel und Root Zertifikat erzeugen:

- Selektieren Sie den Reiter “Create Key/Certificate”.
- Eine Verbindung zum NovaTec Gerät ist nicht unbedingt erforderlich.
- Wählen Sie “Root key (2048b) + Certificate” in der Combobox aus.
- Geben Sie ein CA-Passwort ein. Das Passwort hat eine minimale Länge von vier Zeichen und eine maximale Länge von 20 Zeichen.
- Wiederholen Sie Ihr CA-Passwort. Bitte merken Sie sich das Passwort. Falls Sie mit diesem Root Zertifikat signieren möchten, brauchen Sie dieses Passwort dazu.
- Nächste Schritte sind die Eingaben von CA Identität wie Land, Provinz, Stadt, Organisation, Organisations-Einheit, Common-Name und Email Adresse. Für das Land sind stets zwei Zeichen einzugeben. Die restlichen Eingaben haben eine maximale Länge von 64 Zeichen.
- Geben Sie die Gültigkeit des Root Zertifikats in Anzahl Tage ein.
- Geben Sie einen Verzeichnis-Pfad ein, wo die Datei serial.txt sich befindet.(1)
- Geben Sie einen Verzeichnis-Pfad ein, wo die erzeugte CA privater Schlüssel und Root Zertifikat hingeschrieben werden sollen. Die erzeugten Dateien werden als cakey.pem and ca_cert.crt benannt.
- Wenn die Eingaben soweit sind, drücken Sie die Schaltfläche “Generate key and certificate”. Die Applikation braucht ein Paar Sekunden um den privaten Schlüssel zu erzeugen. Bitte bestätigen Sie die Meldungen mit der „OK“ Schaltfläche.

Note[1]:
Die Serialnummer eines Zertifikats wird in einer Datei serial.txt verwaltet. Wenn diese Datei nicht in dem gegebenen Pfad vorhanden ist, wird die Applikation sie erneut anlegen, dabei wird die Applikation eine Default Start-Serialnummer vergeben.
Wenn Sie die Serialnummer selbst bestimmen möchten, schreiben Sie einfach eine 16-stellige Hexadezimalzahl z. B. 0123456789ABCDEF in die Datei serial.txt. Nach Verbrauch, wird die Nummer in serial.txt inkrementiert.

b) Certificate-Request für Client oder Server erzeugen:

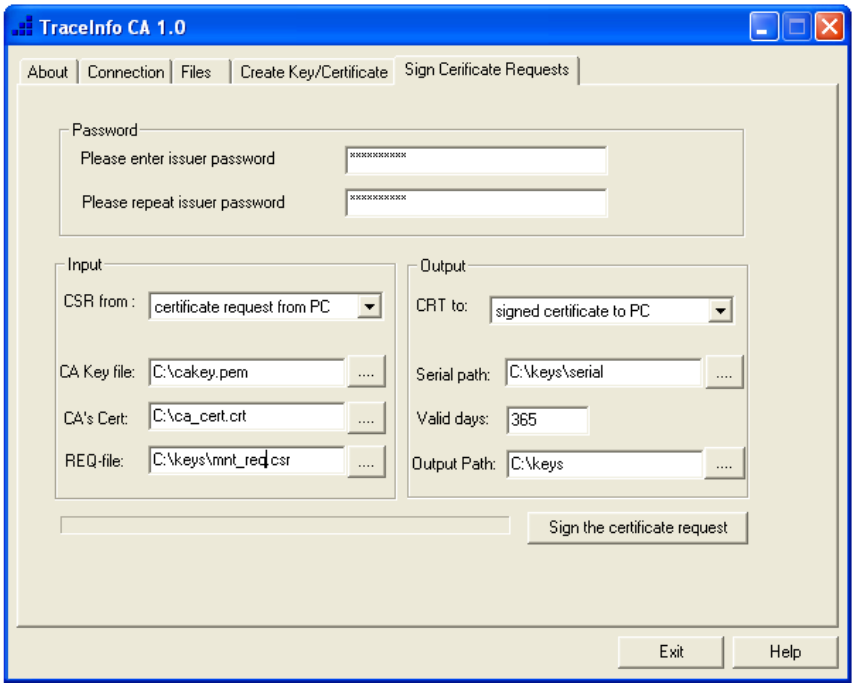


- Selektieren Sie den Reiter “Create Key/Certificate”.
- Eine Verbindung zum NovaTec Gerät ist nicht unbedingt erforderlich.
- Wählen Sie “MNT-key (1024b) + Cert-Request” oder “NMS-key (1024b) + Cert-Request” in der Combobox aus. MNT-Request brauchen Sie für Maintenance und NMS-Request brauchen Sie für den NMS-Server.
- Geben Sie ein Passwort ein. Das Passwort hat eine minimale Länge von vier Zeichen und eine maximale Länge von 20 Zeichen.
- Wiederholen Sie Ihr Passwort. Bitte merken Sie sich das Passwort. Sie brauchen dieses Passwort später um Verbindungen aufzubauen.
- Nächste Schritte sind die Eingaben von Subjects Identität wie Land, Provinz, Stadt, Organisation, Organisationseinheit, Common-Name und Email Adresse. Für das Land sind stets zwei Zeichen einzugeben. Die restlichen Eingaben haben eine maximale Länge von 64 Zeichen.
- Geben Sie die Gültigkeit des Requests in Anzahl Tage ein.
- Geben Sie einen Verzeichnis-Pfad ein, wo der erzeugte CA private Schlüssel und Request hingeschrieben werden sollen.
- Wenn die Eingaben soweit sind, drücken Sie die Schaltfläche “Generate key and certificate”. Die Applikation braucht ein Paar Sekunden um den privaten Schlüssel zu erzeugen. Bitte bestätigen Sie die Meldungen mit der „OK“ Schaltfläche.

DE_TICA_SIGNCERT

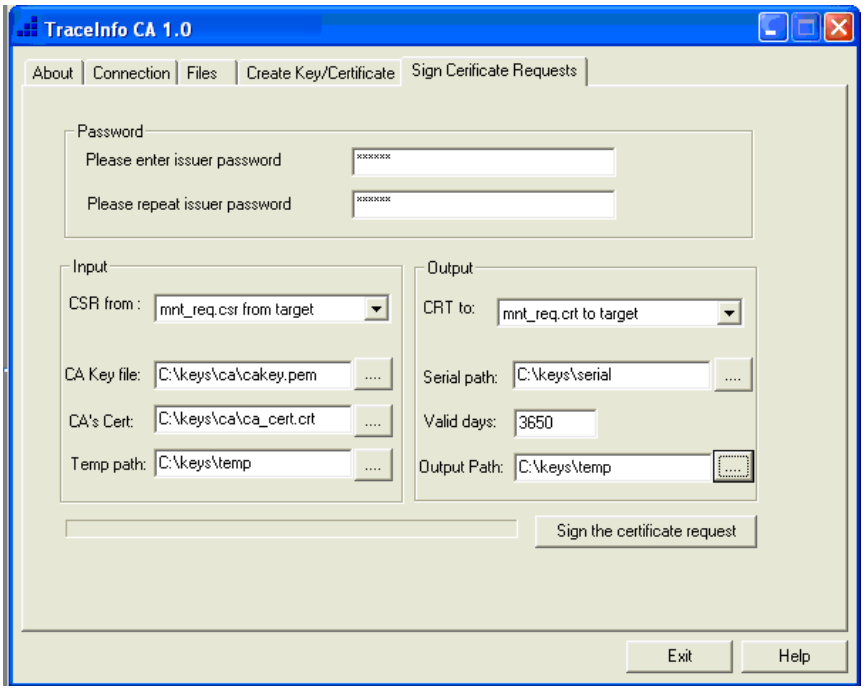
Mit der Applikation TI-CA können Sie einen Certificate-Request in ein Zertifikat signieren, wobei sich der Certificate-Request in einem PC oder in NovaTec Geräte befinden kann.

Fall 1)
Signieren eines Certificate-Request, wobei der Request sich in einem PC befindet. Die signierte Datei wird in einen PC-Pfad zurück geschrieben. Bei Bedarf, kann die signierte Datei in ein NovaTec Gerät zurück geschrieben werden.



