NovaTec Kommunikationstechnik GmbH

Bedienungsanleitung

Installations-/Konfigurations-Handbuch TLS und sRTP

für NovaTec Systeme

Doc-ID	DB.HBTLSSRTP-.NT
Version	3.5
Datum	07.05.2014
Status	Final

INHALT

1 Einleitung- Was kann mit NovaTec Systemen gesichert werden?

NovaTec Gateways stellen gesicherte Kommunikationskanäle für alle drei Instanzen (Maintenance, SIP, CallHome) zur Verfügung. Der Verbindungsaufbau via SIP wird mit TLS gesichert. Die VoIP Kanäle für die Sprach- oder Datenübertragung werden mit sRTP verschlüsselt. Mit TLS können zusätzlich die Verbindungen für die Konfiguration und Wartung der Gateways gesichert werden.

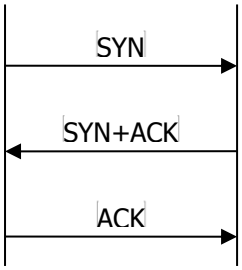
Die Systeme verwenden SSL-Zertifikate nach dem X.509 Standard, um die Authentizität und Integrität der Kommunikationspartner zu prüfen. Diese Zertifikate können mit dem NovaTec Zertifizierungstool TI-CA, dem NovaTec Administration and Management Element Server (NAMES) oder durch Drittanbieter erstellt bzw. signiert werden. Auch per SCEP können Zertifikate signiert werden.

Wichtig: Nach der Aktivierung von TLS ist der ungeschützte Zugang zu den Geräten blockiert. Jeder Zugangsversuch über V24/USB, ISDN und IP wie z.B. HTTP und TELNET wird abgewiesen.

2 Übersicht - Zertifikate handhaben

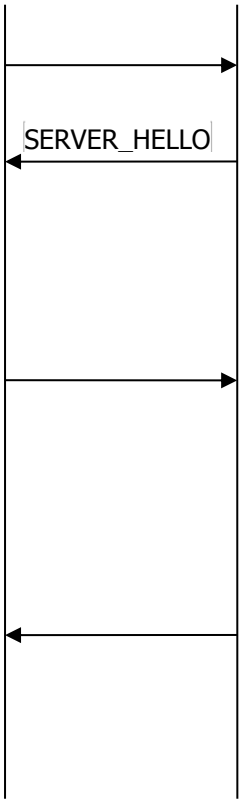
Die in diesem Handbuch beschriebenen Werkzeuge und Arbeitsschritte dienen dazu verschlüsselte Verbindungen zwischen zwei Partnern herzustellen. Neben der gesicherten Sprach- bzw. Datenkommunikation über eine IP-Verbindung mit sRTP wird im Folgenden meist Bezug genommen auf die Sicherung von Kommunikationskanälen mit TLS. Dieses Protokoll führt den notwendigen Schlüsselaustausch durch sowie die optionale Authentifizierung der beiden Kommunikationspartner mit Hilfe von Zertifikaten. Authentifizierung = Identifizierung des Gegenübers durch sein Zertifikat.

Für die SIP-Verbindung zwischen zwei Gateways oder zum Beispiel für die Verbindung des NAME-Servers zu einem Gateway wird zuerst eine TCP Verbindung aufgebaut.



Über diesen TCP Kanal wird anschließend das TSL Handshake-Protokoll ausgeführt.

Hier wird speziell der Austausch der Zertifikate betrachtet.



Der Client sendet ein CLIENT_HELLO zum Server.

Dieser antwortet mit einem SERVER_HELLO, darin enthalten ist u.a.:
Certificate – Der Server sendet immer sein Zertifikat.
***Certificate Request** – Optionale Aufforderung: CLIENT sende dein Zertifikat, damit der Server es prüfen kann.

Der Client antwortet.
***Certificate** – Der Client sendet sein angefordertes Zertifikat.
Client Key Exchange
***Certificate Verify** – Optional wird das Server-Zertifikat geprüft.
Change Cipher Spec
Encrypted Handshake Message

Der Server beendet das Protokoll erfolgreich. Die Verbindung ist jetzt mit den ausgetauschten Schlüsseln gesichert. Client und Server haben sich authentifiziert.
Change Cipher Spec
Encrypted Handshake Message

Mit einem * sind oben im Diagramm optionale Protokollschritte gekennzeichnet. Diese sind konfigurationsabhängig.

Die Konfigurationseinstellungen in Bezug auf die Rolle im TLS-Verbindungsaufbau		
Konfigurationspunkte der Gateways	**TLS-CLIENT**	**TLS-SERVER**
Maintenance		Client -Authentication
CallHome	Server -Authentication	
SIP	Server-Authentication	Client-Authentication

Konfigurationspunkte auf der PC-Seite	**TLS-CLIENT**	**TLS-SERVER**
Maintenance	Server-Authentication	
CallHome		Client-Authentication

Der Initiator einer TLS-Verbindung, der CLIENT, kann das SERVER-Zertifikat prüfen, das dieser an den CLIENT sendet. Diese Prüfung wird, z.B. für SIP, mit dem Konfigurationspunkt „Server-Authentication" aktiviert. Für SIP ist dieser Punkt unter → „System IP options" → „TLS Security" → Reiter „SIP" zu finden (siehe Abbildung 1 - Server- / Client-Authentication). Ist hier der Punkt „Client-Authentication" gesetzt, fordert der SERVER das CLIENT-Zertifikat zur Begutachtung an. Im Gegensatz zu den Instanzen „Maintenance" und „CallHome" besetzt der Gateway im SIP Modus beide Rollen. Wird ein mit TLS gesicherter Ruf von einem Gateway aufgebaut, ist dieser der CLIENT. Erreicht ein SIP-Ruf ein Gateway, ist dieser der TLS-SERVER. Für eine Maintenance-Verbindung ist ein Gateway immer der SERVER, da die Gegenstelle, beispielsweise NAMES oder TI-CA, den Aufbau der TLS-Verbindung beginnen. Dagegen ist der Gateway, sobald dieser einen CallHome-Ruf aufbaut, in der Rolle des TLS-CLIENTs. Entsprechend kann für die Instanz „CallHome" nur die „Server-Authentication" aktiviert werden.

Konfiguration der drei Instanzen

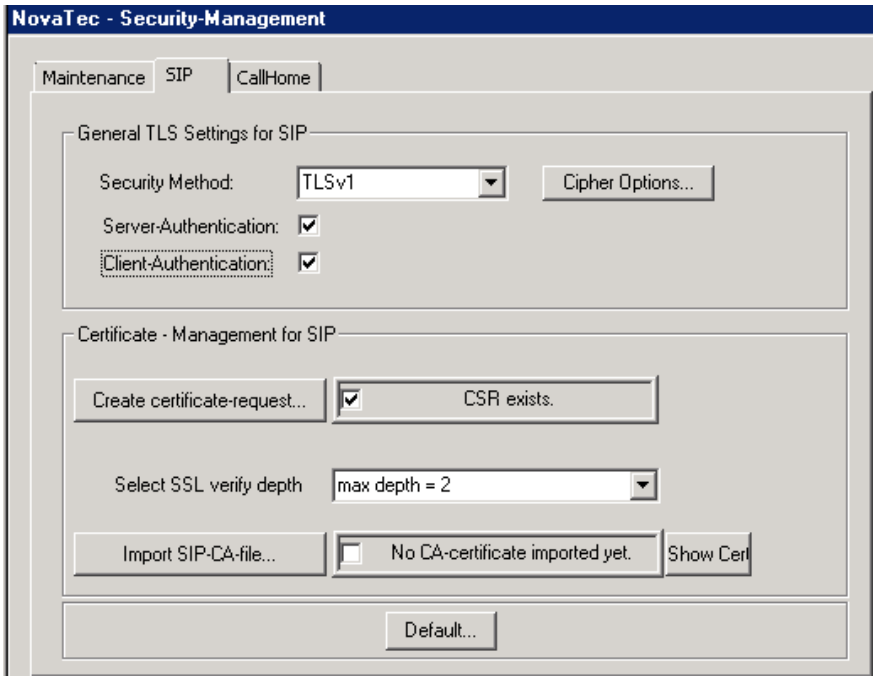


Abbildung 1 - Server- / Client-Authentication

2.1 TLS-Verbindungsaufbau in der Übersicht

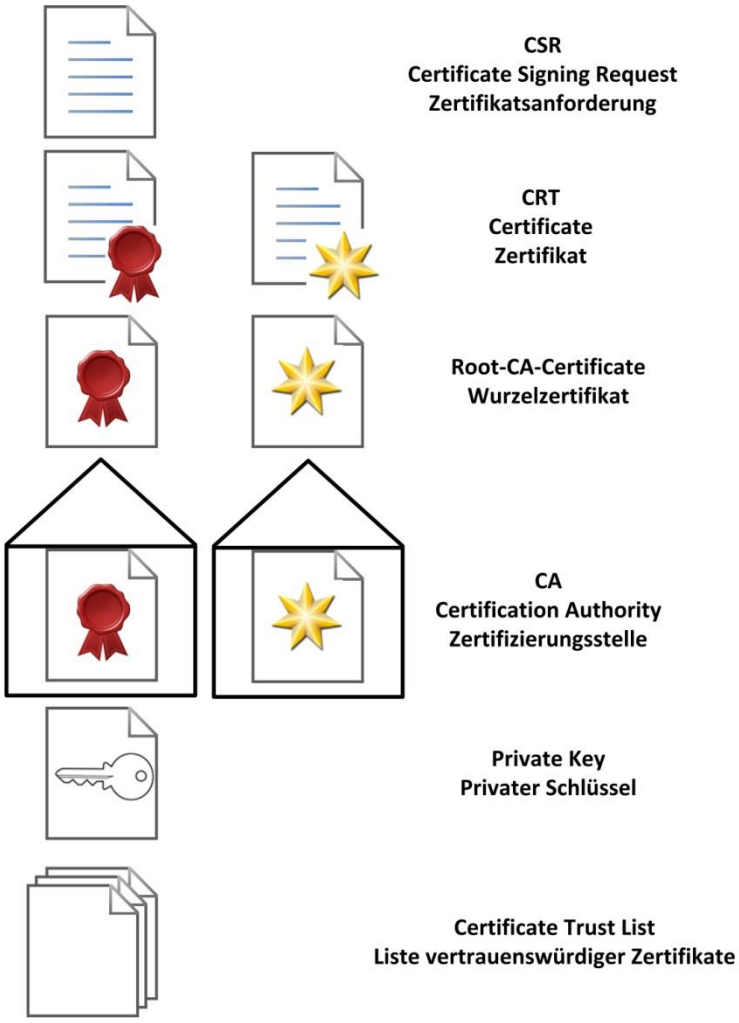


Abbildung 2- Legende für Übersichtsdiagramme

2.2 TLS-Zertifikat im Gateway anlegen

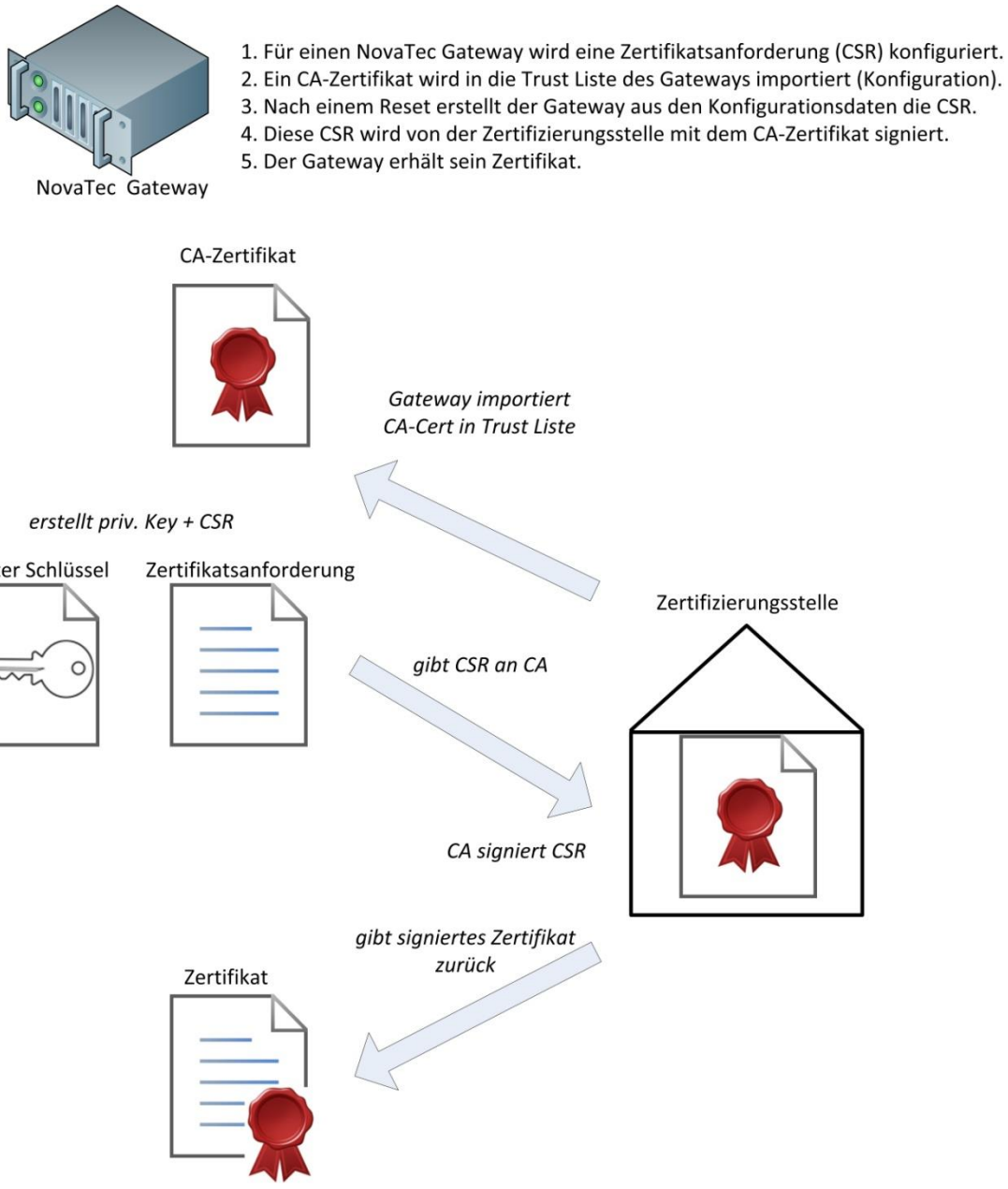


Abbildung 3 - TLS-Zertifikat eines Gateways wird erzeugt

2.3 TLS-Verbindungsaufbau und eine Zertifizierungsstelle

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.

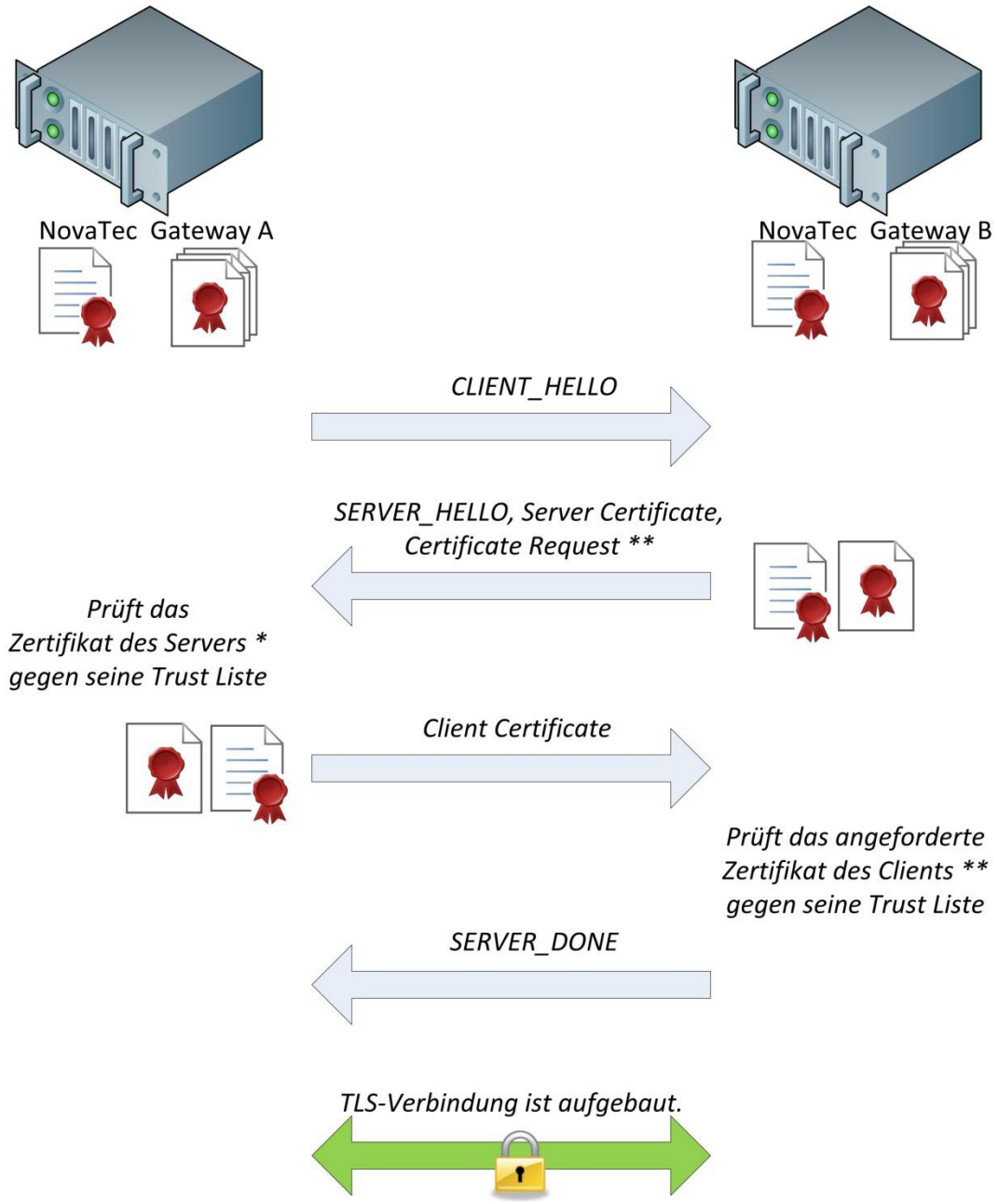


Abbildung 4 - TLS-Verbindungsaufbau - eine CA

2.4 TLS-Verbindungsaufbau und zwei Zertifizierungsstellen

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.

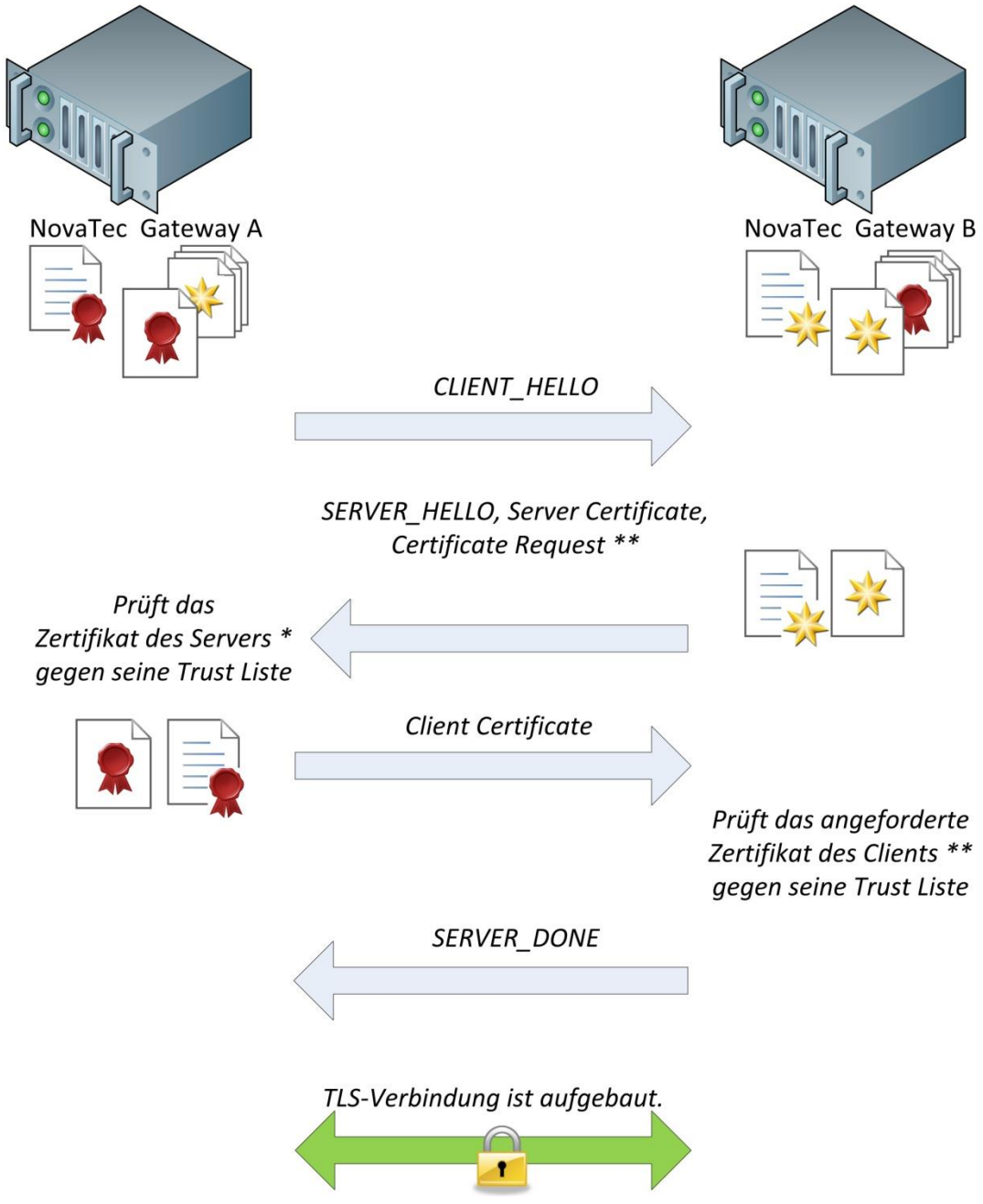


Abbildung 5 - TLS Verbindungsaufbau - zwei CAs

3 Vorbereitende Maßnahmen

3.1 Freischalten der Verschlüsselung in NovaTec Systemen

3.1.1 Bis NMP-Version 00.07.03.00

Bis zur NovaTec NMP-Version 00.07.03.00 ist neben der FW-Lizenz die separate TLS-Lizenz „tls.lic" erforderlich, wenn für das System TLS/sRTP freigeschaltet werden soll.