- Selektieren Sie den Reiter the “Sign Certificate Requests”.
- Eine Verbindung zum NovaTec Gerät ist nur erforderlich, wenn Sie die signierte Datei in ein NovaTec Gerät zurück schreiben möchten.
- Geben Sie ein CA-Passwort ein. Das ist das passende Passwort zu dem CA privaten Schlüssel.
- Wiederholen Sie Ihr CA-Passwort.
- Geben Sie folgende Input-Eingaben ein:
    - Selektieren Sie “certificate request from PC” in der Combobox.
    - Geben Sie den CA privaten Schlüssel ein.
    - Geben Sie das CA Zertifikat ein.
    - Geben Sie den zu signierenden Certificate-Request ein.
- Geben Sie folgende Output-Eingaben ein:
    - Selektieren Sie “signed certificate to PC” in der Combobox.
    - Geben Sie einen Verzeichnis-Pfad ein, wo die Datei serial.txt sich befindet.(1)
    - Geben Sie die Gültigkeit des Zertifikats in Anzahl Tage ein.
    - Geben Sie einen Verzeichnis-Pfad ein, wo das signierte Zertifikat hingeschrieben werden soll.
- Wenn die Eingaben soweit sind, drücken Sie die Schaltfläche“Sign the certificate request”.

Fall 2)
Signieren eines Certificate-Requests, wobei der Request sich in einem NovaTec Gerät befindet. Die signierte Datei kann bei Bedarf, in ein NovaTec Gerät oder in PC zurück geschrieben werden.



- Selektieren Sie den Reiter “Sign Certificate Requests”.
- Eine Verbindung zum NovaTec Gerät ist erforderlich, wenn Sie die signierte Datei in ein NovaTec Gerät zurück schreiben möchten.
- Geben Sie ein CA-Passwort ein. Das ist das passende Passwort zu dem CA privaten Schlüssel.
- Wiederholen Sie Ihr CA-Passwort.
- Geben Sie folgende Input-Eingaben ein:
    - Selektieren Sie “certificate request from target” in der Combobox.
    - Geben Sie den CA privaten Schlüssel ein.
    - Geben Sie das CA Zertifikat ein.
    - Geben Sie einen temporären Pfad ein, wo der Certificate-Request zwischengespeichert wird.
- Geben Sie folgende Output-Eingaben ein:
    - Selektieren Sie “signed certificate to target” in der Combobox.
    - Geben Sie einen Verzeichnis-Pfad ein, wo die Datei serial.txt sich befindet.(1)
    - Geben Sie die Gültigkeit des Zertifikats in Anzahl Tage ein.
    - Geben Sie einen temporären Pfad ein, wo das signierte Zertifikat zwischengespeichert wird.
- Wenn die Eingaben soweit sind, drücken Sie die Schaltfläche “Sign Certificate Requests”.

Note (1):
Die Serialnummer eines Zertifikats wird in einer Datei serial.txt verwaltet. Wenn diese Datei nicht in dem gegebenen Pfad vorhanden ist, wird die Applikation sie erneut anlegen, dabei wird die Applikation eine Default Start-Serialnummer vergeben.
Wenn Sie die Serialnummer selbst bestimmen möchten, schreiben Sie einfach eine 16-stellige Hexadezimalzahl z.B. 0123456789ABCDEF in die Datei serial.txt. Nach Verbrauch, wird die Nummer in serial.txt inkrementiert.

5.2 NovaTec für TLS frei schalten

Der Kunde hat seine Lizenz-Datei erhalten und kann nun mit Hilfe von „NTConf“ sein(e) NovaTec-System(e) für TLS freischalten.

Dazu lädt er seine konventionelle Konfiguration in „NTConf“ und wählt innerhalb des Baumes im linken Teil-Fenster den Knoten „System-IP-Options“ aus.

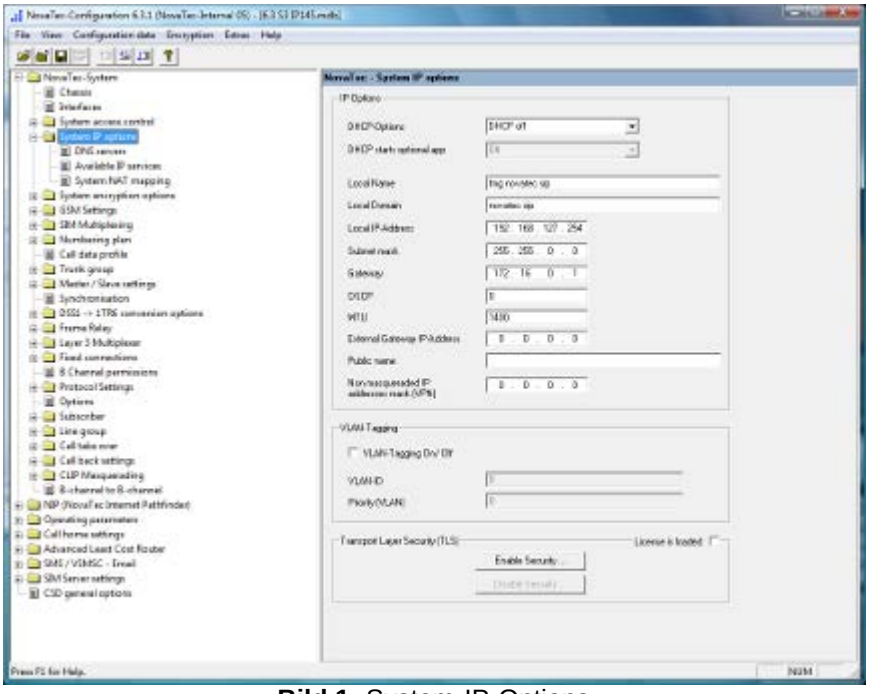


Bild 1: System-IP-Options

Danach betätigt der Kunde im rechten Teil-Fenster den Knopf „Enable Security…“.

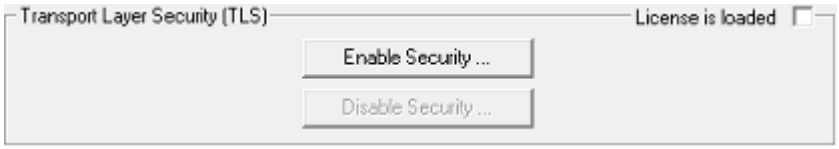


Bild 2: Aktivierung TLS

Es öffnet sich ein Dialog, der den Kunden auffordert, die von NovaTec erhaltene Lizenz im Datei-System zu lokalisieren.

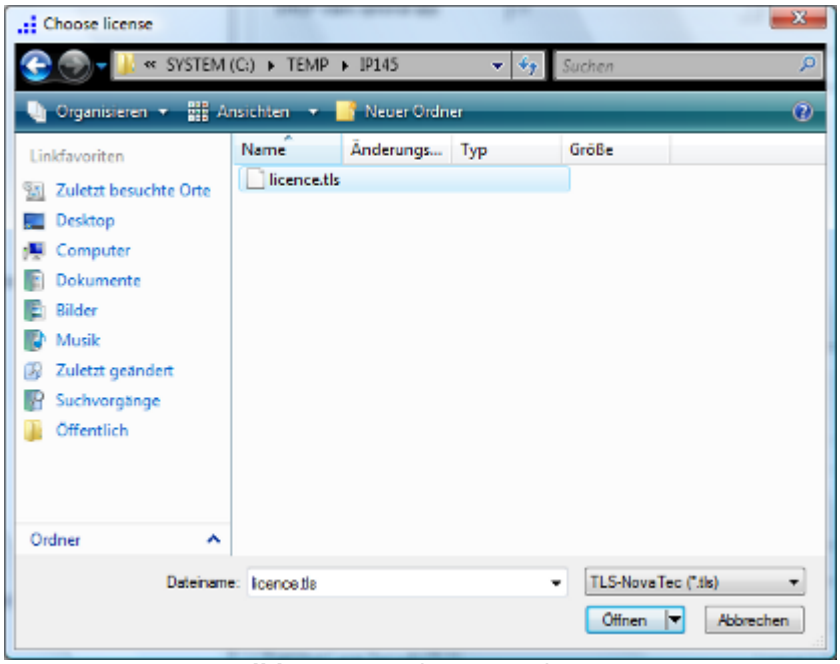


Bild 3: Import einer TLS-Lizenz

Nach erfolgreichem Import der Lizenz wird dies dem Benutzer im rechten Teilfenster durch ein aktiviertes Kästchen (CheckBox) „License is loaded“ angezeigt.