Fragen Sie NovaTec nach der TLS-Lizenz. Nachdem Sie diese "tls.lic" Datei von NovaTec erhalten haben, öffnen Sie bitte die Konfiguration Ihres Systems mit NovaTec-Configuration (ab Version 7.2.0.4) und laden Sie die TLS-Lizenz hoch.

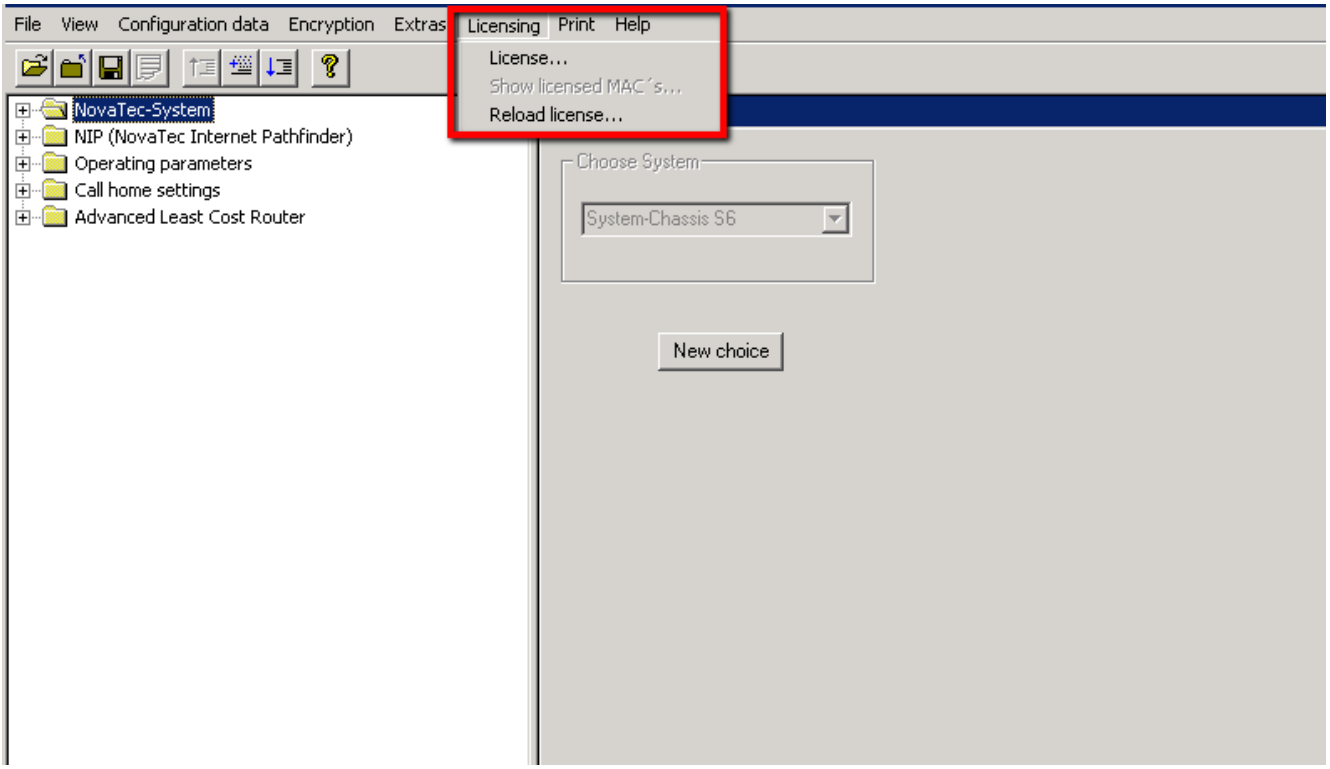


Abbildung 6 - FW-Lizenz laden

Wählen Sie danach im Konfigurationsprogramm "System IP options" aus.

Unten rechts wählen Sie nun „Enable Security" und geben den Pfad zu der gesicherten "tls.lic"-Datei an. Bestätigen Sie die angezeigten Fenster.

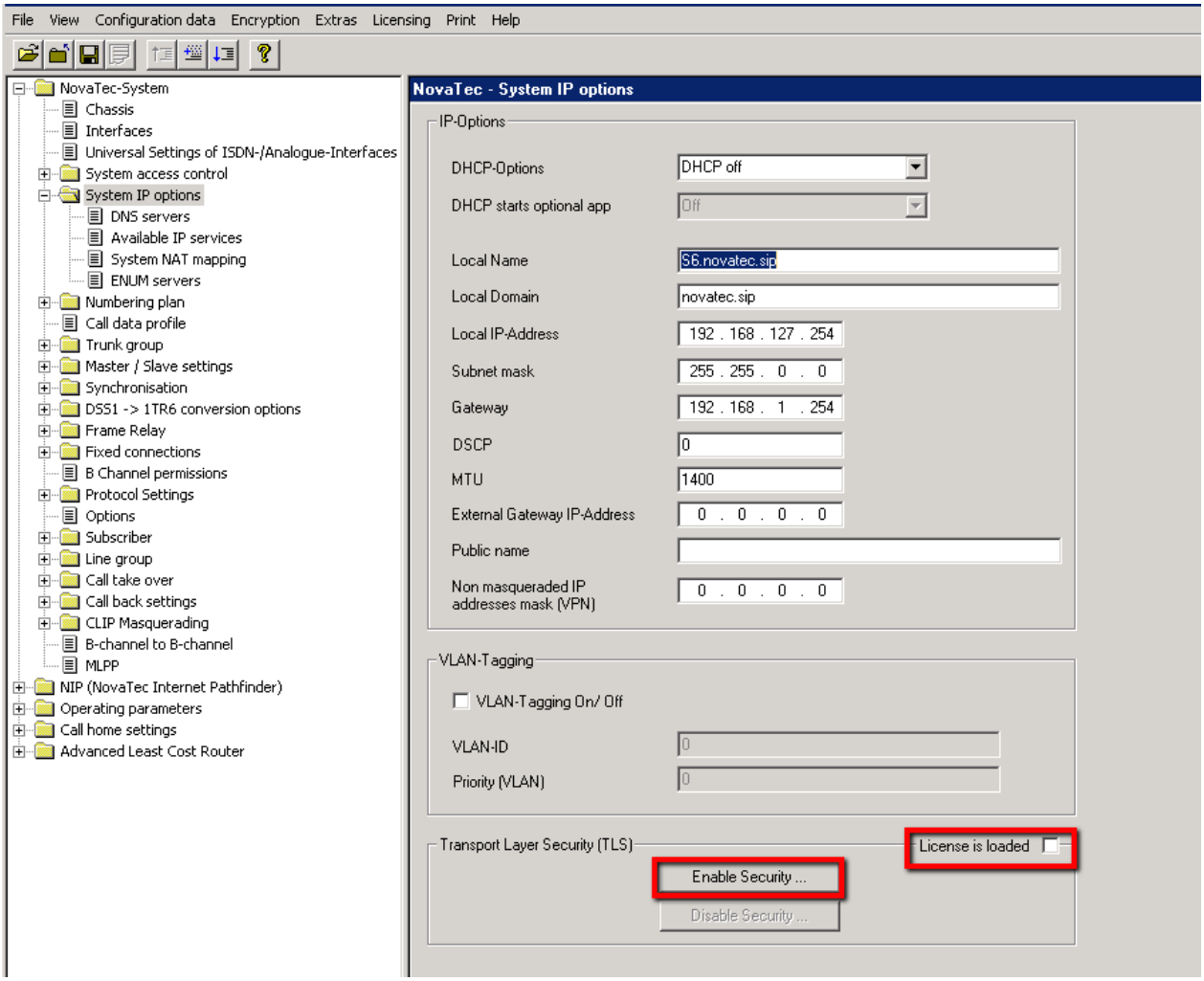


Abbildung 7 - TLS Lizenz ist geladen

3.1.2 Ab NMP-Version 00.07.03.00

Mit Version 00.07.03.00 ist ein neues Lizenzmanagement zur Absicherung der Firmware eingeführt worden. Sie erhalten auf Wunsch die FW-Lizenz mit der integrierten Option „TLS-Erlaubt". Laden Sie bitte die Lizenz erneut hoch (siehe vorhergehendes Kapitel 3.1.1).

Wählen Sie danach im Konfigurationsprogramm "System IP options" aus.

Unten rechts wählen Sie nun „Enable Security".

Wenn im Kästchen „Licence is loaded" ein Haken gesetzt ist, sind TLS und sRTP freigeschaltet.

Im Auswahlmenü in der linken Fensterhälfte wird nun der neue Punkt "TLS Security" unter dem Ordner "System IP options" angezeigt und der Ordner „sRTP encryption options" angelegt.

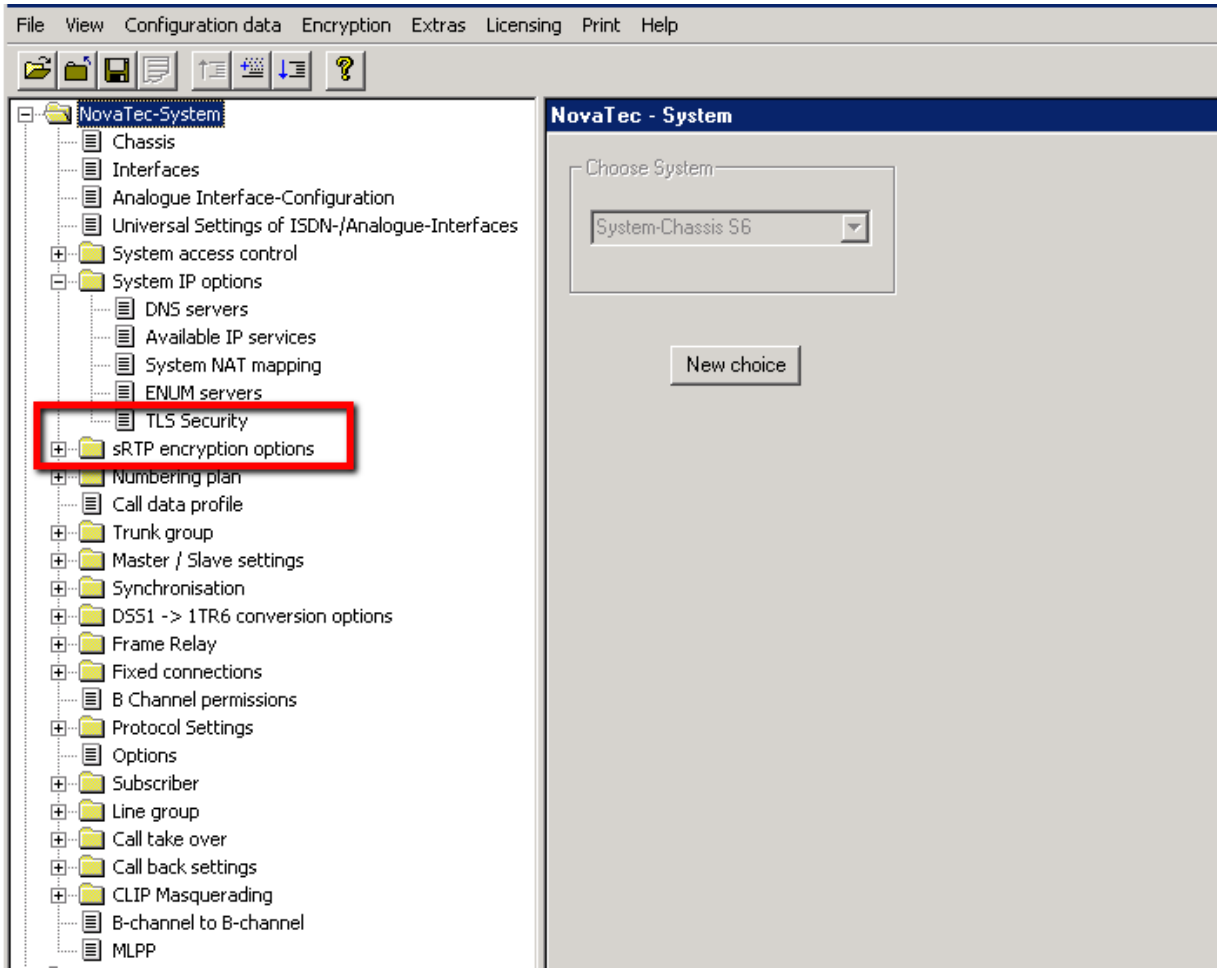


Abbildung 8 - TLS Security ist lizensiert

Hinweis: Nachdem die TLS-Lizenz geladen wurde, und falls SIP konfiguriert ist, werden einige Einstellungen automatisch vorgenommen. In der Vergangenheit mussten diese manuell ausgeführt werden. Bitte überprüfen Sie folgende Einstellungen (siehe auch Kapitel 4.2.4 ff):

1. „System IP options" → „Available IP services": Ein TCP/IP Service für SIP via TLS mit Port 5061 wird eingerichtet. Die Dienste HTTP und TELNET können jetzt aus Sicherheitsgründen nicht mehr aktiviert werden.

2. „NIP" → „SIP" → „Mapping lists" → „User mapping": Der Port 5061 wird der Nutzer-IP-Adresse hinzugefügt.

3. „NIP" → „SIP" → „Mapping lists" → „Local mapping": Der Port 5061 wird der registrierten IP-Adresse hinzugefügt.

3.2 Die TraceInfo-CA

Die NovaTec PC-Applikation „TraceInfo CA" ist eine Zertifizierungsstelle (Certification Authority, kurz: CA). Mit dieser CA lassen sich Zertifikate erstellen und signieren.

Um dieses Programm zu starten, benötigen Sie zwingend einen NovaTec Dongle. Alternativ kann NovaTec die Zertifikate online erstellen und signieren.

Bitte stellen Sie sicher, dass nur ein Dongle (z.B. NMS, TI-CA) am lokalen USB-Port angeschlossen ist.

Die TI-CA benötigt auf allen Betriebssystemen den vollen Zugriff auf die Datei „ticalic.enc". Hier ein Beispiel für die Konfiguration auf einem Windows 2008 Server.

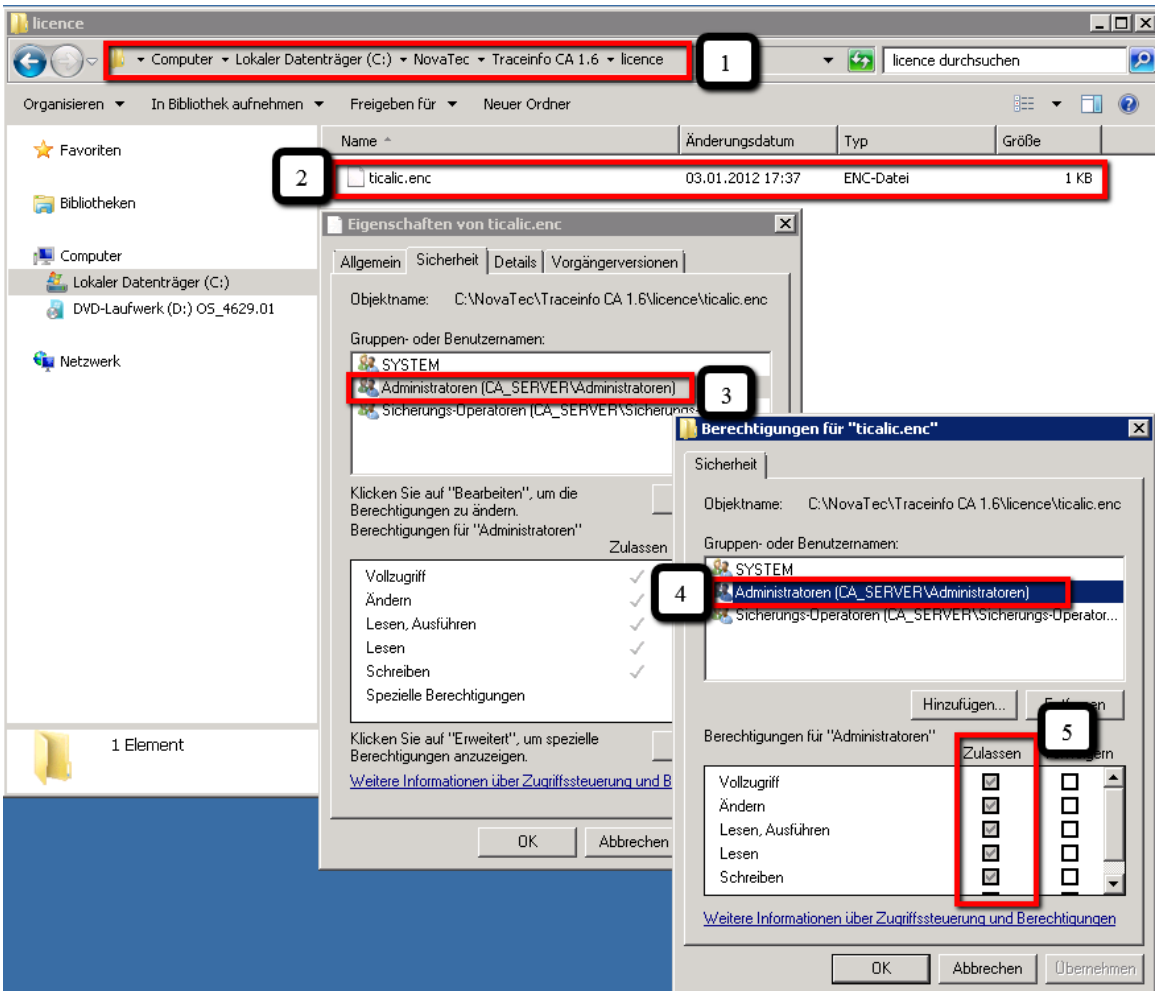


Abbildung 9 - TI-CA Berechtigungen konfigurieren

3.2.1 Die grundlegenden Fähigkeiten der TraceInfo-CA

3.2.1.1 CSR anlegen

Erstellen einer Zertifizierungsanforderung (CSR) inklusiv des mit einem Passwort geschützten privaten Schlüssels:

1) Selbstsigniertes ROOT-CA-Certifikate plus CSR und 2048 bit Key
2) Maintenance-CSR mit 1024 oder 2048 bit Key
3) CallHome-CSR mit 1024 oder 2048 bit Key

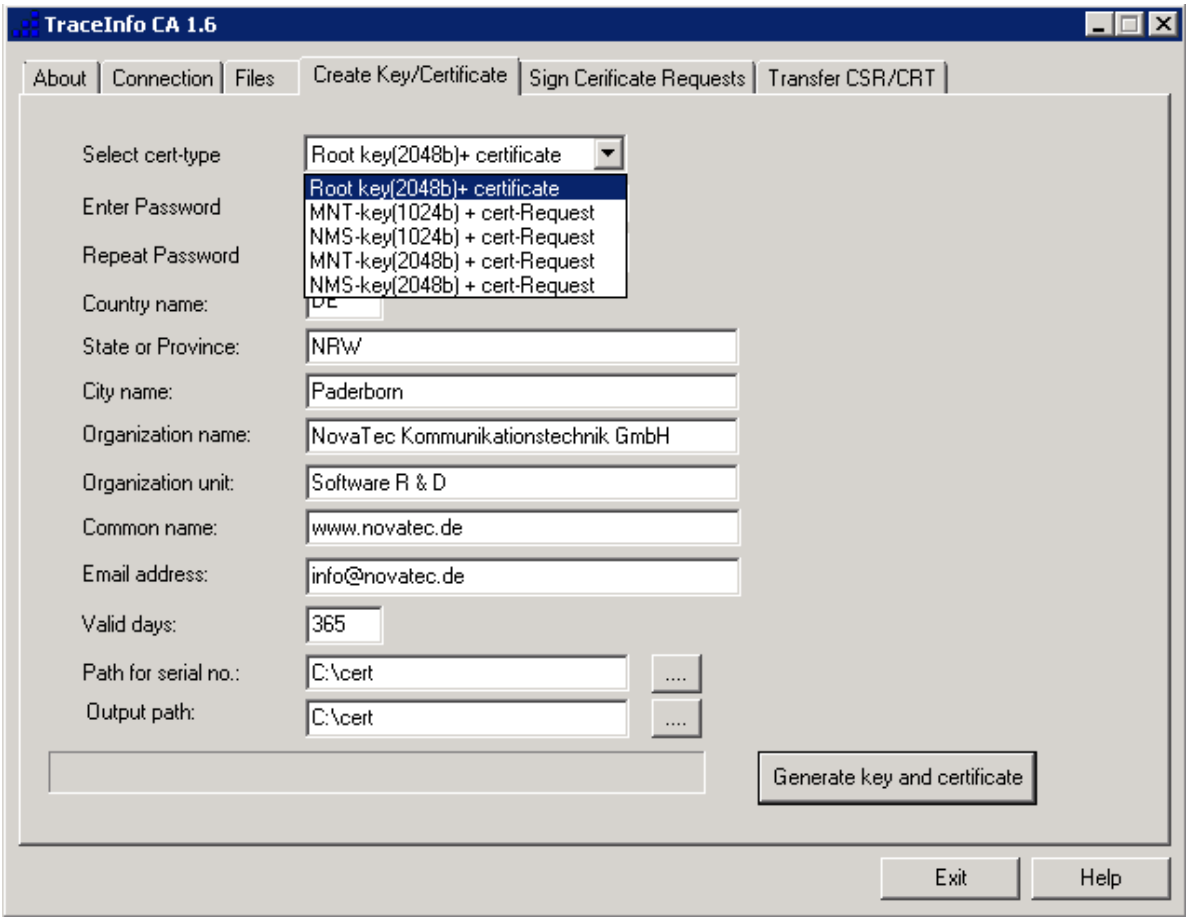


Abbildung 10 - CSR anlegen

3.2.1.2 CSR selbst signieren

Diese CSR, aber auch die durch eine fremde CA erstellte CSR, können von der TI-CA signiert werden. Der Speicherort der CSR und der daraus erstellten Zertifikate kann wie folgt sein:

1) Beliebiger CSR lokal auf PC → Zertifikat lokal auf PC
2) SIP-CSR im Gateway → SIP-Zertifikat im Gateway
3) Maintenance-CSR im Gateway → Maintenance-Zertifikat im Gateway
4) CallHome-CSR im Gateway → CallHome -Zertifikat im Gateway
5) SIP-, MNT- & NMS-CSR im Gateway → SIP-, MNT- & NMS-CSR im Gateway

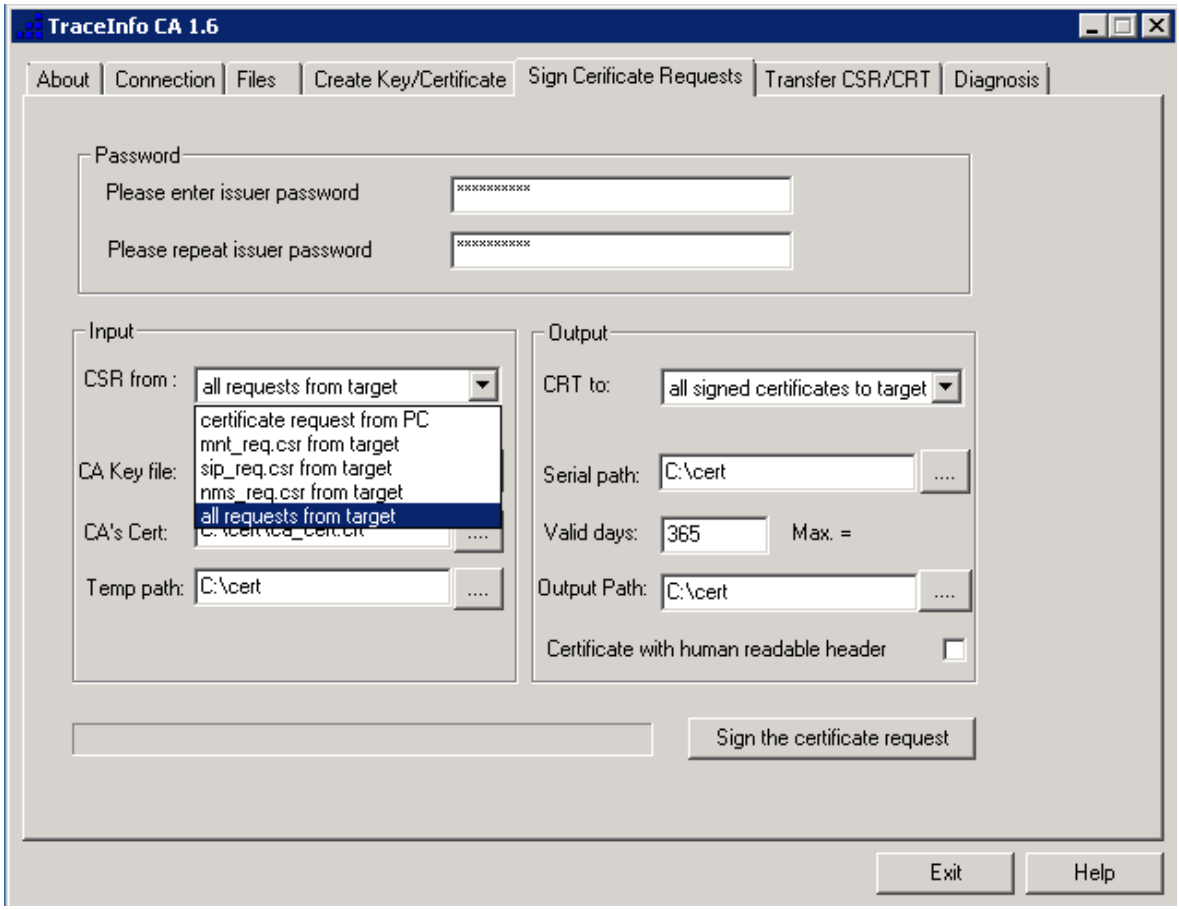


Abbildung 11 - CSR selbst signieren

3.2.1.3 CSR extern signieren

Die mit der TI-CA angelegten Root-, Maintenance- und CallHome-CSR (CA-, MNT, NMS-CSR) sowie die von den NovaTec-Gateways intern erzeugten SIP-, MNT- und NMS-CSR können auch von einer externen Zertifizierungsstelle (CA) signiert werden.

Deshalb können CSR mit der TI-CA von einem Gateway auf einen PC übertragen werden. Nachdem diese Gateway-CSR von einer fremden CA signiert worden sind, können die erhaltenen Zertifikate (CRT) mit der TI-CA zurück auf das NovaTec-System übertragen werden. Dazu dient der Reiter „Transfer CSR/CRT“:

1) Auswahl zu lesender CSR-Type (SIP, MNT oder NMS)
2) Auswahl Speichertort des CSR
3) Auswahl zu schreibender CSR-Type (SIP, MNT oder NMS)
4) Auswahl Speichertort des CSR

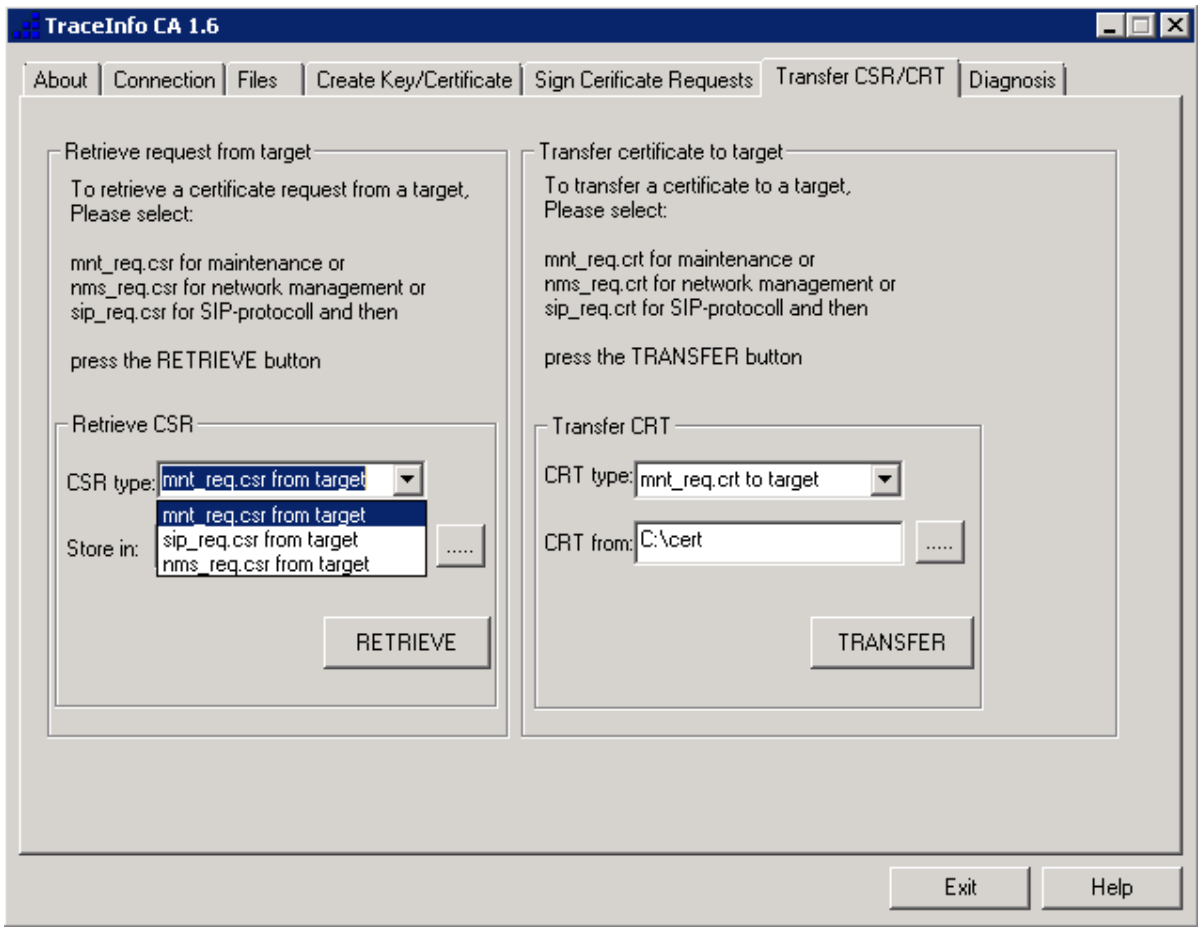


Abbildung 12 - CSR extern signieren

3.2.2 Klartext in Zertifikaten

Wird mit der TI-CA ein Certificate Signing Request (CSR) für eine Drittpartei (z.B. CUCM) signiert, enthält das erstellte Zertifikat Klartext. Einige Anwendungen können nur Zertifikatdateien ohne Klartext verarbeiten. Daher besitzt die TI-CA ab Release 1.3 auf der "Create Key/Certificate" Seite eine Option, um Zertifikate mit oder ohne Klartext zu erstellen (siehe Abbildung 13 - Zertifikat mit/ohne Klartext ausstellen).

Aus Zertifikaten, die mit einer älteren TI-CA Version signiert werden, kann manuell der Klartextteil, wie folgt entfernt werden.

Der vorgeschriebene Teil des Zertifikates beginnt mit der Zeile

„-----BEGIN CERTIFICATE-----"

und endet mit der Zeile

„-----END CERTIFICATE-----".

Bitte benutzen Sie einen Editor wie z.B. WordPad um Klartext und Leerzeilen zu entfernen und das Zertifikat zu sichern. Die beiden oben aufgeführten Zeilen dürfen **nicht** aus dem Zertifikat gelöscht werden. Die Dateien können Sie dann weiterverwenden und sie beispielsweise in den CUCM laden (siehe auch "CUCM Crypto Install Guide").

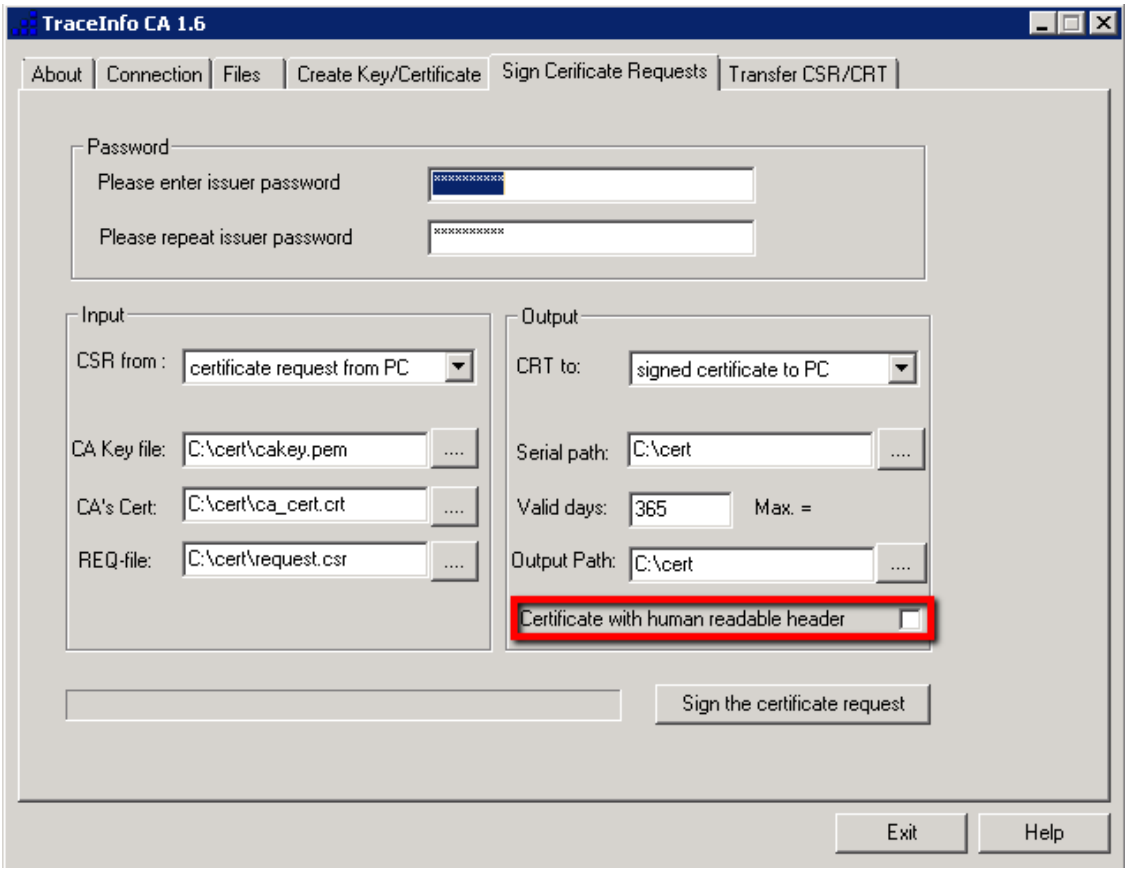
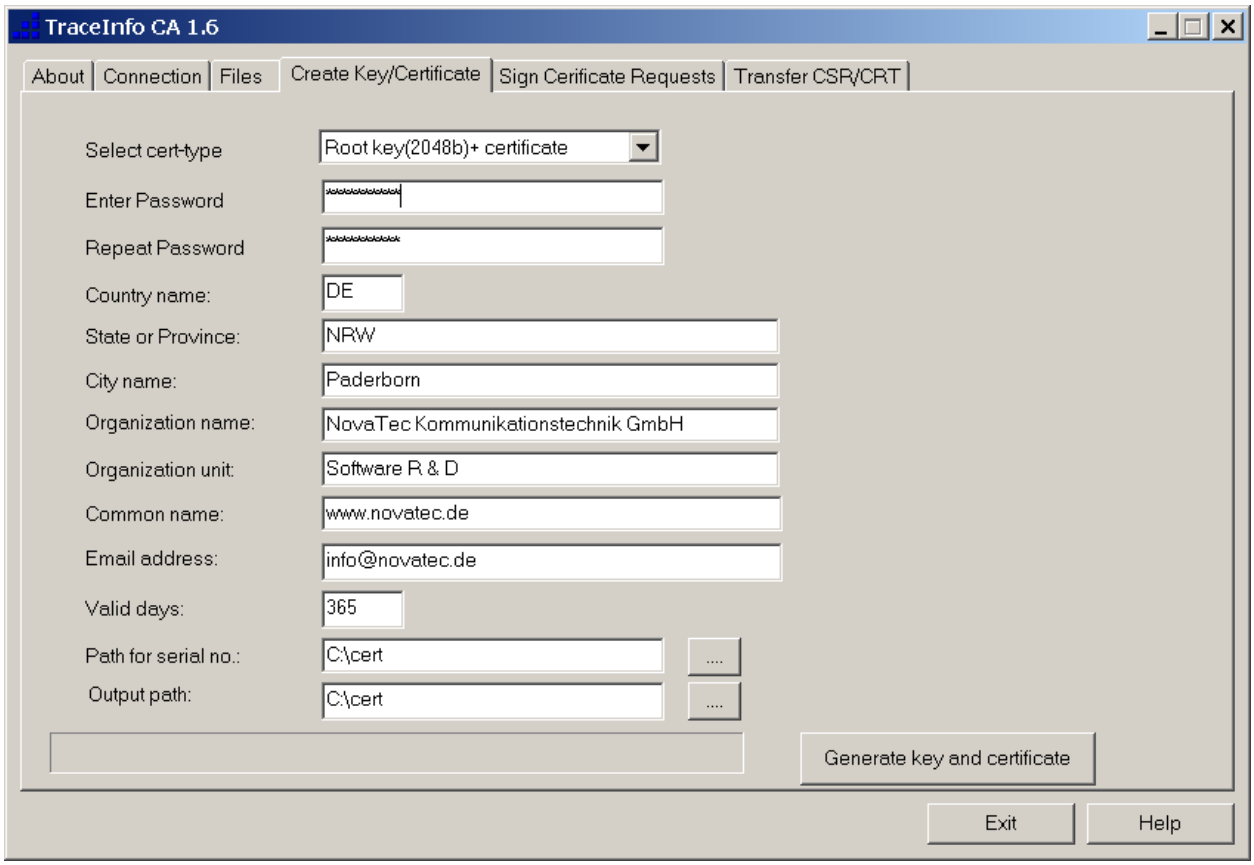


Abbildung 13 - Zertifikat mit/ohne Klartext ausstellen

3.2.3 Root-Zertifikat und Schlüssel erstellen

Erstellen eines selbst signierten Root-Zertifikats und des zugehörigen privaten Schlüssels “CA private key”.



- Eine Verbindung zwischen der TI-CA Applikation und dem Zielsystem ist nicht zwingend erforderlich.
- Wählen Sie "Root key (2048b) + Certificate" in der Auswahl.
- Wählen Sie ein CA-Passwort, dass mindestens 4 und maximal 20 Zeichen lang ist.
- Wiederholen Sie die Eingabe des CA-Passwortes. Schlägt dieser Schritt fehl, erscheint eine Fehlermeldung in der unteren Zeile und der Button "Generate key and certificate" wird deaktiviert.
- Nun geben Sie Land, Staat, Stadt, Unternehmen, Abteilung, Name und Email-Adresse für die CA ein. Das Land muss mit 2 Zeichen angegeben werden, alle anderen Angaben sind auf 64 Zeichen begrenzt.
- Geben Sie die Gültigkeitsdauer des Root-Zertifikates in Tagen an.
- Geben Sie einen Pfad an, unter dem die Serien-Nummer des Zertifikates gespeichert werden soll. (1)
- Geben Sie den Pfad an, unter dem der “CA Private Key“ gespeichert werden soll. Der erstellte Key und das Zertifikat werden hier im Format .pem/.crt mit Default-Namen gesichert: cakey.pem und ca_cert.crt.
- Nachdem diese Angaben gemacht wurden drücken Sie bitte den Button "Generate key and certificate". Es dauert einige Sekunden den „Private „key“ zu generieren. Es werden Statusmeldungen angezeigt.
- Bitte bestätigen Sie diese durch einen Klick auf den Ok-Button.

- Unter dem angegeben Dateipfad sind nun das erzeugte Root-Zertifikat „ca_cert.crt" und der zugehörige private 2048bit RSA Schlüssel „cakey.pem" zu finden.

Anmerkung (1):

Die Serien-Nummer wird in der Datei serial.txt gesichert. Wenn diese Datei im angegebenen Pfad nicht auffindbar ist wird die Applikation eine neue Datei mit einer Default-Startnummer erstellen. Der Nutzer kann die Startnummer selbst definieren, in dem er eine serial.txt Datei mit einem 16-stelligen Hexadezimalcode erzeugt, z.B. 0123456789ABCDEF. Die Applikation wird die aktuelle Seriennummer der Datei serial.txt verwenden.

3.3 SCEP auf Windows Servern konfigurieren

Ab Release 00.07.02.03 wird das Signieren von TLS-Zertifikaten auf NovaTec Gateways mit dem Simple Certificate Enrollment Protocol (SCEP) unterstützt

Für SCEP können als CA Server die „Windows Server 2003 R2 Standard Edition" oder die „Windows Server 2008 Enterprise Version" benutzt werden.

Die Beschreibung der Einrichtung eines Windows Server 2003 als SCEP-Zertifizierungsstelle, sowie das notwendige Add-on (cepsetup.exe) kann vom „Microsoft Download Center" geladen werden.

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

Beim Windows Server 2008 sind die Enterprise und die Datacenter Version durch den „Active Directory Certificate Service" (ADCS) mit dem „Network Device Enrollment Service" (NDES) in der Lage, das SCEP Protokoll auszuführen.

Microsoft gibt an, dass beide Implementierungen sich nach dem Standard von http://tools.ietf.org/html/draft-nourse-scep-18 verhalten.

Beide CA Server können das Enrollment automatisch oder manuell sowie mit bzw. ohne Passwort durchführen. Das Passwort erzeugen die CA Server als „One Time Password" mit einer Gültigkeit von 60 Minuten (für Rollout der Novatec-Syteme nicht geeignet).

Die Kombination von automatisch und ohne Password wird von der Norm aus Sicherheitsaspekten nicht empfohlen, ist aber für den Rollout der Novatec-Syteme geeignet.

4 Konfiguration

4.1 VoIP-Kanäle mit sRTP sichern

Nachdem mit der TLS-Lizenz auch die sRTP Verschlüsselung der VoIP Kanäle freigeschaltet worden ist, können die Konfigurationspunkte für sRTP komplettiert werden.

Die sRTP Einstellungen finden Sie unter dem Menüpunkt → „sRTP encryption option".

Unter dem Punkt → „sRTP encryption profile" können immer die Standardwerte verwendet werden. Hier sind keine Änderungen notwendig.

Stellen Sie jetzt die Verschlüsselungsmethode für sRTP ein. Wählen Sie dazu im Menü den Punkt → „sRTP encryption option" → „sRTP encryption handling profiles" an. Hier legen Sie einen Profilnamen fest und wählen die Methode für den Schlüsselaustausch. Für die häufigsten Anwendungsfälle (z.B. CUCM) ist die Standardmethode „MIKEY / SDP crypto attribute" passend.