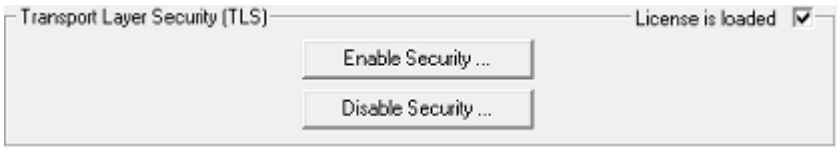


Bild 4: Erfolgreicher Import einer TLS-Lizenz

Ebenso öffnet sich nun innerhalb des Baumes im rechten Teilfenster ein spezieller Knoten „TLS-Security“.

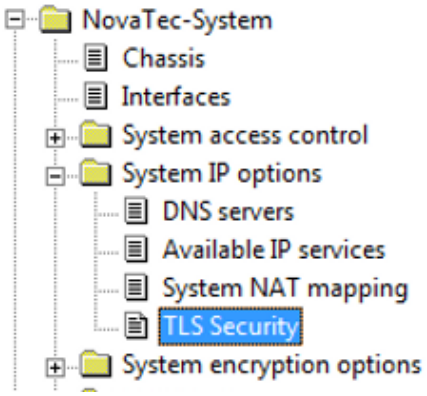


Bild 5: Knoten "TLS-Security"

Nach Auswahl dieses Knotens erscheint im rechten Teil-Fenster ein Fenster mit drei Reitern: Maintenance, SIP und CallHome.

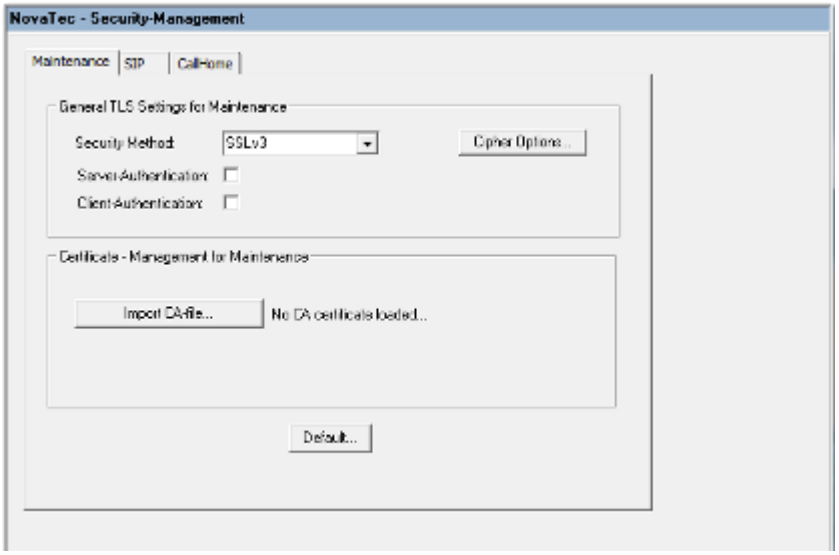


Bild 6: Security-Management

Soll ein CA-Zertifikat importiert werden, wird dies durch Drücken des Knopfes „Import CA-file…“ angestoßen. Es erscheint ein Datei-Öffnen-Dialog um das CA-Zertifikat im Dateisystem zu lokalisieren.

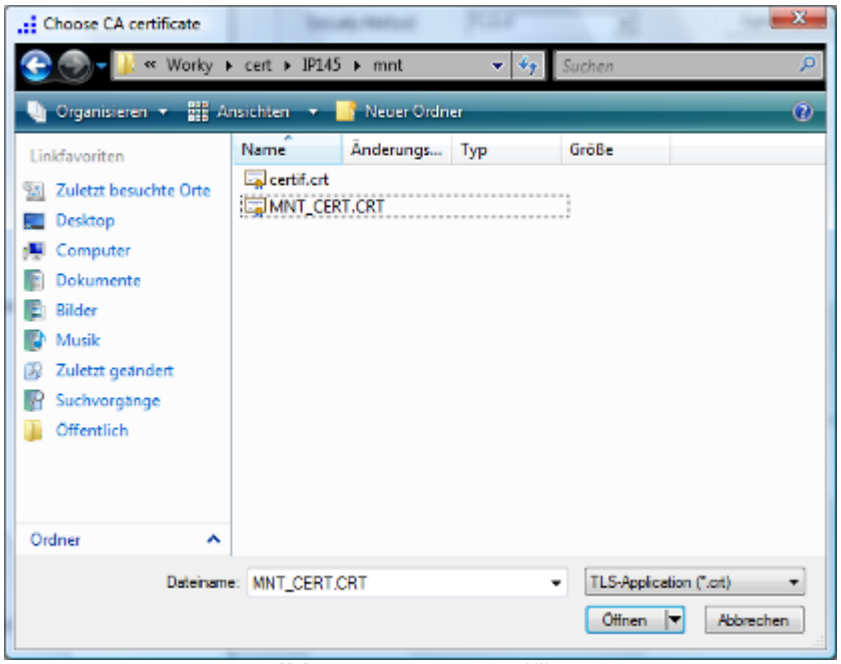


Bild 7: Import CA-Zertifikat

Der erfolgreiche Import des Zertifikats wird im rechten Teilfenster angezeigt.

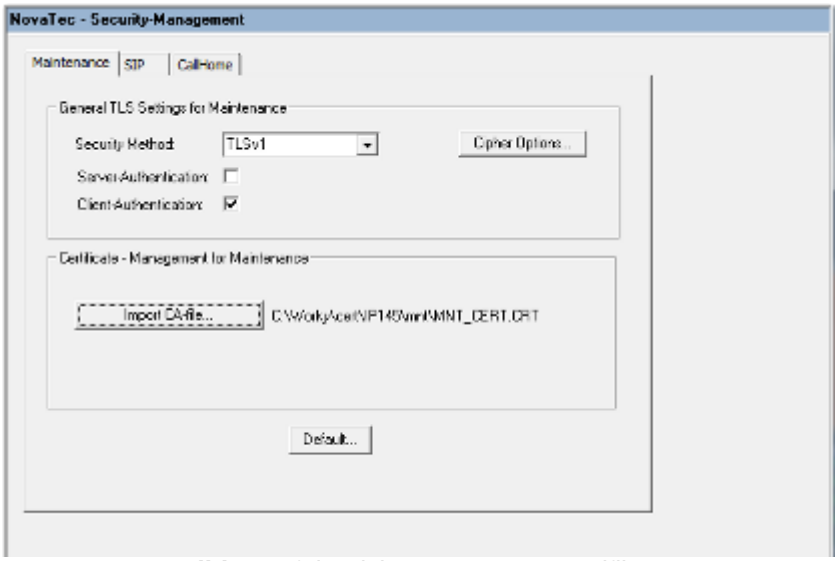


Bild 8: Erfolgreicher Import CA-Zertifikat

Soll z.B. die Verschlüsselung auf bestimmte Algorithmen beschränkt sein, also möchte man die Cipher-Listen definieren, wird dies durch Drücken des Knopfes „Cipher Options…“ angestoßen.

Es erscheint ein Dialog, der es dem Kunden erlaubt, von NovaTec vorgegebene Cipher weiter einzuschränken.