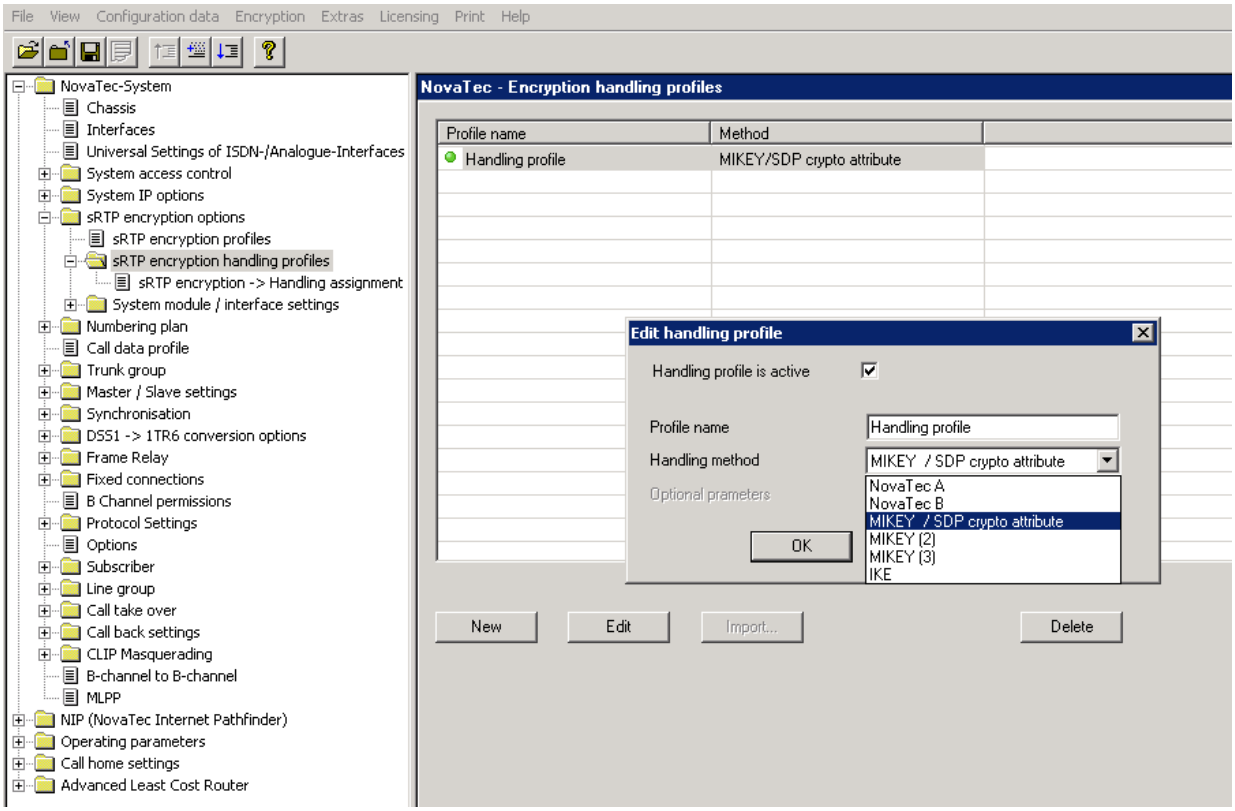


Abbildung 14 - sRTP Encryptionprofil

Danach wird unter → "sRTP encryption → Handling assignment" dem Encryptionprofil die Encryptionmethode zugeordnet.

Anschließend kann dieses Profil unter → „Modul assignment" dem SIP-Modul zugewiesen werden.

Damit sRTP mit dem SIP-Modul verwendet werden kann, muss das aktuell angelegte Encryption-Handlingprofil einer SIP-Verbindung zugeordnet werden. Der betreffende Konfigurationspunkt ist zu finden unter → NIP (NovaTec Internet Pathfinder) → SIP (VoIP) → „User mapping".

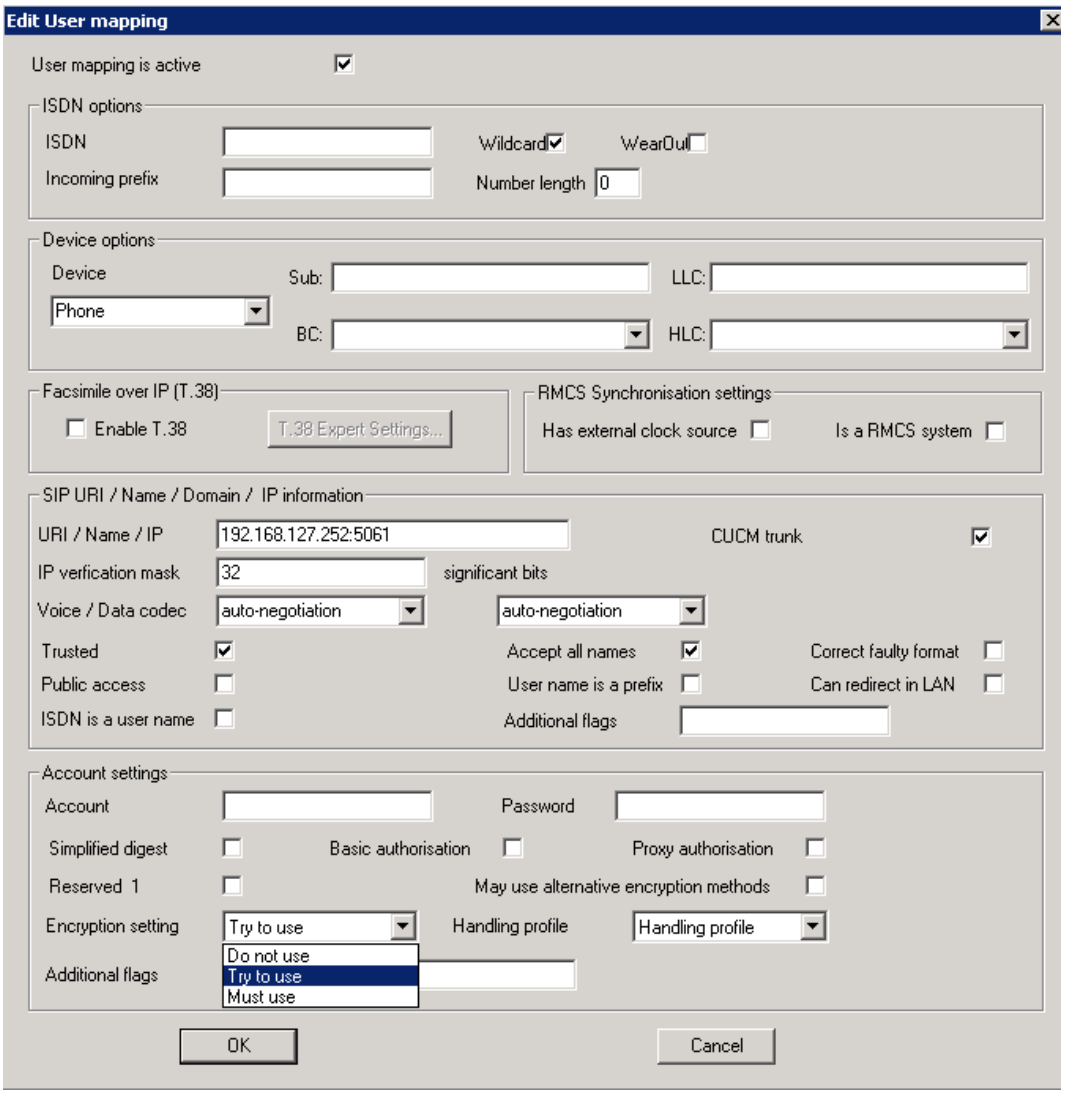


Abbildung 15 - sRTP SIP zuordnen

Unten rechts kann ein angelegtes „Handling profile" ausgewählt werden. Daneben kann links unter "Encryption setting" die sRTP-Verschlüsselung konfiguriert werden.

- „Do not use" → Trotz ausgewähltem Handlingprofils bleibt sRTP deaktiviert.
- „Try to use" → Wenn auf der Gegenstelle sRTP nicht aktiviert ist, wird die Verbindung auch unverschlüsselt aufgebaut.
- „Must use" → Nur wenn auch die Gegenstelle sRTP unterstützt, wird die Verbindung aufgebaut.

4.2 SIP mit TLS sichern

4.2.1 System IP options - enable security

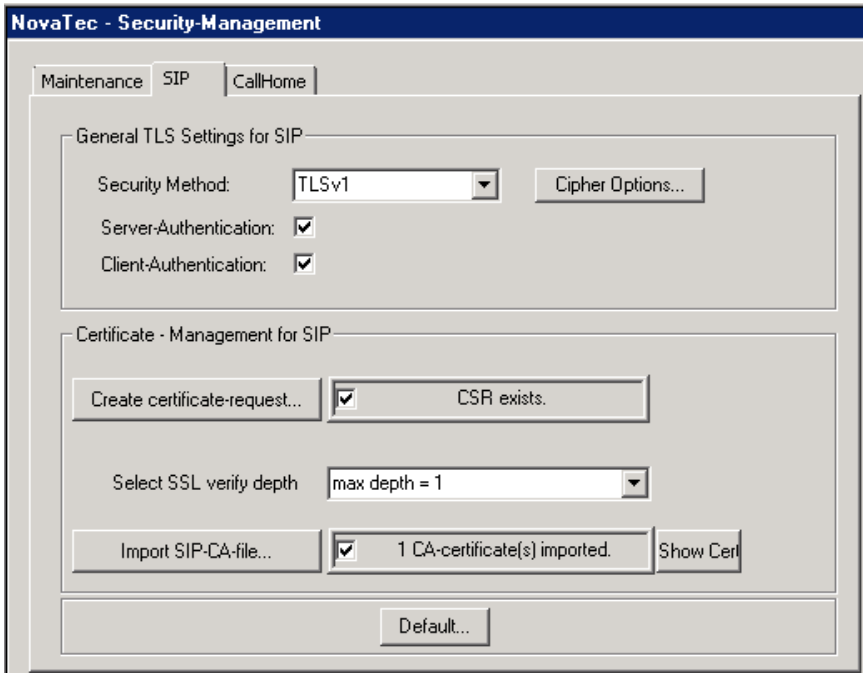


Abbildung 16 - SIP – enable security

Gehen Sie zu „System IP options" → „TLS Security" → und wählen den Reiter „SIP"

- Setzen Sie "Security Method" auf TLSv1.
- Setzen Sie das Häkchen bei "Server-Authentication", um das vom TLS-Server erhaltene Zertifikat zu verifizieren (z.B. S3, S6 und S20 an einem CUCM).
- Setzen Sie das Häkchen "Client-Authentication", um ein Zertifikat von einem TLS-Client anzufragen und zu verifizieren (z.B. Novatec-System als Trunk an einem CUCM).
- Die SSL-Verifizierungstiefe ist jetzt konfigurierbar (Werte von 1 bis 9 – siehe auch openSSL Dokumentation). Die Verifizierungstiefe ist das Limit bis zu dem Zertifikate in einer Kette während des Verifikations-Prozesses genutzt werden. Wenn die Zertifikatskette länger als erlaubt ist, werden Zertifikate über dem Limit ignoriert. Fehlermeldungen werden so generiert, als ob diese nicht existent wären: z.B. (depth = 0) SIP-CRT → (= 1) Sub-CRT → (= 2) Root-CA.

- Klicken Sie auf „Cipher Options", um die für die TLS-Verschlüsselung verwendete Methode festzulegen (empfohlen mit CUCM AES128-SHA). Wählen Sie die Methode „NULL SHA" nur für Debug-Absichten, da in diesem Fall keine Verschlüsselung stattfindet. Wählen Sie nicht die Methode „NULL SHA", wenn sRTP im CUCM konfiguriert ist. Im Allgemeinen ist es nicht zwingend erforderlich hier eine Methode auszuwählen. Wenn Sie keine auswählen, werden von einem NovaTec Gateway 19 Standartmethoden während des TLS-Verbindungsaufbaus angeboten. Wählen Sie hier eine oder mehrere Methoden aus, werden während des TLS-Verbindungsaufbaus nur die hier gesetzten Methoden angeboten und verwendet. Falls die Gegenstelle keine der gewählten Methoden unterstützt, wird der TLS-Verbindungsaufbau nicht gelingen.

4.2.2 Zertifikat-Request erstellen

In diesem Formular werden die Daten für eine Zertifizierungsanforderung (CSR) eingegeben und dieser CSR von einer Zertifizierungsstelle (CA) signiert. Man erhält ein Zertifikat (CRT) mit den hier eingetragenen Daten. Besondere Aufmerksamkeit ist auf den Eintrag für den „Common Name" zu richten, da dieser in einigen Szenarien verifiziert wird (z.B. TLS-Verbindungsaufbau mit CUCM). Wählen Sie diesen Namen mit Bedacht.

Beispiel-Szenarien:

1.) Wird der NovaTec-Gateway als CUCM Line-Anschluss konfiguriert, so ist hier „SEP" gefolgt von der MAC-Adresse des Gateways einzutragen.

2.) Wird der NovaTec-Gateway als CUCM Trunk konfiguriert, so muss der Common Name übereinstimmen mit dem „X.509 Subject Name" in der „SIP Trunk Security Profile Configuration" des CUCM.

Tip: Wird im 2.) Szenario (CUCM Trunk) der SIP-CSR des NovaTec Gateways von NAMES signiert, kann im NAMES-CA-Root-Zertifikat der Common Name übereinstimmend mit dem „X.509 Subject Name" des CUCM gesetzt werden. Wenn auch die „Policy" in der NAMES-CA für das Signieren des SIP-CSR auf „Match" gesetzt wird, werden nur SIP-CSR signiert, deren Common Name identisch sind mit dem „X.509 Subject Name" (siehe NAMES Handbuch 1.6.0a, Kapitel 5.5.3, Absatz 6. „Policy konfigurieren"). Falls der Common Name im SIP-CSR nicht mit dem Common Name des NAMES-CA-Root-Zertifikats übereinstimmt, wird eine Fehlermeldung ausgegeben.

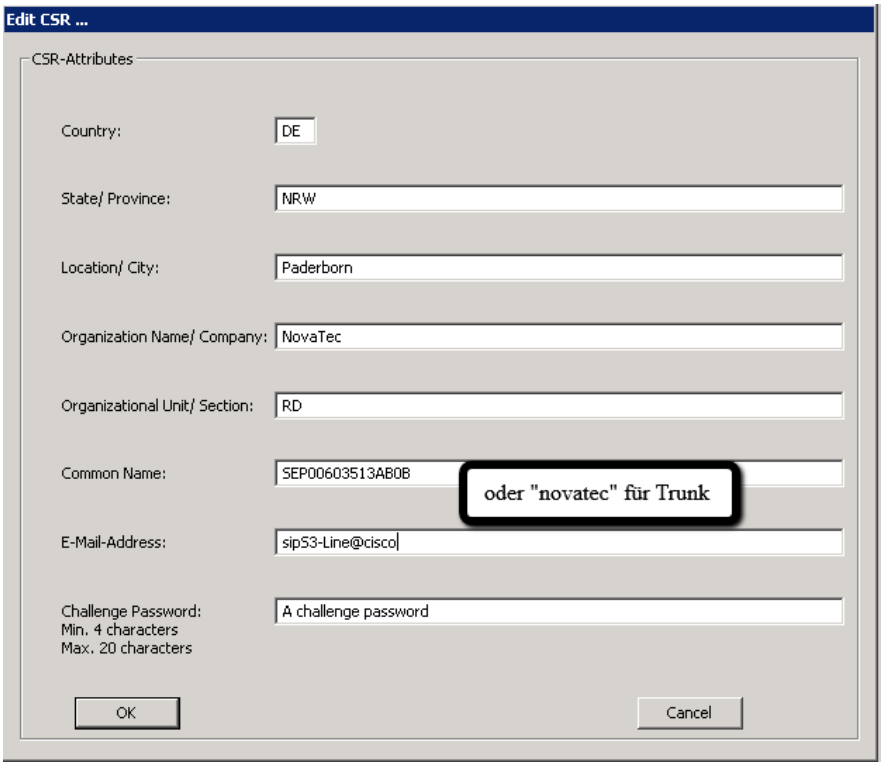


Abbildung 17 - SIP-CSR Common Name

4.2.3 CA-Zertifikat in Trust Liste laden

Empfangene Zertifikate werden gegen CA-Zertikate aus der lokalen „Liste vertrauenswürdiger Zertifizierungsstellen" (Trust List) geprüft. Da der Aussteller eines Zertifikats, dessen CA-Zertifikat in der lokalen Trust Liste gespeichert ist, als vertrauenswürdig gilt, gilt ein Zertifikat als verifiziert, das von diesem Aussteller signiert wurde. Der Aussteller („Issuer") ist in jedem Zertifikat angegeben.

CA-Zertifikate von vertrauenswürdigen Herausgebern können in dem unten abgebildeten Reiter mit der Schaltfläche „Import SIP-CA-file…" in die Trust List der SIP Instanz importiert werden. Vor dem eigentlichen Import wird der Inhalt eines hierfür ausgewählten Zertifikats angezeigt. Der Anwender kann den Import abbrechen, falls das Zertifikat ihm nicht zusagt. Die Anzahl der in der Trust List vorhandenen CA-Zertifikate wird dort auch mitgeteilt. Jederzeit kann der Inhalt der importierten Zertifikate auch mit der Schaltfläche „Show Cert" angezeigt werden.

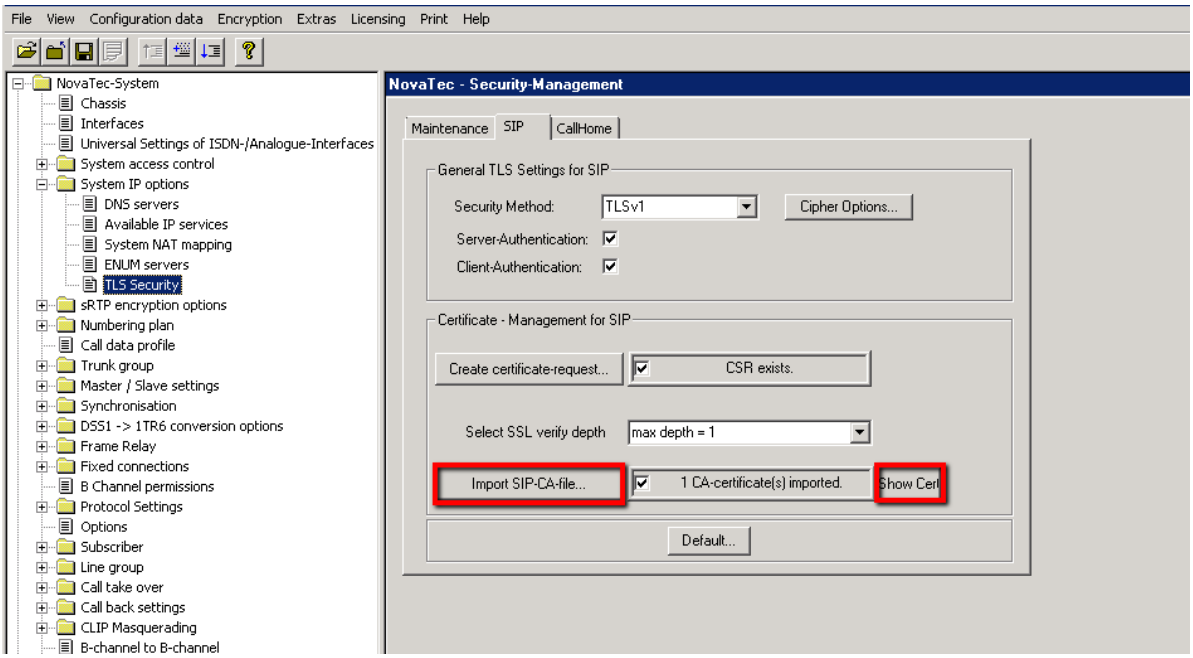


Abbildung 18 - Trust Liste - CA-Zertifikat laden

Gewöhnlich wird während des TLS-Verbindungsaufbaus, beispielsweise für SIP, nicht nur das angeforderte SIP-Zertifikat geliefert, sondern eine komplette Kette von Zertifikaten. Somit ist es ausreichend nur das höchste CA-Zertifikat in die lokale Trust Liste zu importieren. Eine Kette besteht, neben dem CA-Zertifikat, eventuell aus Sub-CA-Zertifikaten bis zu demjenigen herunter, mit dem das SIP-Zertifikat signiert worden ist. Die Gegenstelle liefert eine Zertifikatskette nur, wenn dort die Kette komplett vorliegt. Fehlt ein Element, ein Zertifikat, wird nur das angeforderte SIP-Zertifikat geliefert. Die Kette muss dann der Empfänger mit Zertifikaten aus seiner lokalen Trust Liste vervollständigen können. Diese müssen dort importiert sein.

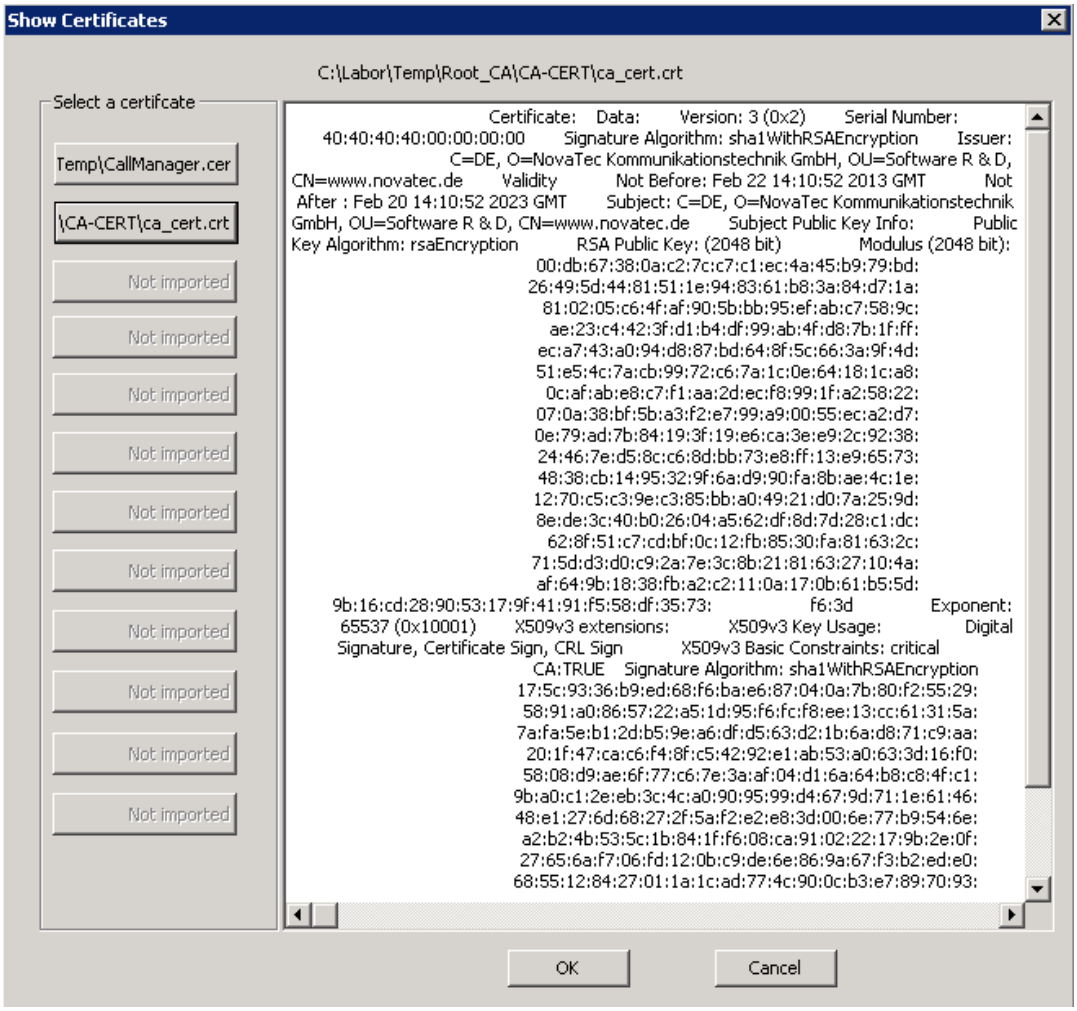


Abbildung 19 - Trust Liste - Zertifikat anzeigen

4.2.4 SIP-TLS User Mapping – CUCM Trunk

Gehen Sie jetzt nach „NIP" -> „SIP" -> „Mapping lists" -> „User mapping".

Hier sind folgende Einstellungen für eine gesicherte SIP-Verbindung relevant:

- Der Eintrag der TLS-Portnummer 5061 im Feld "URI / Name / IP".

Falls der NovaTec Gateway an einem TLS gesicherten CUCM Trunk angeschlossen ist.

- Die Checkbox „CUCM trunk" setzen.

Wenn auch der eigentliche Sprach- bzw. Datenkanal mit sRTP gesichert sein soll:

- Die sRTP-Konfigurationsfelder „Encryption setting" und „Handling profile" einstellen.

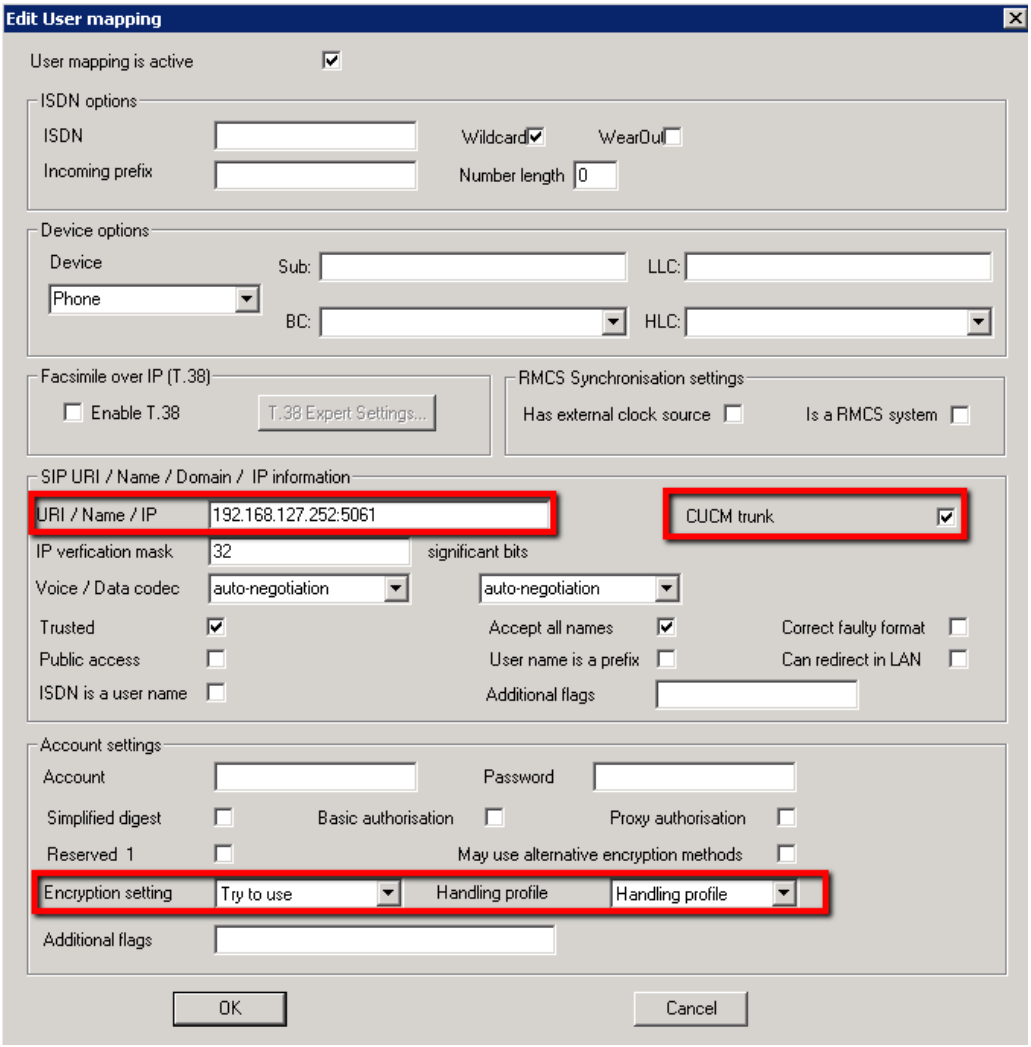


Abbildung 20 - SIP-TLS User Mapping

4.2.5 SIP-TLS Local Mapping – CUCM Trunk

Rufen Sie „NIP" → „SIP" -> „Mapping lists" → „Local mapping" auf.

Hier sind folgende Einstellungen für eine gesicherte SIP-Verbindung relevant:

- Der Eintrag der TLS-Portnummer 5061 im Feld "Registrar".

Falls das NovaTec Gateway an einem TLS gesicherten CUCM Trunk angeschlossen ist:

- Die Checkbox „CUCM trunk" setzen.

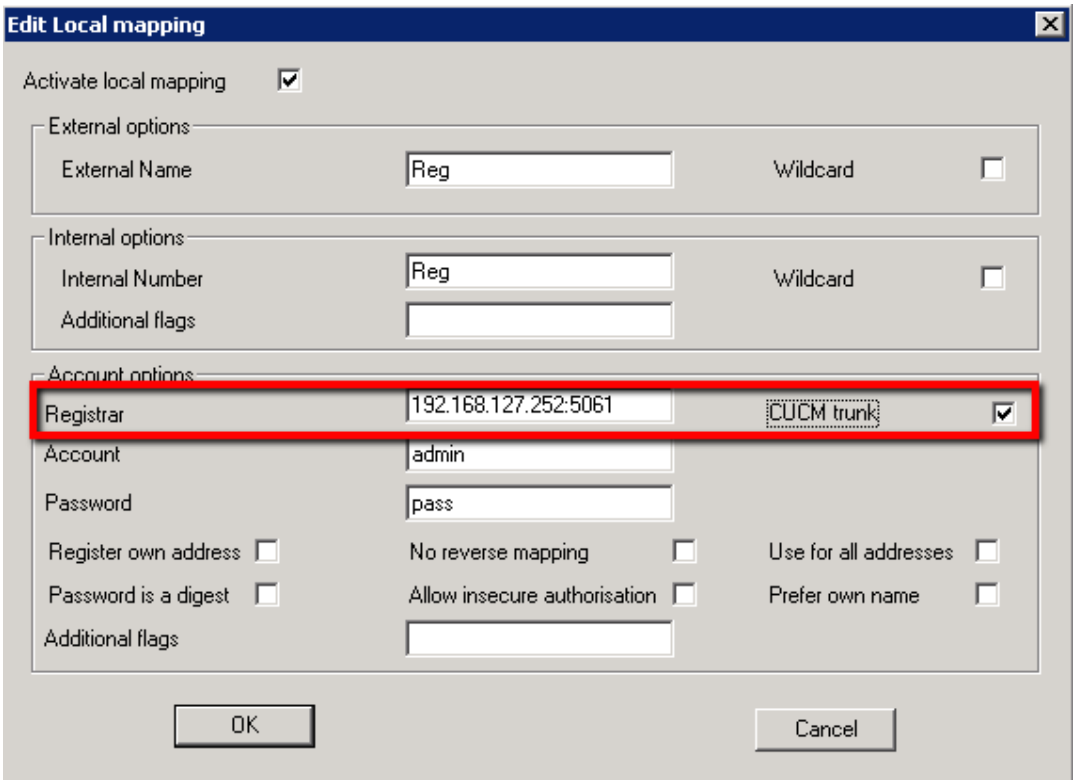


Abbildung 21 - SIP-TLS Local Mapping

4.2.6 SIP-TLS Optional Flags

Gehen Sie jetzt zu „NIP" -> „SIP" -> „General Settings" -> „Optional Flags 2".

Setzen Sie das Flag „Register as CISCO device at UCM", wenn das NovaTec Gateway, hier häufig eine S3, an einem (auch ungesicherten) Line-Anschluss eines CUCM betrieben wird.

Setzen Sie das Flag „Establish TLS connection queue", wenn das NovaTec Gateway an mehreren mit TLS gesicherten CUCM Trunks betrieben wird. Dies bewirkt, dass mehrere gleichzeitig stattfindende Anfragen eine TLS-Verbindung aufzubauen, sich nicht gegenseitig blockieren.

Das Flag bitte nur setzen, wenn im SIP User und Local Mapping mehr als drei CUCM Trunk-Adressen eingetragen sind und festgestellt wurde, dass der TLS-Verbindungsaufbau zu vielen Trunks nicht wie erwartet funktioniert.

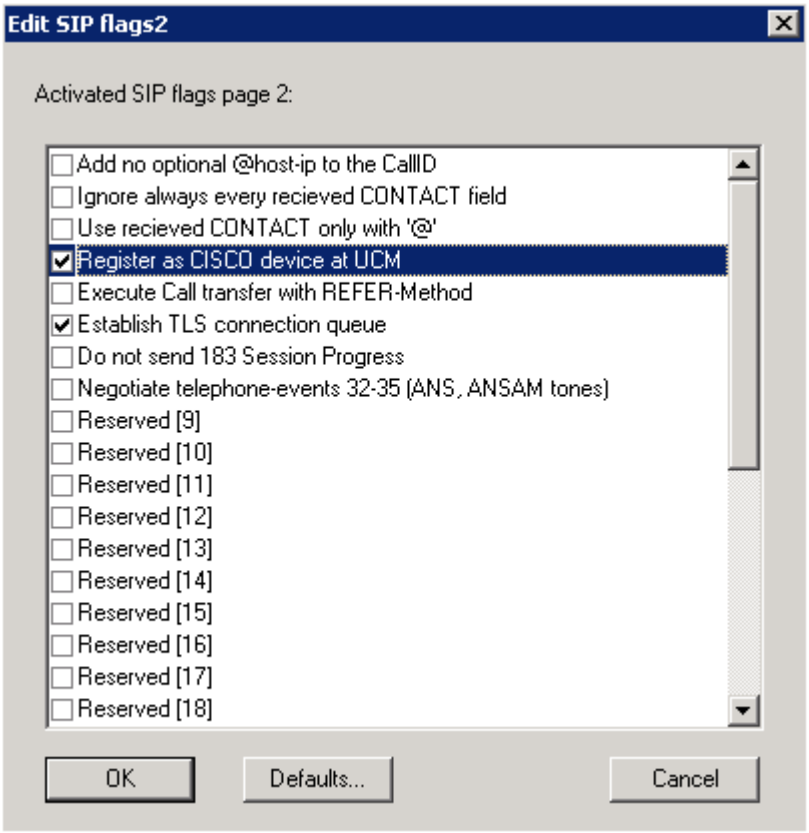


Abbildung 22 - SIP-TLS Optional Flags 2

4.3 SCEP

Ab Release 00.07.02.03 wird das "Simple Certificate Enrollment Protocol (SCEP)" unterstützt. Die NovaTec Konfiguration wurde unter dem Menüpunkt „Operating parameter" um die „SCEP Settings" erweitert. Diese beinhalten die globalen Einstellungen für alle drei Instanzen (NMT, SIP, CallHome). Sämtliche Einstellungen sind für Windows 2003 und 2008 Server gleich. Erläuterungen hierzu im Anhang unter 7.3 SCEP Applikation.

4.3.1 Einstellungen für den Einsatz von SCEP

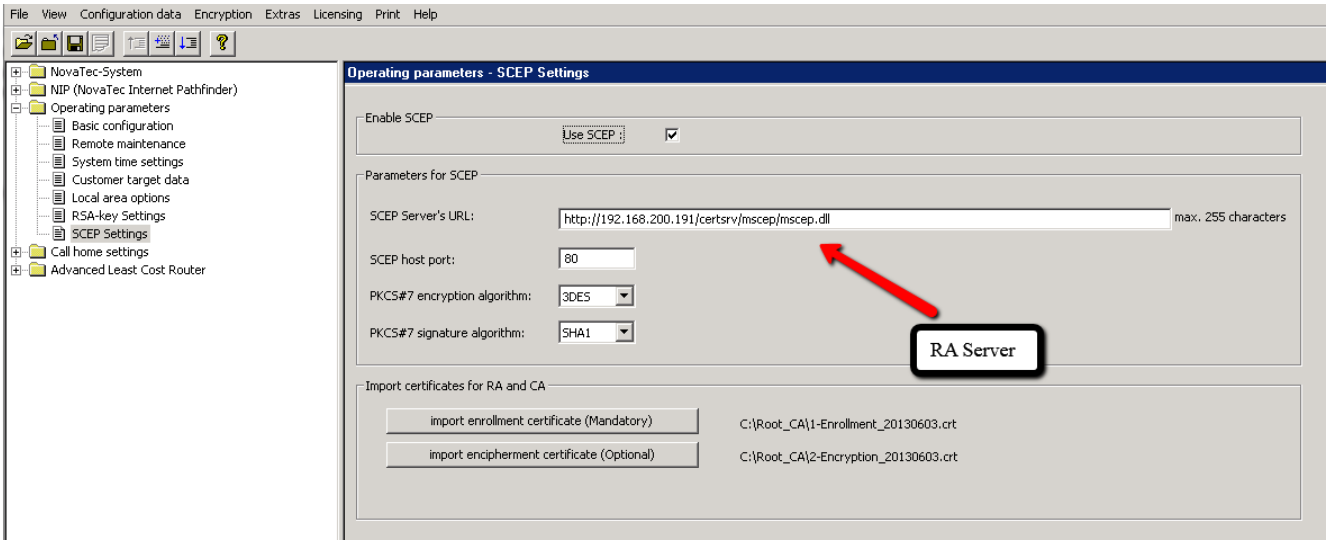


Abbildung 23 - SCEP Server URL

Durch Aktivierung des „UseSCEP" Feldes müssen verschiedene zusätzliche Parameter eingestellt werden. In das Eingabefeld für die SCEP Server URL wird die Microsoft Standard URL http://FQDN/certsrv/mscep/mscep.dll eingetragen. Die Eingabe der „FQDN" Server Domäne (caserver1.novanet.local) erfordert eine zusätzliche DNS Auflösung, und stellt dadurch die Vertrauenswürdigkeit der Gegenstelle her. Anstatt der „FQDN" kann auch eine Server IP Adresse eingegeben werden. Da das SCEP Protokoll „http" basierend ist, ergibt sich, dass der Default Port 80 ist. Als nächstes können die PKCS#7 basierenden Algorithmen für Encryption und Signatur bestimmt werden. Nach Norm sind dies: DES, 3DES, Blowfish sowie md5 und sha1.

4.3.2 Registration Authority Zertifikate

Wird ein Microsoft Server als CA Zertifizierungsstelle für das Enrollment mit SCEP eingesetzt, müssen zwei Registration Authority (RA) Zertifikate für das „Enrollment" von diesem importiert werden. Das eine mit "*usage: Digital Signature, Non Repudiation*" ist ein signiertes RA Zertifikat (Enrollment Certificate), und das andere mit "*usage: Key Encipherment, Data Encipherment*" ist für die Encryption (Encipherment Certificate). Beide müssen aus der Zertifizierungsstelle des CA Servers im bas64 Format exportiert werden.

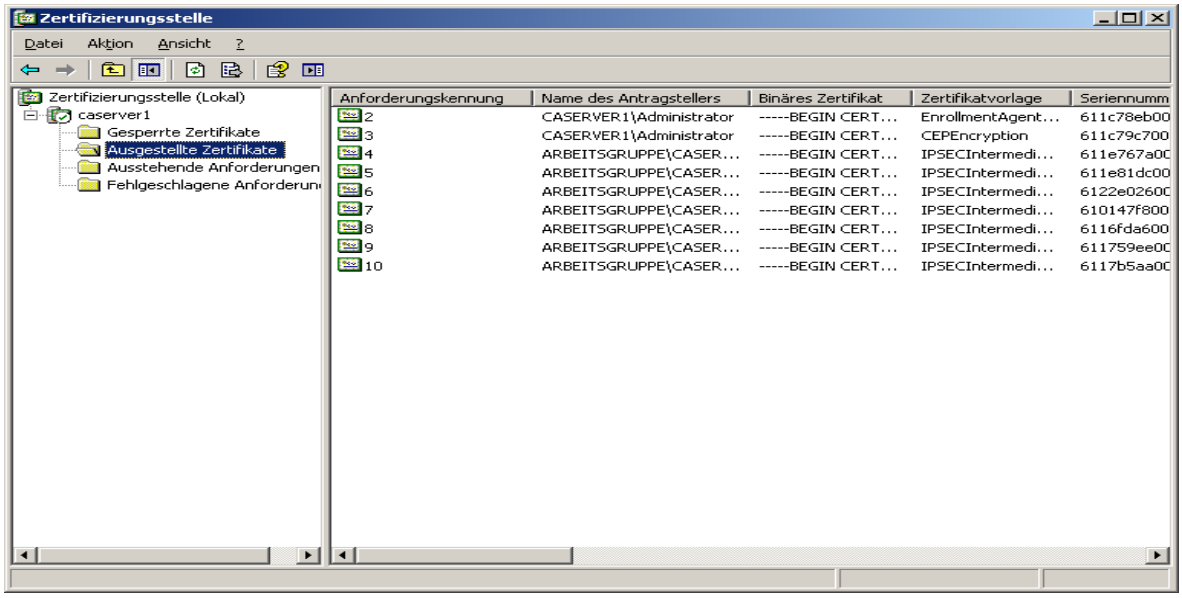


Abbildung 24 - Export der beiden Enrollment Zertifikate

In der Liste (Abbildung 24 - Export der beiden Enrollment Zertifikate) sind die beiden ersten Zertifikate für das „Enrollment" verantwortlich. Der Export startet mit einem Doppelklick auf die entsprechende Reihe. Beide Zertifikate müssen Base-64 kodiert sein. Zum Import der Zertifikate in die NovaTec Konfigurationsoberfläche muss die Extension *.cer* in .crt umbenannt werden.

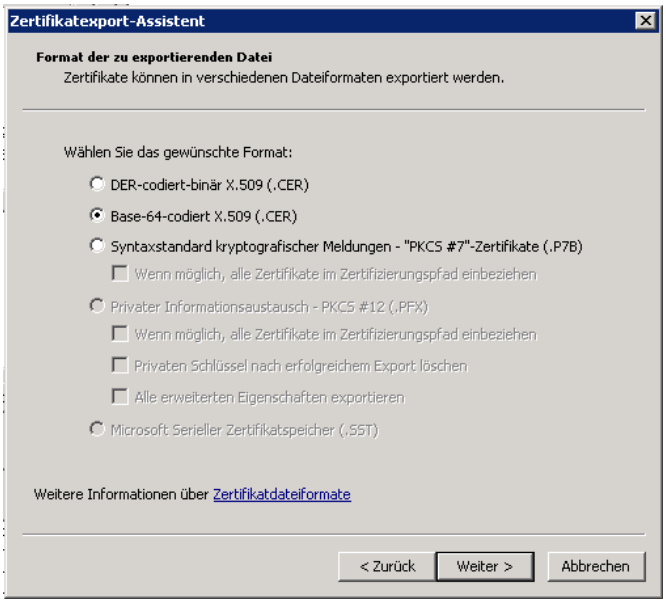


Abbildung 25 – Exportdateiformat

4.3.3 CA-Kette

Alle drei Instanzen (MNT, SIP und CallHome) des NovaTec Gateways benötigen natürlich auch das „Public CA Certifikate" bzw. eine Zertifikatskette.