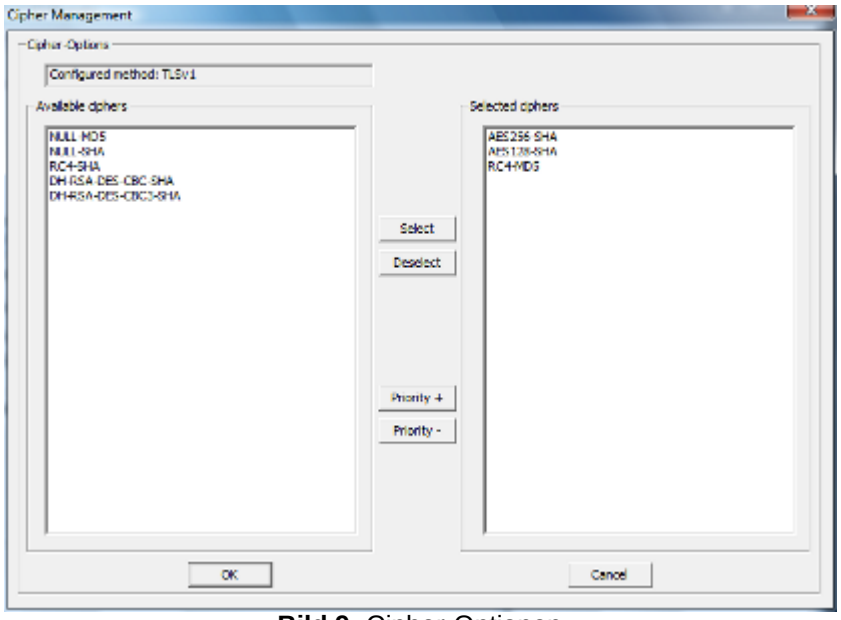


Bild 9: Cipher-Optionen

Im linken Teilfenster werden die vorgegebenen Cipher aufgeführt, im rechten Teilfenster die benutzerdefinierte Cipher-Liste.

Cipher aus dem linken Teilfenster werden entweder durch Doppel-Klick oder durch Drücken des Knopfes „Select“ in das rechte Teilfenster übernommen. Ebenso werden Cipher aus dem rechten Teilfenster durch

Doppel-Klick oder durch Drücken des Knopfes „Deselect“ wieder aus der benutzer-spezifischen Liste entfernt.

Die Priorität der Cipher spielt eine entscheidende Rolle – diese kann durch die Knöpfe „Priority+“ und „Priority-“ verändert werden.

Ist die TLS-Konfiguration erstellt, kann man diese mit Hilfe von „NTConf“ auf das Ziel-System überspielen.
Ist im Ziel-System TLS aktiviert, muss natürlich auch die Konfiguration im TLS-Mode überspielt werden.
Dazu wird der Menüpunkt „Network Options“ unterhalb „Extras“ ausgewählt.

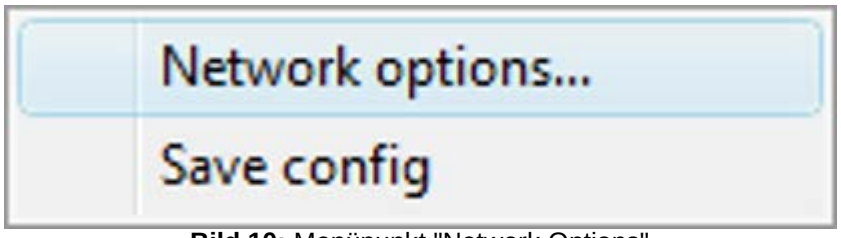


Bild 10: Menüpunkt "Network Options"

Nach Auswahl dieses Menüpunktes erscheint ein Dialog, der es erlaubt, Verbindungsparameter festzulegen.

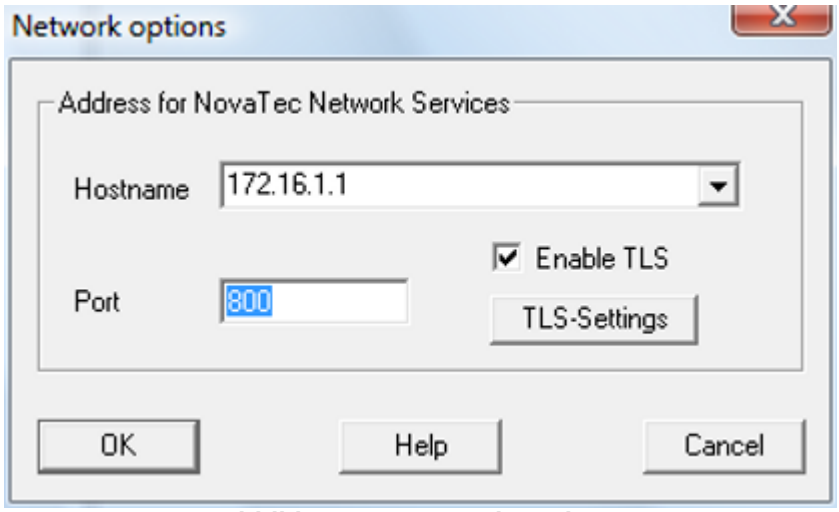


Abbildung 11: Network-Options

Durch Aktivierung des Häkchens „Enable TLS“ wird der darunterliegende Knopf „TLS-Settings“ eingeschaltet und betätigt.

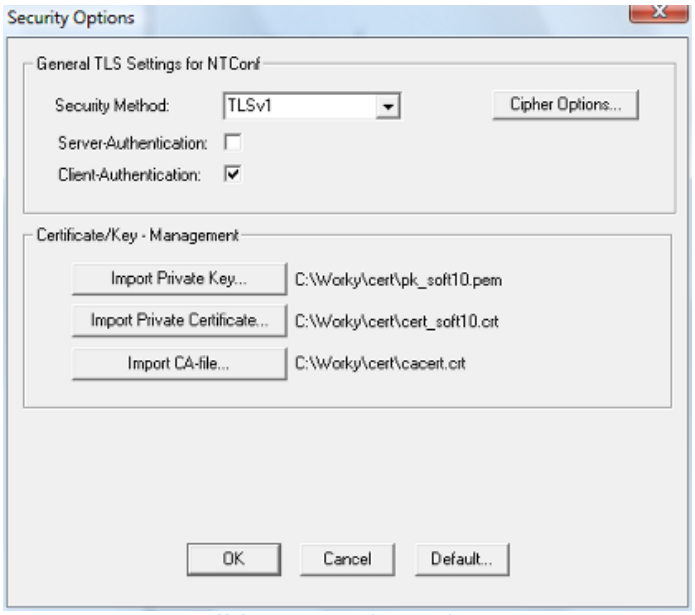


Bild 12: Security Options

Nach Auswahl der schon o. a. Optionen können zusätzlich zum Import eines CA-Zertifikats innerhalb dieses Dialogs der private Schlüssel und das private Zertifikat des Anwenders importiert werden.

Nun kann die Konfiguration zum Zielsystem übertragen werden. Während des Verbindungsaufbaus zum Zielsystem wird die Passphrase des privaten Schlüssels des Anwenders erfragt. Dies ist notwendig, damit der private Schlüssel geöffnet werden kann.

Bild 13: Eingabe "passphrase"