Auf dem Microsoft CA Server startet der Export mit einem Rechtsklick im Baum der Zertifizierungsstelle → CA Server → Eigenschaften → Zertifikat anzeigen → Details → In Datei kopieren …

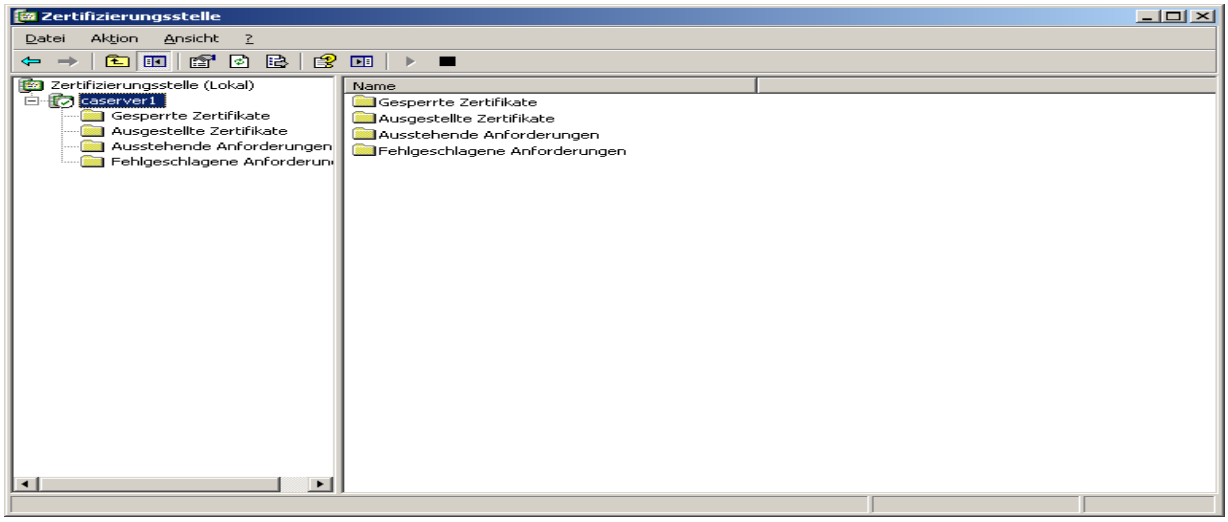


Abbildung 26 - SCEP CA Export

Die Zertifikate werden in die NovaTec Konfiguration importiert unter dem Menüpunkt „NovaTec-System" → „System IP options" → „TLS Security". Dort den jeweiligen Reiter „Maintenace", „SIP" oder „CallHome" auswählen, und unter „Import …CA-file" den Dateiimport starten.

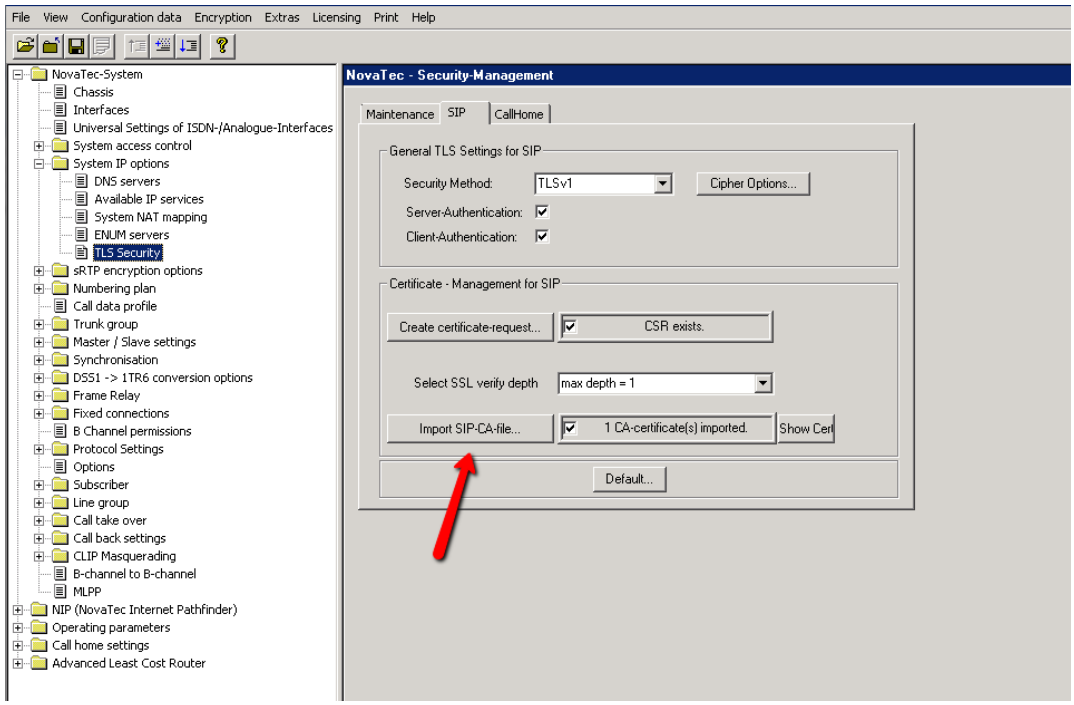


Abbildung 27 - SCEP CA Import

Wenn kein optionales Challenge Password verwendet wird (siehe Kapitel 4.3.4), ist die Konfiguration von SCEP hiermit abgeschlossen.

Nach der Übertragung der Konfiguration in das System und dessen Neustart, werden die TLS-Zertifikate der drei Instanzen per SCEP auf dem Gateway signiert.

Der Ablauf der Signierung mit SCEP sowie die danach noch manuell auszuführenden Schritte sind im Kapitel 5.2 beschrieben.

4.3.4 Challenge Password

Ist das optionale Challenge Password in der Registry des CA Servers aktiviert, benötigen alle drei Instanzen (MNT, SIP und CallHome) des NovaTec Gateways ein „One Time Password".

Mit einem Browser die Seite „http://CA Server Name/certsrv/mscep" bei Windows 2003 oder bei Windows 2008 „http://CA Server Name/certsrv/mscep_admin" öffnen.

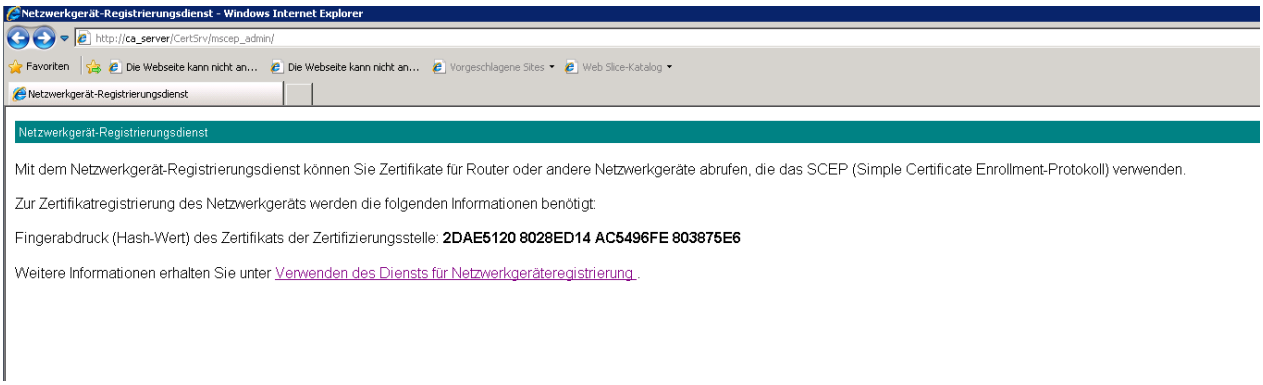


Abbildung 28 - Kopieren des Challenge Passwords

Das Challenge Password ist eine Random-Zeichenfolge und kann per „copy and paste" vom Web-Browser in die NovaTec Konfiguration übernommen werden (Abbildung 29 - Einfügen des Challenge Passwords).

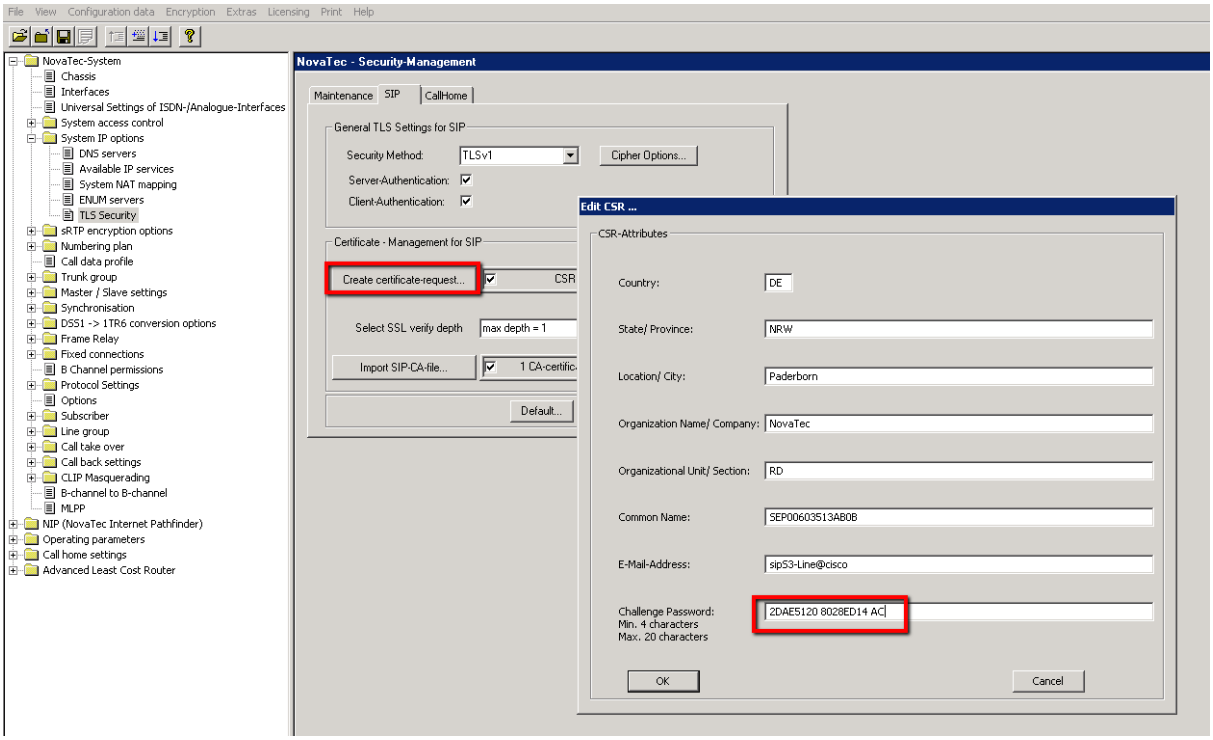


Abbildung 29 - Einfügen des Challenge Passwords

Hiermit ist die Konfiguration von SCEP abgeschlossen.

Nach der Übertragung der Konfiguration in das System und dessen Neustart, werden die TLS-Zertifikate der drei Instanzen per SCEP auf dem Gateway signiert.

Der Ablauf der Signierung mit SCEP sowie die danach noch manuell auszuführenden Schritte sind im Kapitel 5.2 beschrieben.

4.4 NAMES

NovaTec Administration and Management Element Server (NAMES) ist ein Elementmanger für alle NovaTec Gateway Produkte. Mit NAMES können Rollout und Inbetriebnahme der Gateways sowie Überwachung, Administration, Konfiguration und Softwareupdates der Gateways im Lifebetrieb durchgeführt werden.

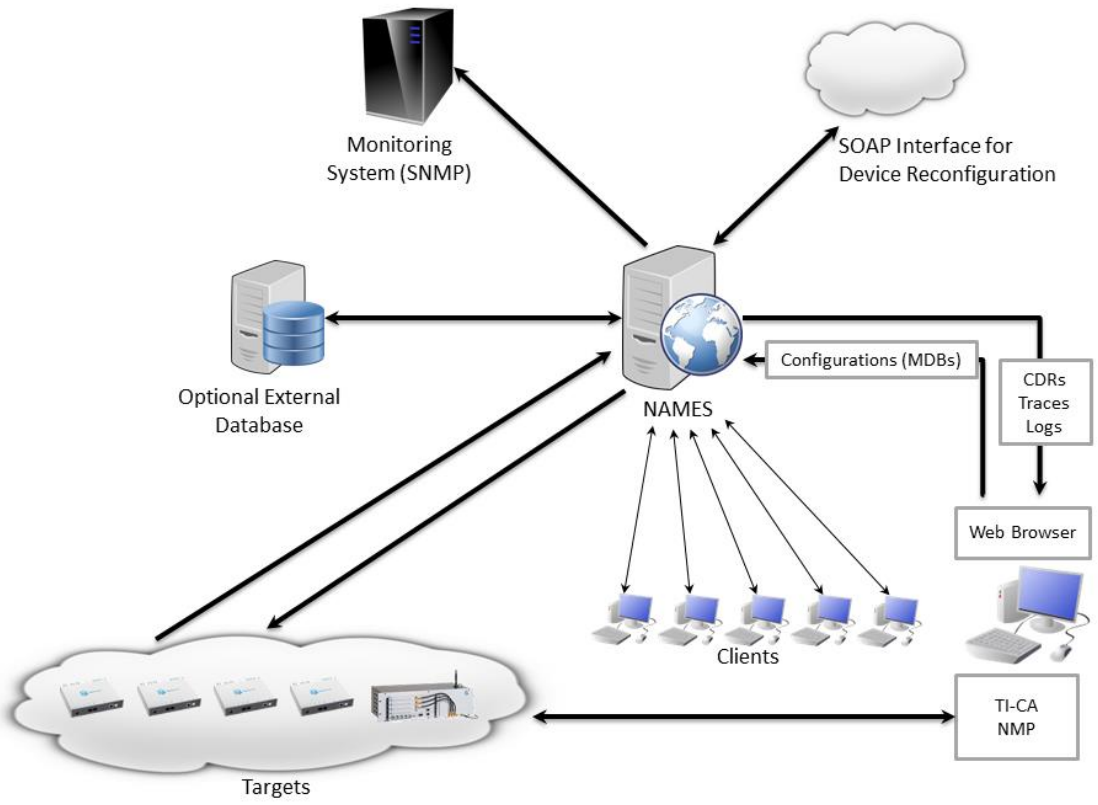


Abbildung 30 - NAMES Architektur

Zur Verwendung von NAMES müssen die dargestellten Verbindungen möglich sein. Eventuell vorhandene Firewalls zwischen den Systemkomponenten müssen entsprechend den Angaben im Dokument „IP-Port Matrix der NovaTec Systeme und Anwendungen" konfiguriert werden, um die Kommunikation zuzulassen. Das Dokument kann von der NovaTec-Website unter http://www.novatec.de/handbooks/IP-Portmatrix.pdf heruntergeladen werden.

In NAMES ist eine Zertifizierungsstelle (CA) integriert. Damit kann NAMES Zertifizierungsanforderungen (CSR) der drei Instanzen (MNT, SIP, NMS) auf NovaTec Systemen signieren. Es müssen keine zusätzlichen Parameter in der Konfiguration der Systeme eingestellt werden, damit diese durch NAMES signiert werden können.

Auch kann NAMES eine mit TLS gesicherte MNT-Verbindung zu den verwalteten Gateways aufbauen.

Das NAMES Benutzerhandbuch bietet eine detaillierte Anleitung.

Es folgt eine Kurzanleitung.

4.4.1 NAMES als CA

Für die NAMES CA werden ein CA-Zertifikat und ein privater Schlüssel benötigt. Es kann eine extern generierte Zertifikat-Datei sowie die zugehörige Schlüssel-Datei hochgeladen werden. Allerdings kann NAMES auch ein selbstsigniertes Zertifikat und einen privaten Schlüssel generieren. Wenn NAMES als Sub-CA in einer vorhandenen PKI verwendet werden soll, so muss ein CSR erstellt und an die übergeordnete Certificate Authority übermittelt werden, die dann ein neues CA-Zertifikat für diesen CSR ausstellen muss. Dieses von einer externen CA ausgestellte Zertifikat muss in die NAMES CA hochgeladen werden.

Danach kann NAMES NovaTec Gateways signieren, wenn der Job „Zertifikat signieren" ausgeführt wird und im Gateway konfigurierte CSRs angelegt sind.

4.4.2 Gesicherte Verbindung zum Gateway

Ist im Gateway für „Maintenance" eine gesicherte Verbindung konfiguriert und das TLS-Zertifikat für diese Instanz im Gateway signiert, kann NAMES diese sichere Verbindung nutzen. In NAMES wird dazu ein SSL-Kontext einem Target zugeordnet, wodurch dann eine TLS-Verbindung zum Gateway aufbaut wird.

In NAMES können diese SSL-Kontexte angelegt werden. In einem SSL-Kontext werden für eine gesicherte Verbindung verschiedene SSL-Parameter zusammengefasst (ROOT-CA-Zertifikat, eigenes Zertifikat, privater Schlüssel). Zusätzlich kann das CA-Zertifikat einer oder mehrerer vertrauenswürdiger Zertifizierungsstellen in den Kontext hochgeladen werden.

4.5 Maintenance / CallHome sichern

Damit die TCP/IP Verbindungen zwischen NovaTec Anwendungen und NovaTec Gateways mit TLS gesichert werden können, ist als Voraussetzung eine Firmware-Lizenz mit aktivierter TLS-Option bei NovaTec zu beantragen, und diese mit der Konfiguration in das Gateway zu laden (siehe Kapitel 3.1 Freischalten der Verschlüsselung in NovaTec Systemen).

Danach kann mit den hier aufgeführten Arbeitsschritten, eine TLS gesicherte Verbindung zwischen einem NovaTec Gateway und NovaTec Applikationen, wie NAME-Server, TraceInfo-Client, TI-CA oder einem CallHome-Server eingerichtet werden.

1) Die TI-CA benötigt ein ROOT-Zertifikat.

2) Für die PC-seitige Zertifizierung von Maintenance- bzw. CallHome-Verbindungen stellt die TI-CA Zertifizierungsanforderungen (CSR) aus.

3) Diese CSR für die PC-Seite werden durch die TI-CA signiert, oder an eine externe CA zum Signieren gegeben.

4) In der Konfiguration des Gateways werden die notwendigen Einstellungen für die Maintenance- bzw. CallHome-CSR des NovaTec Gateways gemacht. Auch wird das passende Root-CA-Zertifikat in die Trust Liste importiert.

5) Nach dem Neustart mit dieser Konfiguration generiert der NovaTec Gateway die konfigurierten Zertifizierungsanträge.

6) Die CSR auf dem NovaTec Gateway werden entweder durch die TI-CA signiert oder mit der TI-CA von dem Gateway heruntergeladen und zum Signieren an eine externe CA gegeben.

7) Die von einer externen CA ausgestellten Zertifikate werden mit der TI-CA in den NovaTec Gateway transportiert. Von der TI-CA direkt signierte Zertifikate sind schon im Gateway gespeichert.

8) Nach einem Reset sind die Zertifikate auf dem Gateway aktiv.

9) Die unter 3) ausgestellten Zertifikate werden auf der PC-Seite installiert. Zum Beispiel in einen NAMES SSL-Kontext geladen (siehe NAMES Handbuch) oder in der TI-CA unter dem „Connection – Network Options" Menü importiert. Jetzt können durch TLS gesicherte Verbindungen zwischen NovaTec Gateways und NovaTec Applikationen genutzt werden.

4.5.1 Die TI-CA benötigt ein ROOT-Zertifikat

Das Root-Zertifikat kann, wie unter Kapitel 3.2.3 Root-Zertifikat und Schlüssel erstellen beschrieben, von der TI-CA selbst, oder von einer externen CA signiert werden. Die weitere Verwendung eines selbst oder extern signierten Root-Zertifikats unterscheidet sich nicht.

4.5.2 Maintenance- und CallHome-CSR ausstellen

Mit der TI-CA werden Zertifizierungsanforderungen (CSR) unter dem Reiter „Create Key/Certificate" erstellt. Wie in Kapitel 3.2.1.1 CSR anlegen beschrieben, können für Maintenance (MNT) und CallHome (NMS) CSR und Schlüssel mit 1024 oder 2048 bit Schlüssellänge erstellt werden.

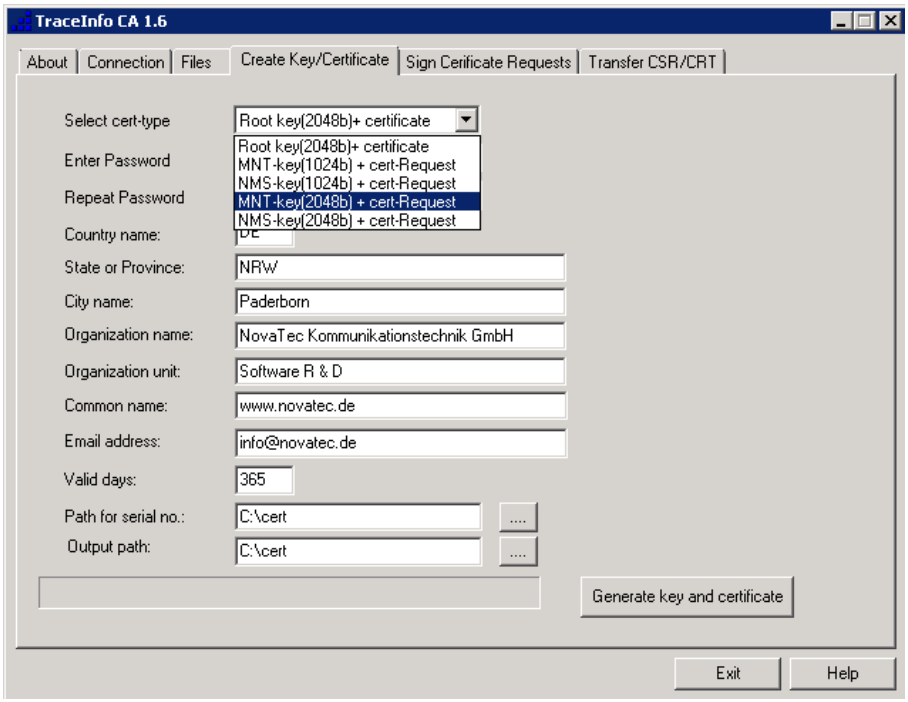


Abbildung 31 - MNT & NMS CSR erstellen

Mit Betätigen der Schaltfläche „Generate key and certificate" werden die Datei mit dem privatem Schlüssel und der CSR generiert. Diese werden in den unter „Output path" angegebenen Dateipfad abgelegt. Der CSR kann zum Signieren an eine externe Zertifizierungsstelle (CA) gegeben oder mit der TI-CA signiert werden.

4.5.3 TI-CA signiert MNT- & NMS-CSR

- TI-CA Reiter „Sign Certificate Requests"

Input:

- "CSR from:" "certificate request from PC" wählen
- Für „CA Key file:" und „CA's Cert:" sind die Dateien des ROOT-Zertifikats zu wählen, mit dem der MNT bzw. NMS-CSR signiert werden soll.
- Das „REQ-file:" ist der oben erstellte MNT- oder NMS-CSR.