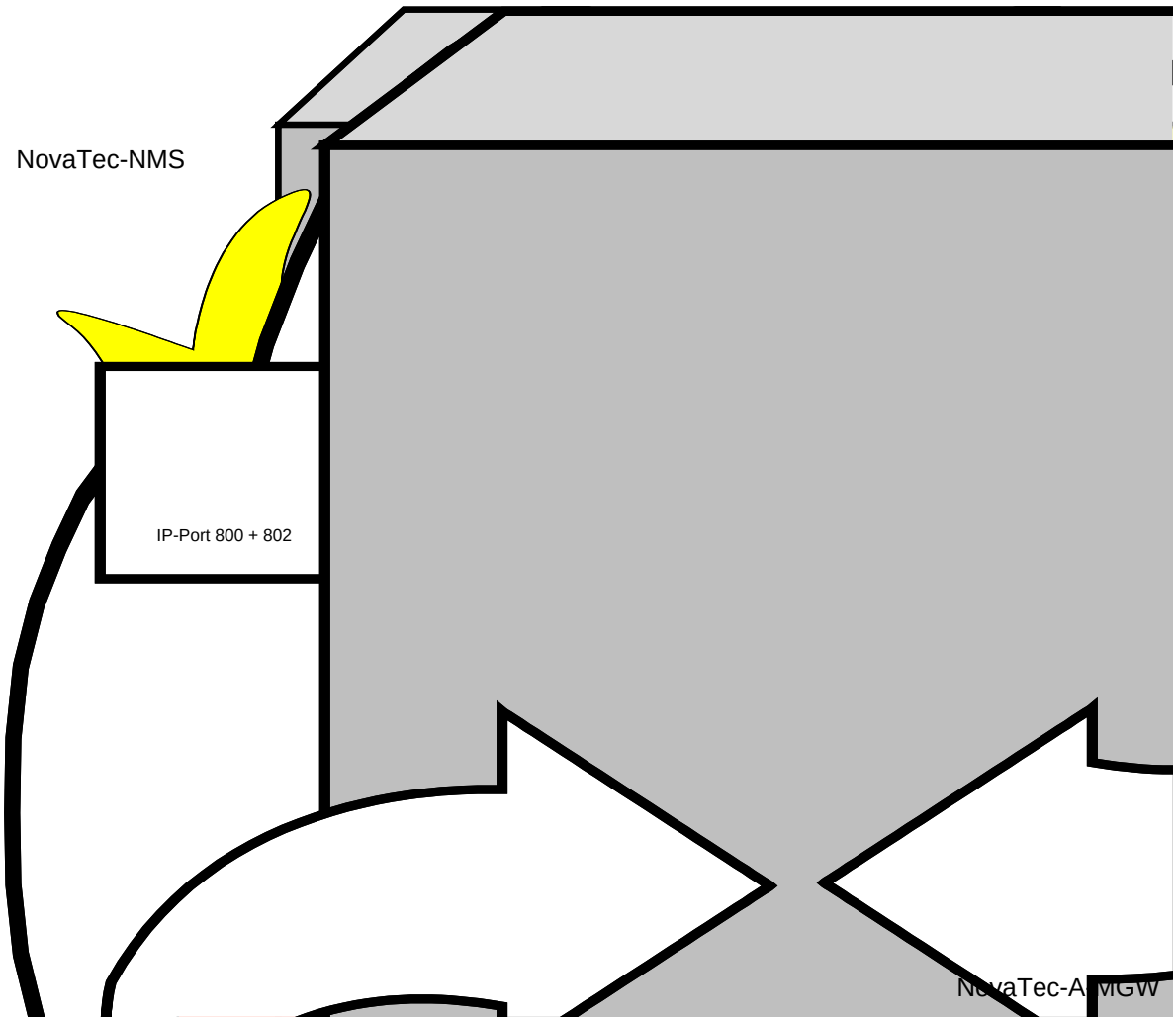
6 Das Network Management System

6.1 Installation des NMS

Auf einem Server, auf dem das NovaTec Network Management System läuft, müssen folgende Software-Pakete installiert werden damit das NMS funktioniert und der direkte Zugriff auf ein A-MGW möglich ist:

- **NovaTec Network Management System**
- **NovaTec Maintenance Package**

Der Server selbst muss natürlich im LAN eingebunden sein. Die IP-Ports 800 und 802 müssen in der Firewall frei geschaltet werden, um den Zugriff in beide Richtungen zu ermöglichen.



Folgende Systemvoraussetzungen sollte der Server minimal erfüllen, um einen schnelle Abarbeitung eines Zielsystems zu gewährleisten:

Windows XP
2 GB RAM
1 GHz CPU

6.2 Funktionsweise des NMS 6.x

Auf dem Server laufen folgenden Anwendungen:

Maintenance Package:
Hierdurch erfolgt der direkte Zugriff auf ein Zielsystem. Das Paket beinhaltet die notwendigen Applikationen um manuell auf ein A-MGW zugreifen zu können, um z. B. die CDRs auszulesen, die Firmware zu aktualisieren, Traces und Logbücher auszulesen oder den Status abzufragen.

Job Management:
Die Job Management Applikation ist Teil des NovaTec-NMS-Pakets und steuert, welche Zielsysteme auf das NMS zugreifen dürfen bzw. welche Zielsysteme das NMS akzeptiert und welche Aufgaben (Jobs)

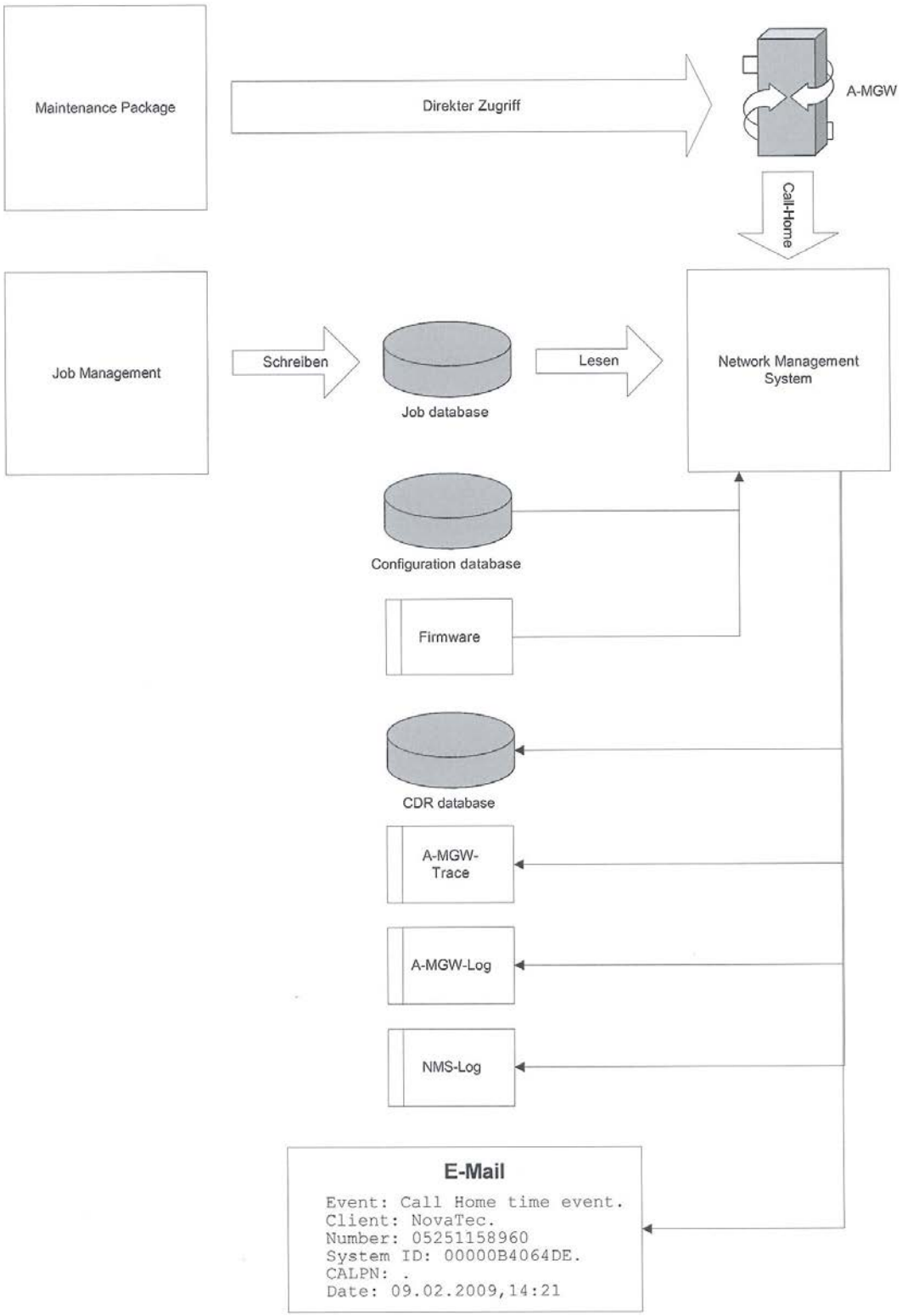
durchzuführen sind, wenn sich ein Zielsystem meldet. Alle Jobs können spezifisch pro Zielsystem gesteuert werden.

Network Management System:
Das Network Management System ist die Applikation, welche die kommenden Verbindungen vom Zielsystem/A-MGW entgegennimmt und die notwendigen Aufgaben (Jobs) entsprechend der Vorgaben des Job Management durchführt. Zum Betrieb des NMS muss also auf jeden Fall eine Job Database existieren. Soll das NMS eine Aktualisierung der Konfiguration oder Firmware eines Zielsystems durchführen so muss die entsprechende Konfiguration (configuration database) und Firmware für das NMS hinterlegt sein. Die Daten können lokal auf dem Server liegen oder auf einem Fileserver. Natürlich muss das NMS die notwendigen Zugriffsrechte auf diese Daten haben. Um die Gesprächsdaten speichern zu können, wird eine existierende (am Anfang leere) CDR Database benötigt. Traces und Logbücher des Zielsystems/A-MGW und die Logdatei des NMS selbst werden neu erstellt und nicht in einer Datenbank gespeichert.

Das NMS hat keinen direkten Zugriff auf die Zielsysteme sondern wartet darauf, dass sich diese per Call-Home melden. Ein Zielsystem führt einen Call-Home durch, wenn ein entsprechendes Ereignis auftritt und Call-Home für dieses Ereignis konfiguriert ist. Das Zielsystem kann auf Wunsch so konfiguriert werden, dass in Abhängigkeit vom Ereignis jeweils ein anderer Server gerufen wird.

Das NMS verschickt auf Wunsch eine E-Mail, um über das aufgetretene Ereignis zu informieren. Hierbei werden die Zielsysteme zu Kunden zugeordnet. Für jeden Kunden kann eine E-Mail-Adresse konfiguriert werden.

Das folgende Bild zeigt schematisch wie der Zugriff auf den A-MGW erfolgt und welche Daten vom NMS verarbeitet bzw. erzeugt werden können:


Maintenance Package
Direkter Zugriff
A-MGW
Call-Home
Job Management
Schreiben
Job database
Lesen
Network Management System
Configuration database
Firmware
CDR database
A-MGW-Trace
A-MGW-Log
NMS-Log
E-Mail
Event: Call Home time event.
Client: NovaTec.
Number: 05251158960
System ID: 00000B4064DE.
CALPN: .
Date: 09.02.2009,14:21

Folgende Ereignisse werden zurzeit unterstützt:

- **Budget Limit reached**
  Das konfigurierte Budget-Limit wurde erreicht.
- **Call data filled**
  Der CDR-Speicher im Zielsystem ist voll (bzw. halbvoll).
- **Client Callback failure**
  Bei der Durchführung eines Callbacks ist ein Fehler auf der Client-Seite aufgetreten.
- **Server Callback failure**
  Bei der Durchführung eines Callbacks ist ein Fehler auf der Server-Seite aufgetreten.
- **EWU Board removed from System**
  Ein EWU-Einschub wurde aus dem Zielsystem entfernt.
- **SIM removed from SCU**
  Aus einem SCU-Einschub wurde eine SIM entfernt.
- **Falls short of ASR limit**
  Die konfigurierte ASR-Schwelle wurde unterschritten.
- **GSM ASR event**
  Die konfigurierte ASR-Schwelle für das GSM-Netz wurde unterschritten.
- **ISDN ASR event**
  Die konfigurierte ASR-Schwelle für das ISDN wurde unterschritten.
- **SIP ASR event**
  Die konfigurierte ASR-Schwelle für das SIP-Netz wurde unterschritten.
- **Layer 1 or Layer 2 inactive**
  An einer Punkt-zu-Punkt-Schnittstelle ist die Schicht-1 oder Schicht-2-Verbdindung .zusammengebrochen.
- **Log filled**
  Das Logbuch ist voll.
- **Trace filled**
  Der Speicher für Tracedateien ist voll.
- **Ping timeout to TIME server**
  Die Verbindung zum TIME Server ist unterbrochen.
- **SOS client unreachable**
  Die Verbindung zum SOS Client ist unterbrochen.
- **SOS SIM error**
  Beim Zugriff auf eine SIM ist ein Fehler aufgetreten.
- **Systemstart default**
  Das Zielsystem hat einen Reset durchgeführt und läuft in der Defaultkonfiguration.
- **Systemstart normal**
  Das Zielsystem hat einen Reset durchgeführt und läuft mit der zuletzt aufgespielten Konfiguration.
- **Time event**
  Das Zielsystem meldet sich nach einem konfigurierbaren Zeitraum. Es ist kein besonderes Ereignis aufgetreten.
- **TIP Running errors**
  Im TIP-Betrieb ist ein Fehler aufgetreten.
- **TIP Startup errors**
  Beim Starten der TIP-Schnittstellen ist ein Fehler aufgetreten.
- **Trace warning**
  Im Zielsystem wurde eine Warning erzeugt.
- **Trace error**
  Im Zielsystem ist ein Fehler aufgetreten.

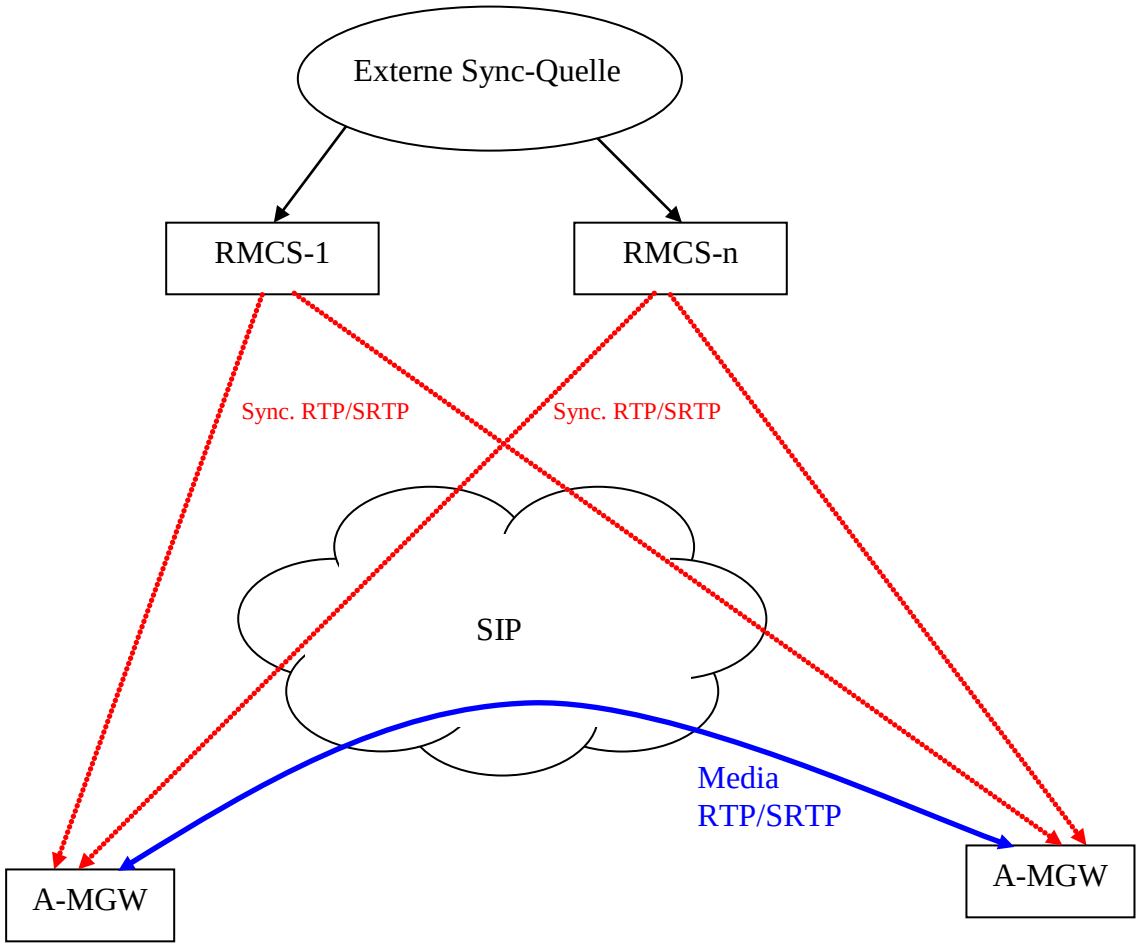
Die **grau** dargestellten Ereignisse sind für die geplanten Einsatzbereiche des A-MGW nicht relevant. Sie wurden nur der Vollständigkeit halber gelistet und um zu zeigen, dass die unterschiedlichsten Ereignisse realisiert werden können.