Output:

- "CRT to: "certificate request to PC" wählen
- "Serial Path:" Den Pfad für die verwendete Seriennummer des zu generierenden Zertifikats angeben.
- „ Valid days:" Die gewünschte Gültigkeitsdauer einstellen.
- „Output Path:" Hier wird das erstellte Zertifikat gespeichert.
- „Cerificate with human readable header" deaktivieren.
- Mit Betätigung der Schaltfläche „Sign the Certificate request" wird das Zertifikat erzeugt und im gewählten „Output Path:" abgelegt.

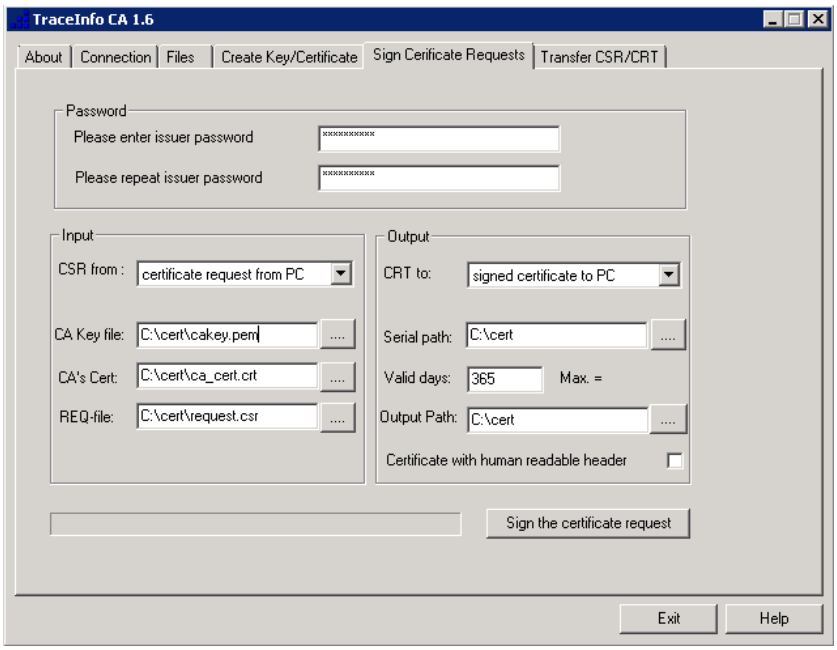


Abbildung 32 - TI-CA signiert MNT- & NMS-CSR

4.5.4 Konfiguration der MNT- & NMS-CSR

In der NovaTec Konfiguration den Menüpunkt → „NoavTec-System" → „System IP options" → TLS-Security" den Reiter „Maintenance" (MNT) bzw. CallHome (NMS) wählen.

Die Zertifizierungsanforderungen (CSR) für die Instanzen Maintenance bzw. CallHome werden für beide ähnlich konfiguriert.

- Als „Security Method:" muss „TLSv1" ausgewählt werden.

Der einzige Unterschied besteht darin, dass im Gateway für MNT die „Client-Authentication" aktiviert werden kann, da hier der Gateway während des TLS-Verbindungsaufbaus die Rolle des Servers einnimmt. Dieser fordert das Client-Zertifikat von der PC-Applikation an und prüft dieses, wenn dieses Feature aktiviert ist.

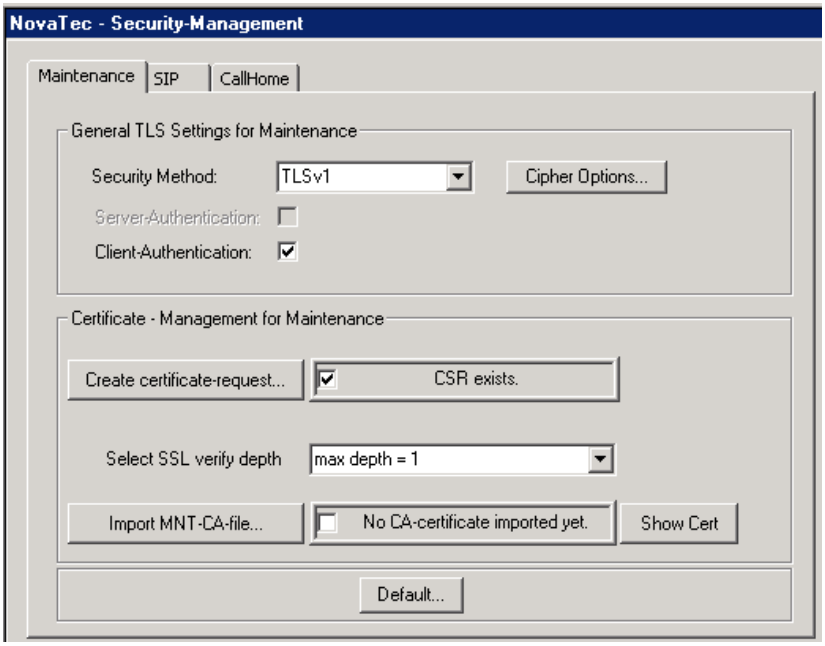


Abbildung 33 - CSR für MNT konfigurieren

Dagegen wird die CallHome-Verbindung vom Gateway initiiert. Dieses ist während des TLS-Verbindungsaufbaus der Client. Die Gegenstelle, der Server, sendet zwar immer im Rahmen des TLS-Protokolls sein Zertifikat an den Client, aber er prüft es nur, wenn das Feature „Server-Authentication" auf seiner Seite konfiguriert ist.

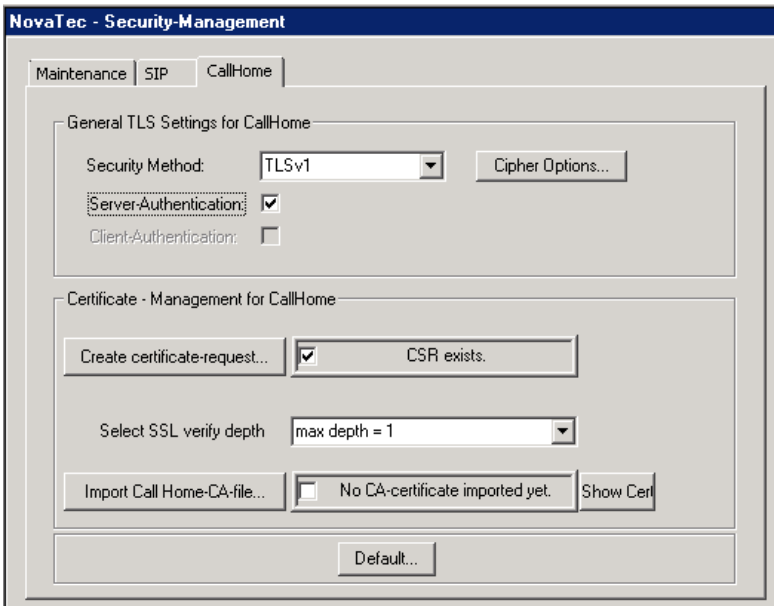


Abbildung 34 - CSR für NMS konfigurieren

- Es wird empfohlen die „Client-Authentication" und die „Server-Authetication" zu aktivieren, damit die Identität der TLS-Gegenstelle verifiziert werden kann, und somit eine höhere Sicherheit dieser Verbindung erreicht wird.

- „Create certificate-request…" Hier ist das Formular für den CSR-Inhalt auszufüllen. Es kann ein passendes „Challenge Password" eingetragen werden, wenn der MNT- bzw. NMS-CSR auf dem Gateway mit SCEP (z.B. Windows 2008 Server) signiert wird. Die anderen Angaben sind gemäß der für die Installation vereinbarten PKI-Vereinbarung oder nach freiem Wunsch zu machen.

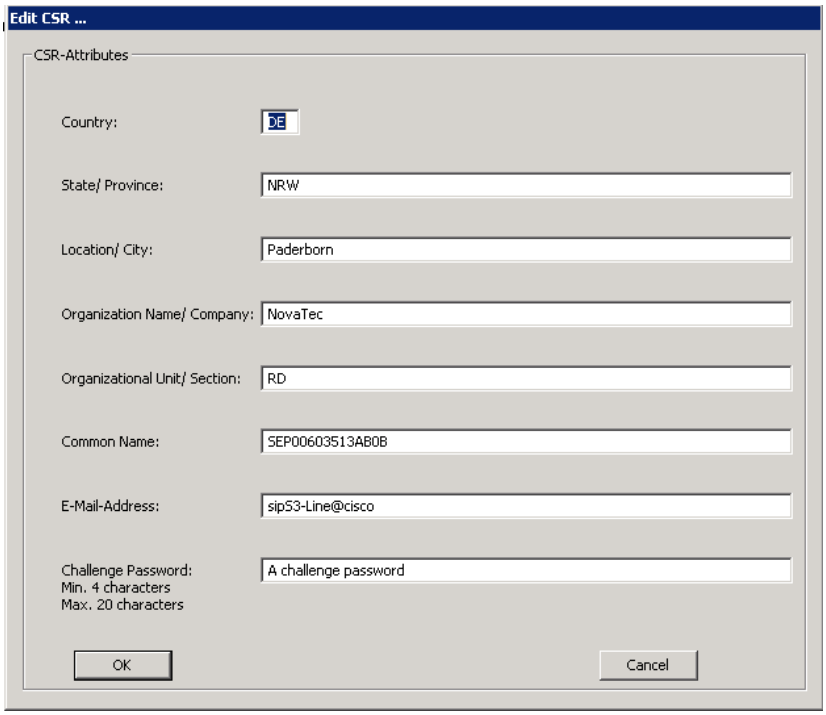


Abbildung 35 - MNT- / NMS-CSR Formular

- „Select SSL verify depth" Hier wird die Verifizierungstiefe der Zertifikatskette vorgegeben.
- „Import Call Home-CA-file…" Es können CA-Zertifikate in die Trust Liste des Gateways geladen werden. Der Inhalt der Zertifikate kann vor und nach dem Import angezeigt werden. Die Anzahl importierter CA-Zertifikate wird angezeigt. Das Gateway überprüft anhand dieser CA-Zertifikate die Identität der TLS-Gegenstelle für MNT- bzw. NMS-Verbindungen.

4.5.5 MNT- / NMS-CSR wird erzeugt

Nach einem Reset werden die konfigurierten Zertifikatsanträge im Gateway erzeugt.

4.5.6 TI-CA signiert MNT- bzw. NMS-Zertifikat

Wenn die TI-CA mit dem Gateway verbunden ist, kann diese den MNT- bzw. NMS-CSR einzeln auf dem Gateway signieren. Falls auch ein SIP-CSR angelegt worden ist, können diese drei CSR gemeinsam in einem Arbeitsgang signiert werden.

→ Folgen Sie den Schritten, die für den 3. und 4. Fall in Kapitel 5.1 „Signieren mit TI-CA" beschrieben sind. Wählen Sie dort unter Input „CSR from:"

- „mnt_req_csr from target", wenn nur der MNT-CSR signiert werden soll.
- „nms_req_csr from target", wenn nur der NMS-CSR signiert werden soll.
- „all requests from target", wenn alle im Gateway vorhandenen CSR (MNT, NMS & SIP), gemeinsam in einem Arbeitsgang signiert werden sollen.

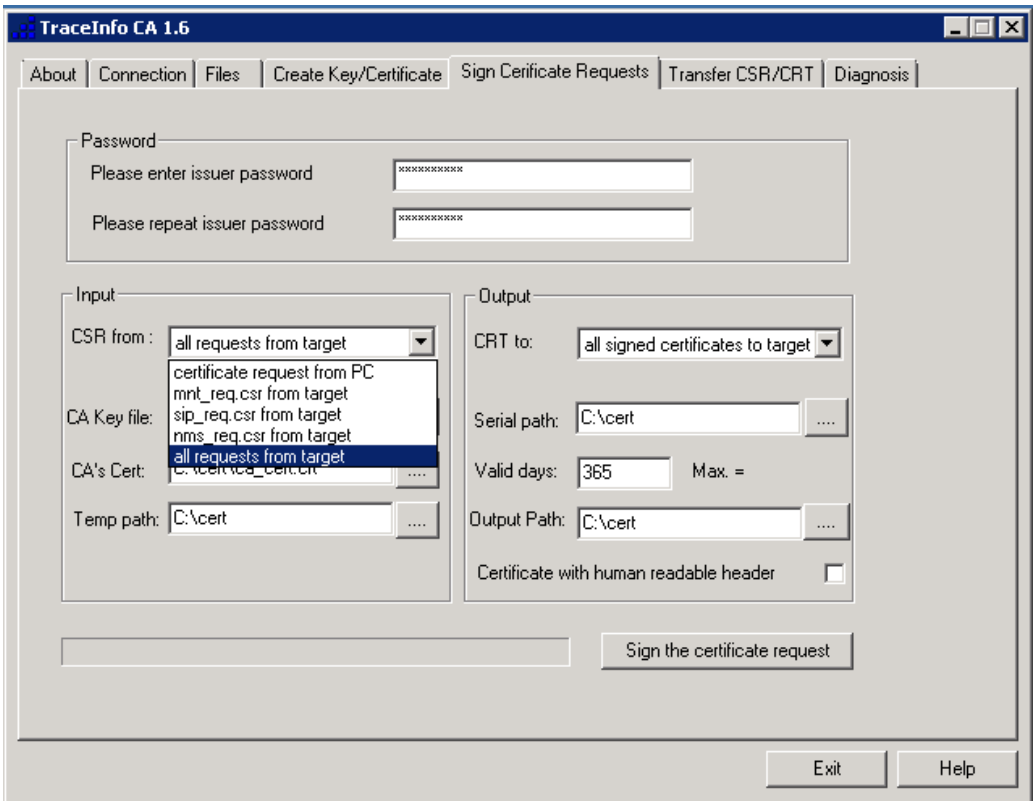


Abbildung 36 - Input: TI-CA signiert MNT- / NMS-CSR auf Gateway

Die Zieleinstellungen für den „Output" werden automatisch analog den Input Einstellungen gesetzt.

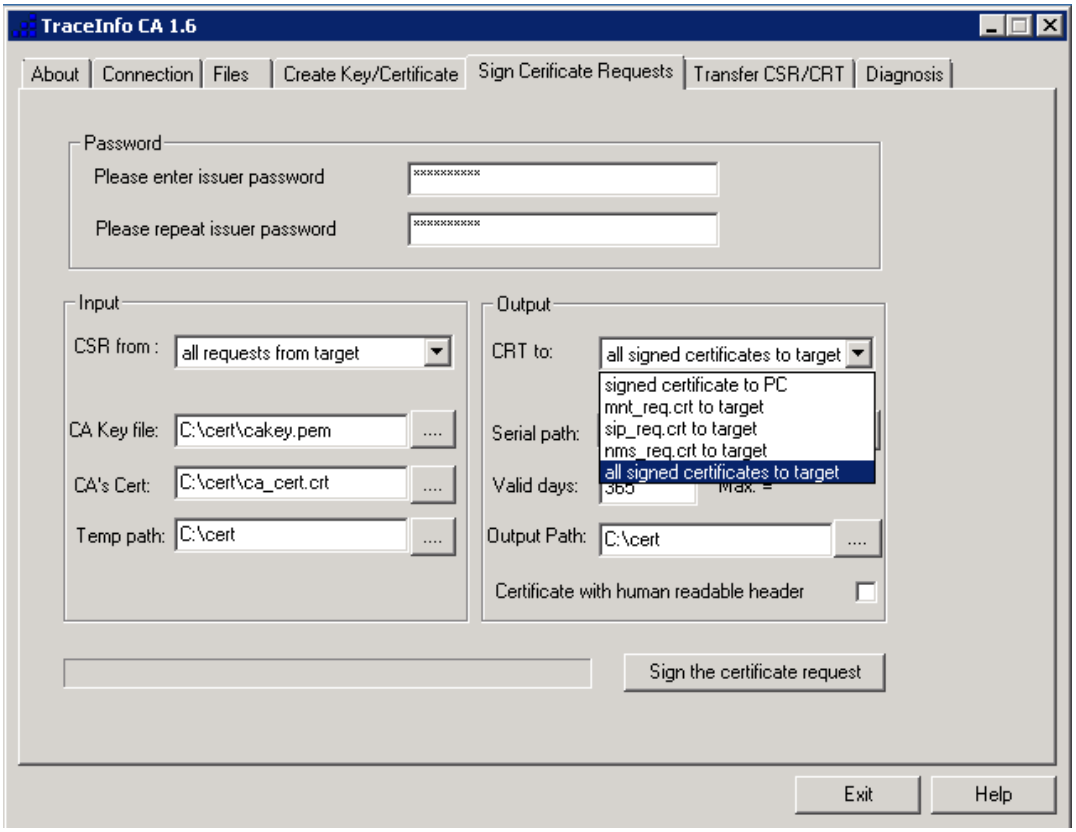


Abbildung 37 - Output: TI-CA signiert MNT- / NMS-CSR auf Gateway

4.5.7 Extern signierte MNT- & NMS-CRT in Gateway laden

Wenn die TI-CA mit dem Gateway verbunden ist, kann diese ein extern signiertes MNT- bzw. NMS-Zertifikat in ein NovaTec-Gateway laden.

Folgen Sie den Schritten in Kapitel 3.2.1.3 CSR extern signieren.

4.5.8 Reset ausführen

Nach einem Reset sind die Zertifikate auf dem Gateway aktiv.

4.5.9 MNT- & NMS-CRT auf der PC-Seite installieren

Die unter „TI-CA signiert MNT- & NMS-CSR Zertifikate werden auf der PC-Seite installiert. Zum Beispiel in einen NAMES SSL-Kontext geladen (siehe NAMES Handbuch) oder in der TI-CA bzw. im NovaTec Konfigurationsprogramm unter dem „Connection – Network Options" Menü importiert. Danach können durch TLS gesicherte Verbindungen zwischen NovaTec Gateways und NovaTec Applikationen genutzt werden.

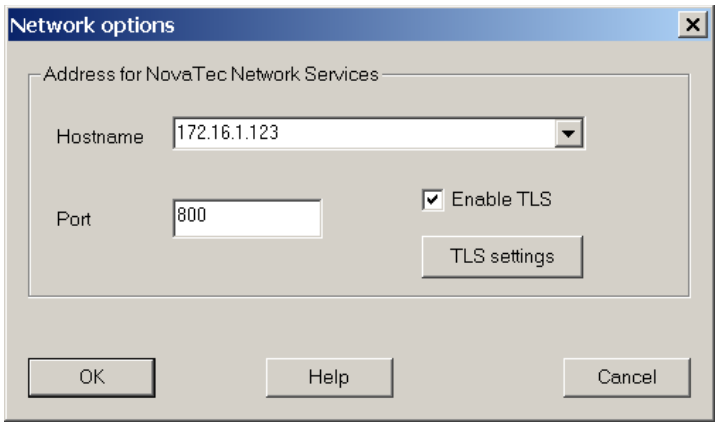


Abbildung 38 - TLS für MNT einschalten

Starten Sie die NovaTec Applikation auf einem PC, dessen Verbindung zu einem Gateway mit TLS gesichert werden soll.

- Im Fenster für die „Network options" geben Sie die IP-Adresse des Gateways an und schalten mit „Enable TLS" TLS aktiv.

Mit der Schaltfläche „TLS settings" wird das Fenster geöffnet, indem die für die TLS-Verbindung notwendigen Einstellungen getätigt werden.

- „Security Method:" auf „TLSv1" setzen.
- Die "Cipher Options…" können auf den Standardeinstellungen verbleiben.
- Empfohlen ist die Aktivierung der „Server-Authentication". Die PC-Applikation prüft dann das TLS-Zertifikat des Gateways und bestätigt dessen Identität.
- Mit „Import Private Key…" wird die private Schlüssel-Datei „mnt_key.pem" geladen, die die TI-CA zusammen mit der MNT-Zertifizierungsanforderung (CSR) angelegt hat.
- Mit „Import Public Key…" wird das signierte MNT-Zertifikat (CRT) importiert.
- Zuletzt wird unter „Import CA-file…" das CA-Zertifikat in die Trust Liste der Anwendung geladen, mit dem die TI-CA oder eine externe CA das MNT-Zertifikat signiert hat.
- Mit „OK" werden die Einstellungen bestätigt und aktiviert.

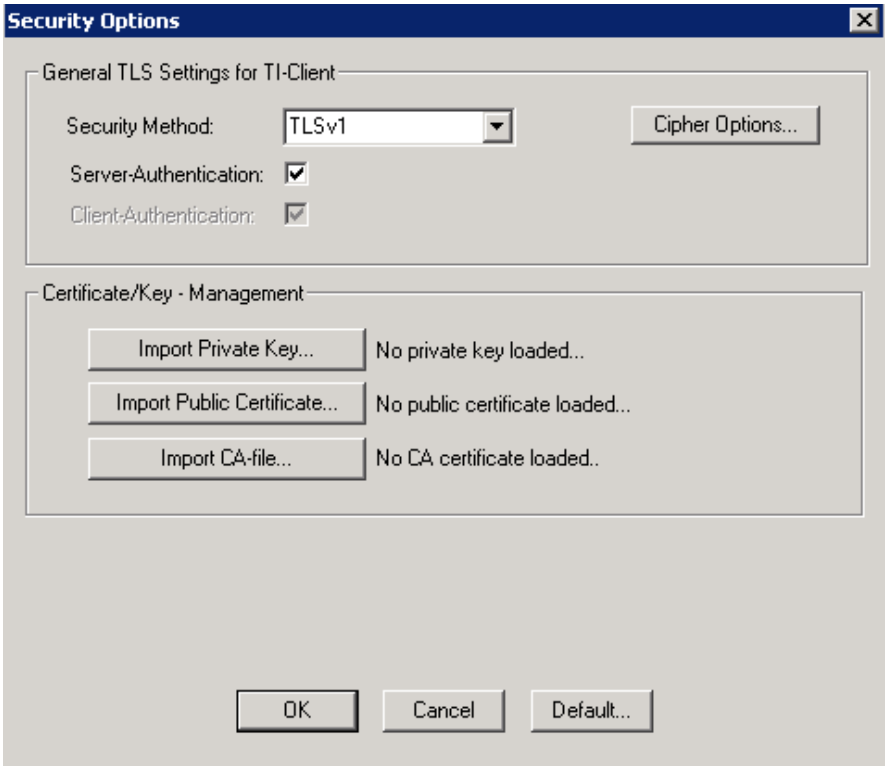


Abbildung 39 - TLS-Zertifikate für MNT laden

4.6 TLS und sRTP deaktivieren

4.6.1 Verschlüsselung für SIP und Wartung ausschalten

Gehen Sie auf NovaTec-System -> System IP options.