7 NovaTec Sync. Admin

Der NovaTec Sync. Admin besteht aus mehreren NovaTec Hardware- und Software- Komponenten, die in einem “Konzert” gemeinsam für eine Taktsynchronisation aller NovaTec-Komponenten in einem TDM-, IP- oder gemischten Netz Sorge tragen.
Die Bestandteile sind im Einzelnen:

1- Der RTP Master Clock Source (RMCS)
2- Die Sync. Manager Tasks in den jeweiligen A-MGWs
3- Das Konfigurations-Tool

Bei der Synchronisation über ein RMCS wird vor dem Aufbau des eigentlichen SIP-Rufes eine SIP-Verbindung zu einem RMCS-Server aufgebaut. Die Synchronisation erfolgt dann anhand des RTP-Stroms welcher vom RMCS-Server empfangen wird. Ein RMCS-Server hat immer eine externe Taktquelle (PRI/BRI oder GPS). Als Alternative kann auch ein System mit hochgenauem 1-Herz-Quartz eingesetzt werden.



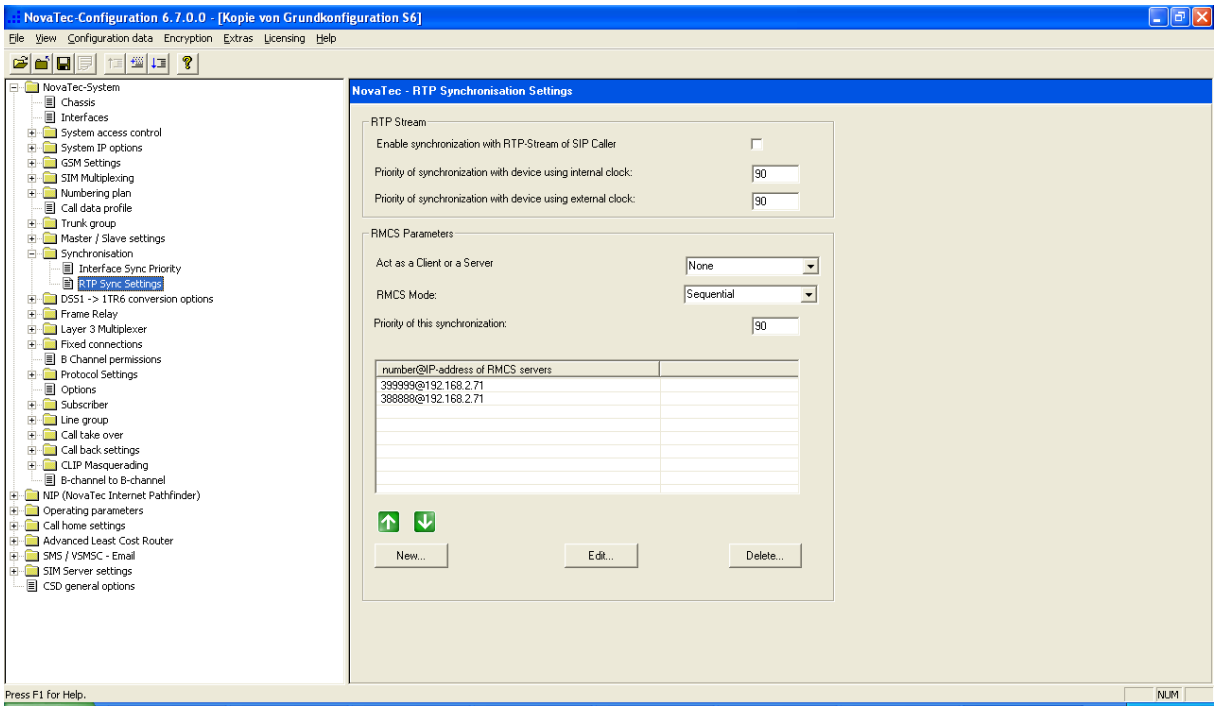
Folgende Regeln werden umgesetzt:

- Ein RMCS-Ruf wird nur für Datenverbindungen aufgebaut.
- Falls ein RMCS-Server nicht erreicht werden kann, dann wird versucht den nächsten konfigurierten RMCS-Server zu erreichen.
- Wird während eines SIP-Rufes der RMCS-Ruf getrennt, so wird sofort der nächste RMCS-Server gerufen.
- Wenn kein Kanal für den RMCS-Ruf frei ist, dann wird der Datencall abgelehnt.
- Wenn kein RMCS-Server erreicht werden kann, dann wird der Datencall abgelehnt.
- Für den RMCS-Ruf werden beliebige, freie BCU-SIP-Kanäle belegt. Alternativ ist es auch möglich auf dem A-MGW einen Kanal für den RMCS-Server zu reservieren um sicherzustellen, dass immer ein Kanal für die Synchronisationsverbindung frei ist.
- Die Auswahl eines RMCS ist mit den Methoden sequentiell oder Round-Robin per Konfiguration möglich.

7.1 Konfiguration des RMCS-Clients

Bei Anbindung der Systeme über einen Soft-Switch wie Cisco CUCM, sind auf der Client-Seite zusätzliche Einstellungen wie folgt vorzunehmen:

7.1.1 RTP Sync. Settings



Folgende Einstellungen sind vorzunehmen:

Feld „Act as a Client or a Server“:
Gibt an ob das System als Client oder Server läuft. Logischerweise muss hier „Client“ ausgewählt werden.

Feld „RMCS Mode“:
Gibt an ob die RMCS-Server vom Client mit der Methode Sequentiell oder Round-Robin ausgewählt werden. Beide Einstellungen sind möglich. Bei Sequentiell wird immer der 1. Server in der Liste gerufen und nur der nächste Server belegt, wenn der RMCS-Ruf zum 1. Server nicht aufgebaut werden kann. Bei Round-Robin wird immer der nächste Server ausgewählt. Ist das Ende der Liste erreicht wird wieder beim 1. Server angefangen.

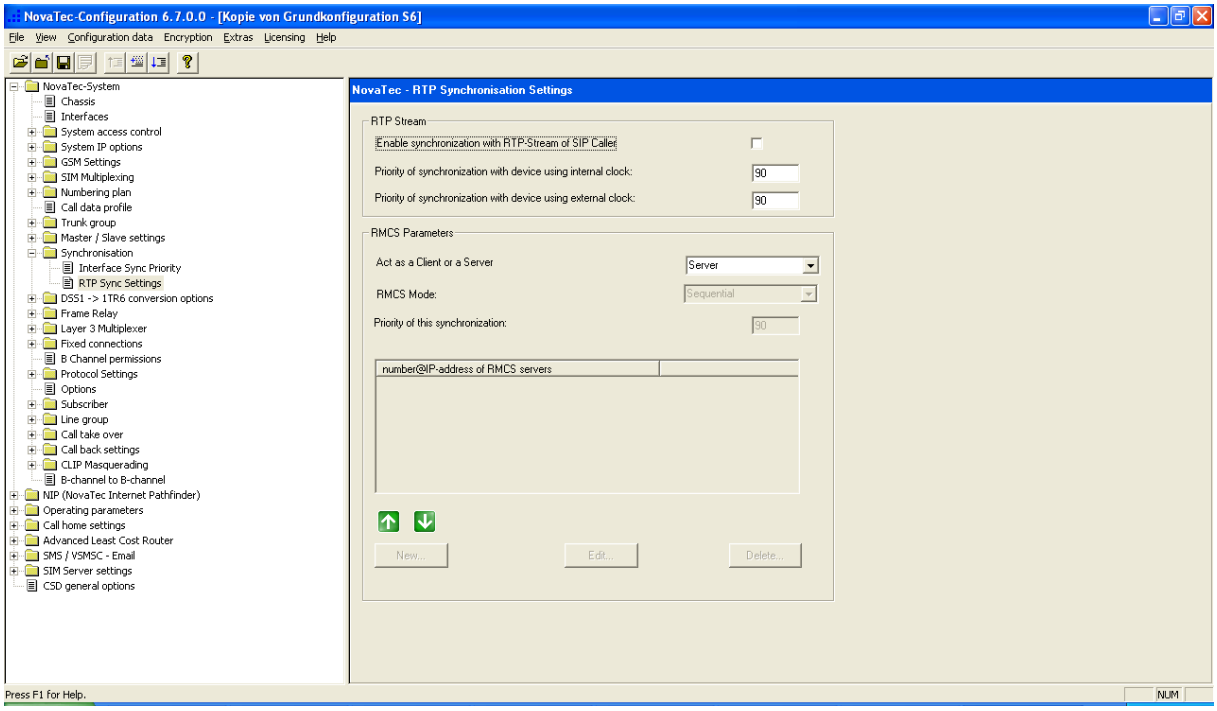
Feld „Priority of this synchronization“:
Gibt an welche Synchronisationspriorität der RTP-Strom vom RMCS-Server auf dem Client bekommt. Der eingetragene Wert wird auch unter „Interface Sync Priority“ zusammen mit allen anderen Prioritäten angezeigt.

Liste „number@IP-address of RMCS servers“:
Hier werden alle RMCS-Server eingetragen auf die der Client zugreifen soll. Entscheidend ist hierbei nur die Nummer. Die IP-Adresse ist an dieser Stelle nur informativ. Im SIP-User-Mapping wird die Nummer in eine SIP-Adresse umgesetzt. Wenn der CUCM aber sowieso als SIP-Gegenstelle für alle Rufnummern eingetragen ist braucht an den SIP-User-Mappings nichts geändert zu werden.

7.2 Konfiguration des RMCS-Servers

Auf der Server-Seite sind die Einstellungen an den folgenden Stellen vorzunehmen:

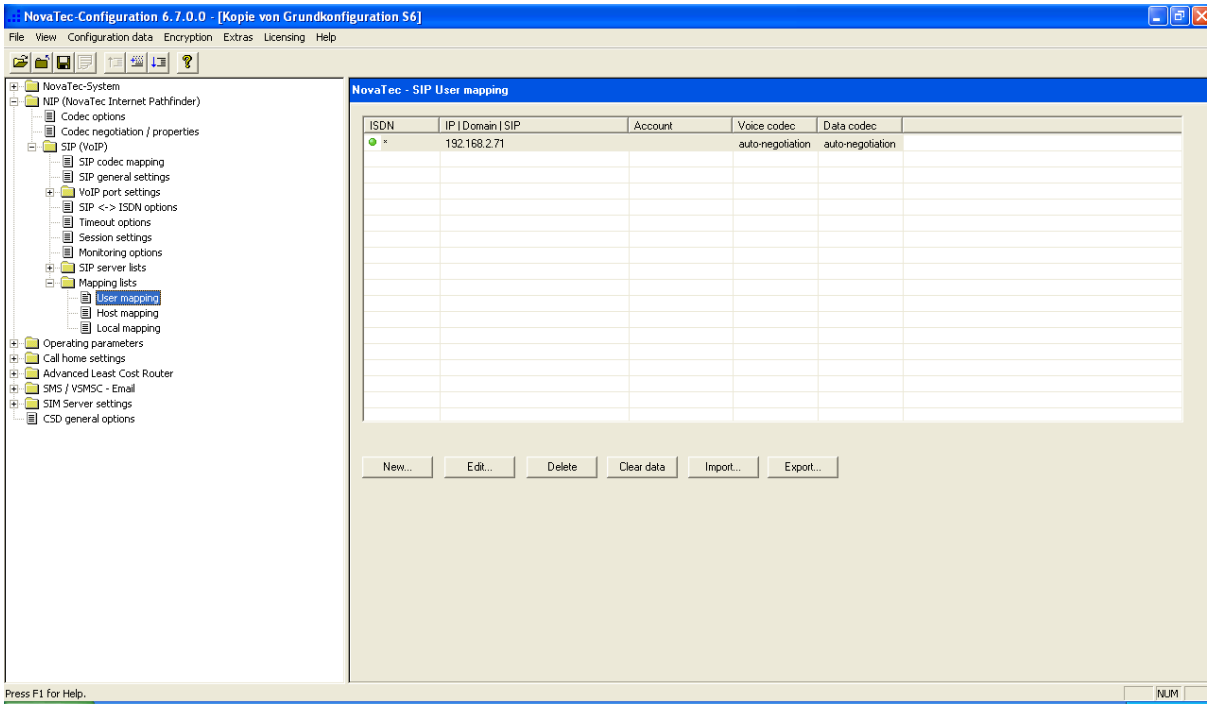
7.2.1 RTP_Sync_Settings



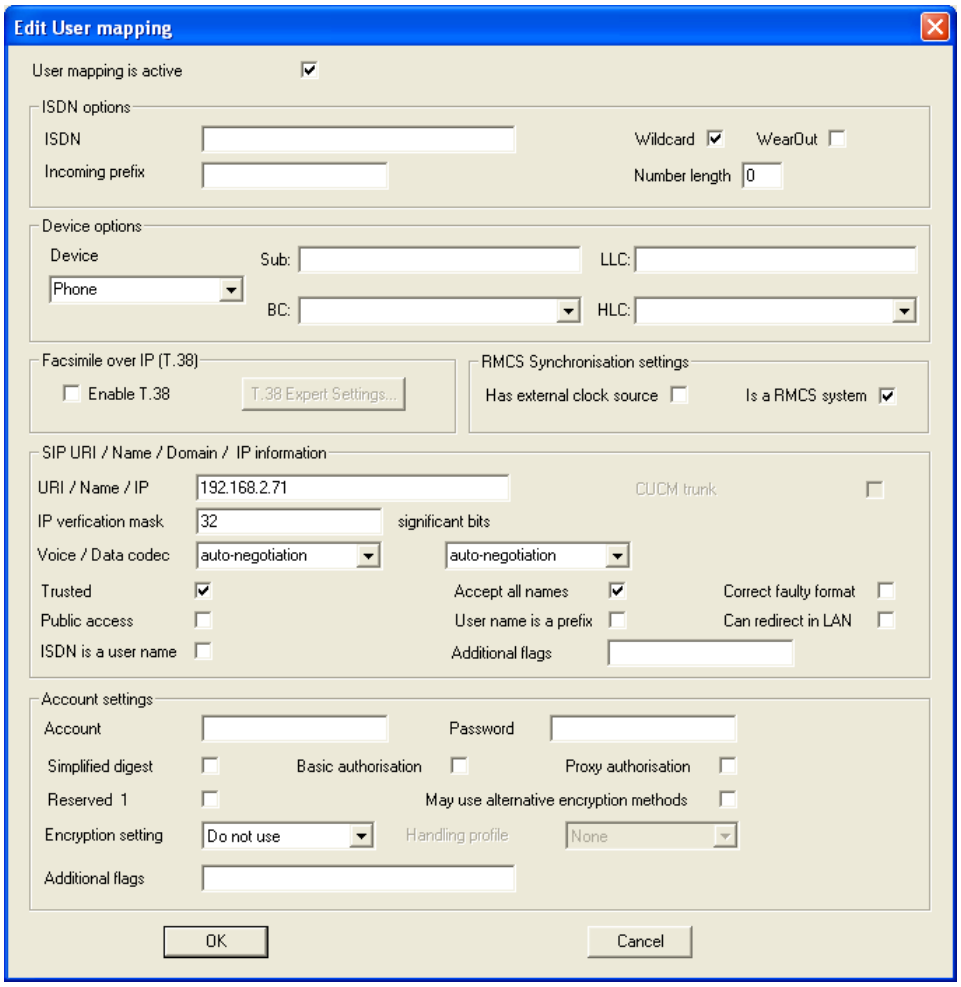
Feld „Act as a Client or a Server“:
Hier ist Server auszuwählen.

Alle anderen Felder sind für den Server nicht relevant.

7.3 User Mapping



Alle RMCS-Server-Systeme müssen einen Eintrag unter „User Mappings“ bekommen. Der nächste Screenshot zeigt, welche Einstellungen vorzunehmen sind:



Hier ist wichtig, dass das Flag „Is a RMCS system“ gesetzt ist, damit der RMCS-Server den Ruf als Synchronisationsruf annimmt. Ansonsten sind alle Einstellungen wie bei normalen User-Mapping Einträgen vorzunehmen. Im Feld „ISDN“ kann eine beliebige ISDN-Nummer eingetragen werden, da der RMCS-Server nur angerufen wird und nicht selber Synchronisationsrufe aufbaut.

Der RMCS Server wird wie jedes NovaTec-System über einen SIP-Trunk am CUCM angebunden.

Bei Anwendung von TLS sind die entsprechenden Einstellungen wie sonst auch in den NovaTec Systemen vorzunehmen.