Wählen Sie "Disable Security …" und bestätigen Sie die angezeigten Fenster. Im Baum auf der linken Seite wird nun der Knotenpunkt „TLS security" unter „System IP options" entfernt.

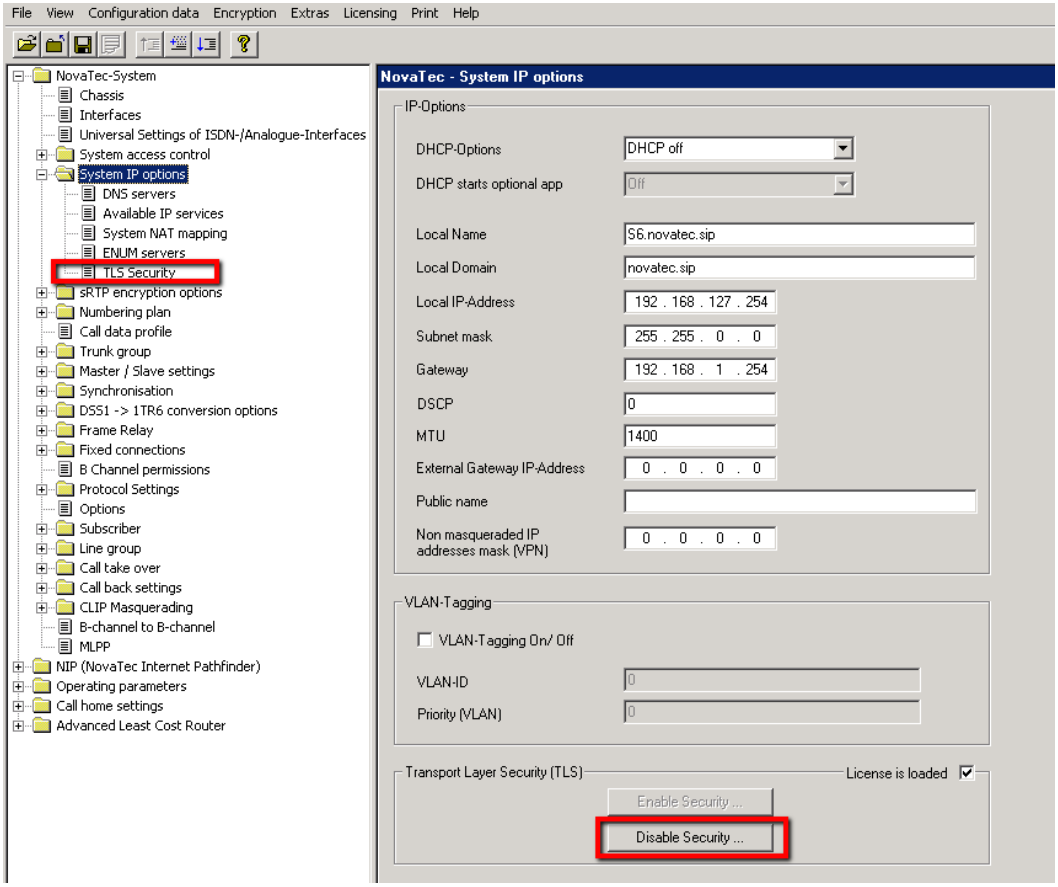


Abbildung 40 - TLS in Konfiguration deaktivieren

4.6.2 Ändern des IP-Transport-Services

Nun wird das Übertragungsprotokoll TCP für TLS ausgeschaltet und UDP aktiviert.

Die Umschaltung auf SIP-UDP erfolgt ab Version 6.6 automatisch, für eine ältere Version sollten die folgenden Schritte durchgeführt werden:

- Gehen Sie auf NovaTec-System -> System IP options -> Available IP services.
- Doppel-klicken Sie auf TLS-SIP Dienst (Bezeichnung kann abweichen) und nehmen Sie das Häkchen bei "Activate service" raus.
- Bestätigen Sie mit "OK".

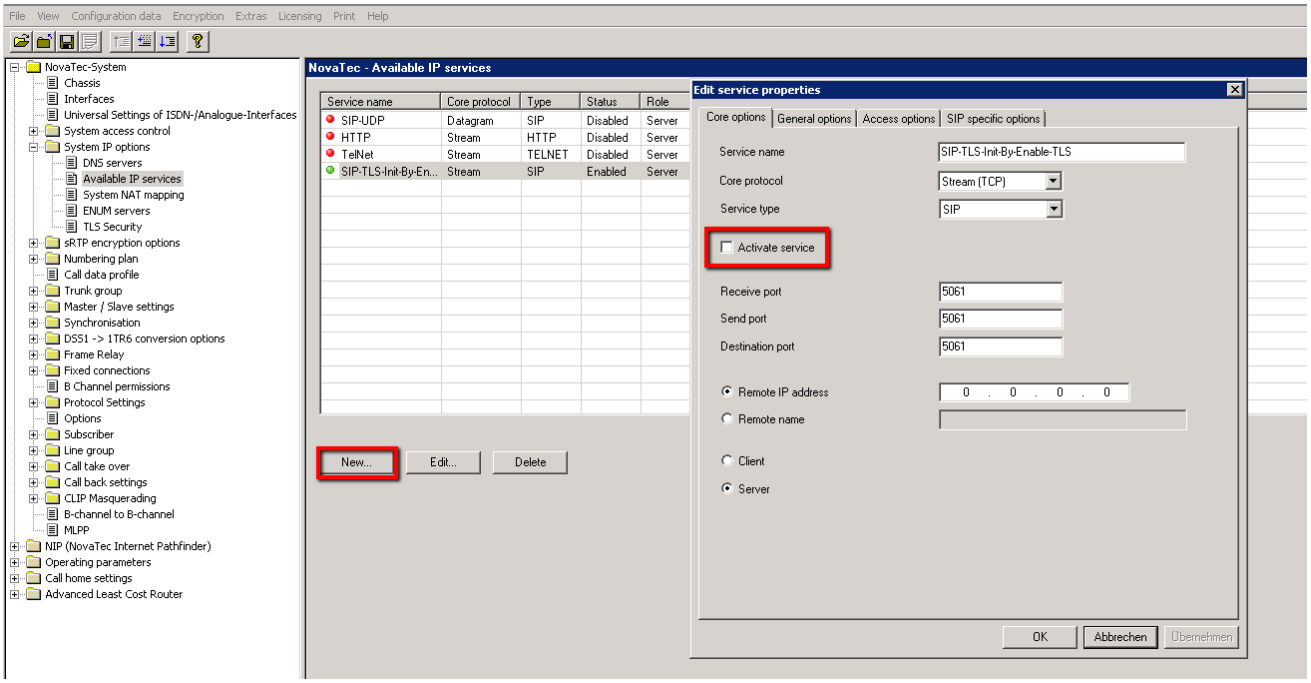


Abbildung 41 - Ungesicherten IP-Service prüfen

- Wenn dort kein UDP-Dienst aktiviert ist, doppel-klicken Sie den Eintrag und setzten Sie das Häkchen bei "Activate service".
- Wenn kein UDP-Dienst verfügbar ist, betätigen Sie den Button "New…", um diesen Dienst für SIP einzurichten.
- Geben Sie einen Namen für den Service ein und wählen Sie "Datagram (UDP)" als neues IP-Protokol.

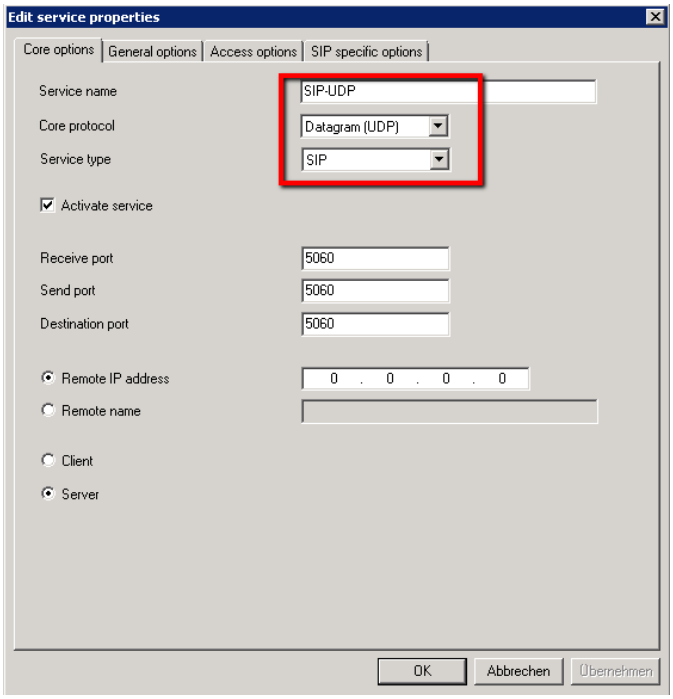


Abbildung 42 - UDP Dienst für SIP einrichten

- Im Reiter "Access options" nehmen Sie das Häkchen bei "Activate authorization" heraus.

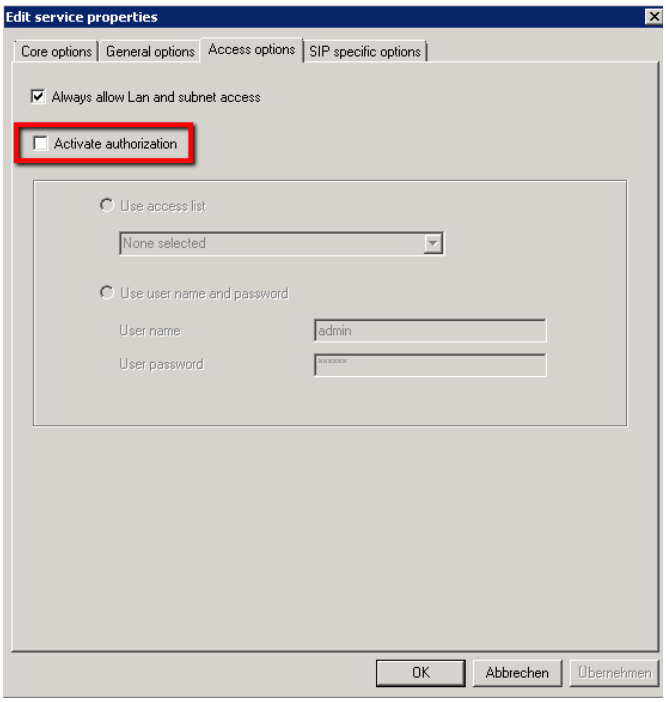


Abbildung 43 - Access Options

- Wählen Sie im Reiter “SIP specific options” den “Session Owner”-Namen frei aus.

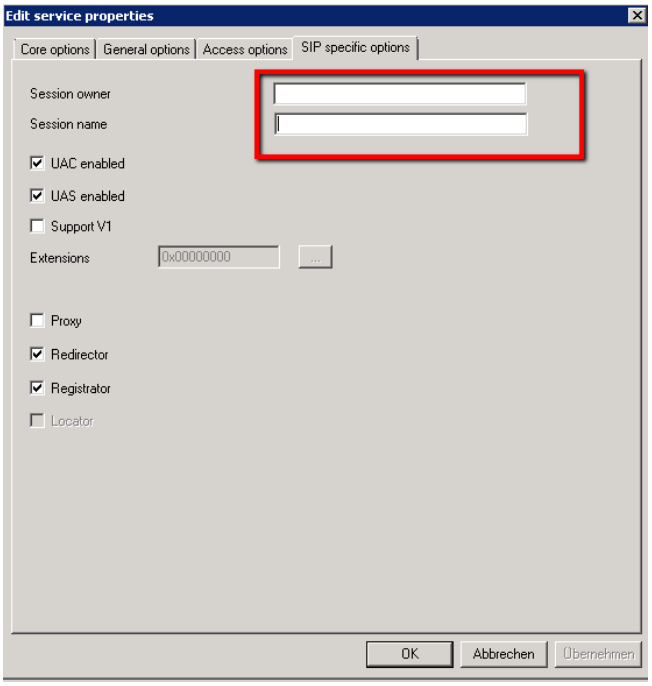


Abbildung 44 - SIP Session Owner

Das neue ungesicherte Übertragungsprotokoll ist nun eingerichtet.

4.6.3 TLS-Ports entfernen und von sRTP zu RTP wechseln

- Gehen Sie nun zu „NIP" → „SIP" → „Mapping lists" → „User mapping".
- In dem „URI/Name/IP"-Feld entfernen Sie TLS-Port „:5061".
- Um sRTP zu deaktivieren, bestätigen Sie "Do not use" für "Encryption setting".

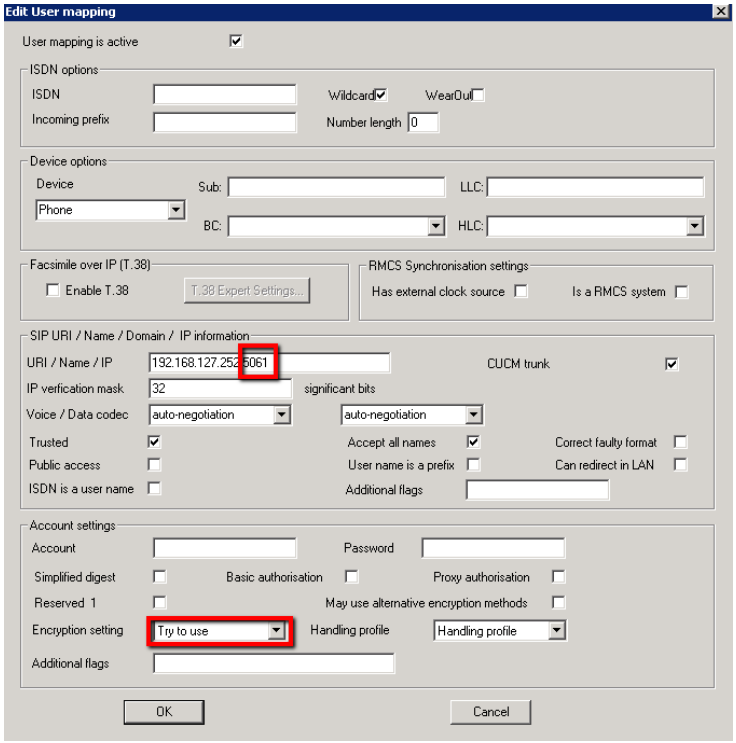


Abbildung 45 - User Mapping sRTP deaktivieren

- Gehen Sie jetzt auf „NIP" → „SIP" → „Mapping lists" → „Local mapping".
- Im „Registrar"-Feld entfernen Sie bitte den TLS-Port „:5061".

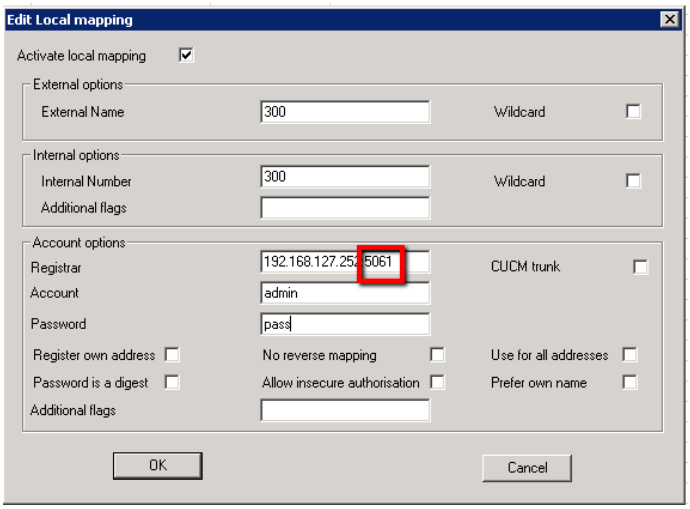


Abbildung 46 - Local mapping

5 Zertifikate erstellen

Mit dem Neustart des NovaTec-Systems werden für jede der drei Instanzen, falls konfiguriert, Zertifizierungsanforderungen (Certificate Signing Request - CSR) im System erstellt. Diese kann von einer Zertifizierungsstelle (CA) signiert werden. Man erhält das gewünschte TLS-Zertifikat. Als Registrierungsstelle kann TI-CA, ein Windows Server mit SCEP oder NAMES eingesetzt werden.

5.1 Signieren mit TI-CA

Mit der TI-CA können Zertifizierungsanforderungen (CSR-Dateien) zu Zertifikaten signiert werden.

Lokal auf einem PC gespeicherte CSR-Dateien können signiert werden. Auch kann die TI-CA das Signieren von CSR-Dateien direkt auf einem NovaTec-System durchführen.

1. Fall – Die CSR liegt lokal auf dem PC vor und das Zertifikat wird auch lokal gespeichert.
2. Fall – Die CSR von einem NovaTec System liegt lokal vor, das signierte Zertifikat wird anschließend auf das entsprechende NovaTec-System zurückgeschrieben.
3. Fall – Die CSR befindet sich auf einem NovaTec-System, das signierte Zertifikat wird dorthin zurückgeschrieben.
4. Fall – Wie 3. Fall, nur werden die CSR der drei Instanzen (MNT, SIP, NMS) auf einem System zusammen signiert.

- Starten Sie die TI-CA Anwendung.
- Falls dieses Fenster eingeblendet wird, fehlt der USB-Dongle, der die TI-CA Anwendung freischaltet.

Abbildung 47 - TI-CA ohne Dongle gestartet

- Nur im 1. Fall ist keine online Verbindung zu einem NovaTec-System notwendig.
- In den anderen Fällen, wenn sich, vor dem Signieren der CSR oder nach der Signierung, das ausgestellte Zertifikat auf einem NovaTec-System befindet, bauen Sie mit der TI-CA eine Verbindung zum Zielsystem auf. Tragen Sie unter dem Reiter „Connection" → „Settings" die IP-Adresse des Zielsystems ein.
- Anschließend bauen Sie die Verbindung mit „Connect" auf. Eventuell müssen Sie unter „Username" und „Password", die von Ihnen gewählten Zugangsdaten eintragen.

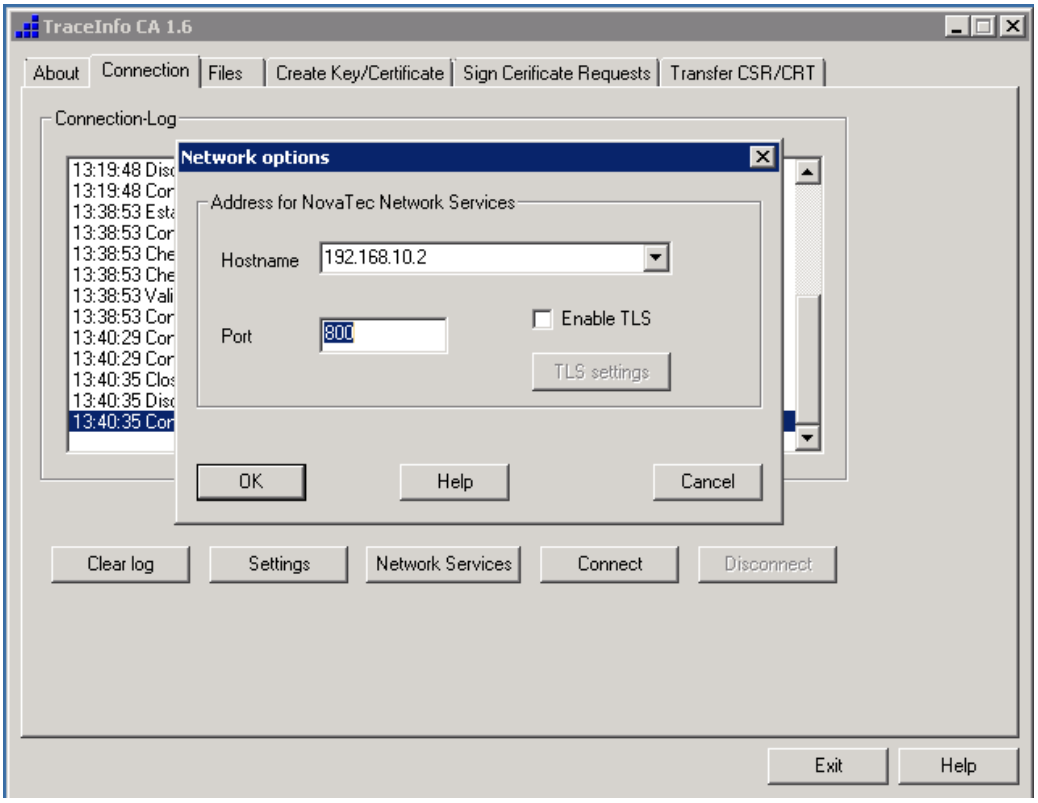


Abbildung 48 - Zielsystem adressieren

- Alle weiteren Einstellungen für das Signieren mit der TI-CA sind auf dem Reiter „Sign Certificate Requests" vorzunehmen.
- Geben Sie dort das CA Passwort ein, welches mit dem „CA private key" (cakey.pem) verknüpft ist.
- Wiederholen Sie die Passworteingabe. Sollte dieser Schritt fehlschlagen, erscheint eine Fehlermeldung in der unteren Zeile und der Button "Sign the certificate request" wird deaktiviert.
- Die weitere Eingabemaske ist links in die „Input" Box und rechts in die „Output" Box gegliedert. Unter „Input" werden die Daten des CSR eingeben sowie der Speicherort des CA Zertifikats und der zugehörigen privaten Schlüsseldatei. Unter „Output" werden die Daten eingestellt, die das auszustellende Zertifikat betreffen.

Zum 1. Fall) Der lokal vorliegende und zu signierende CSR, muss nicht mit TI-CA angelegt worden sein. Auch von externen Anwendungen erstellte Zertifizierungsanforderungen können auf diese Weise signiert werden.

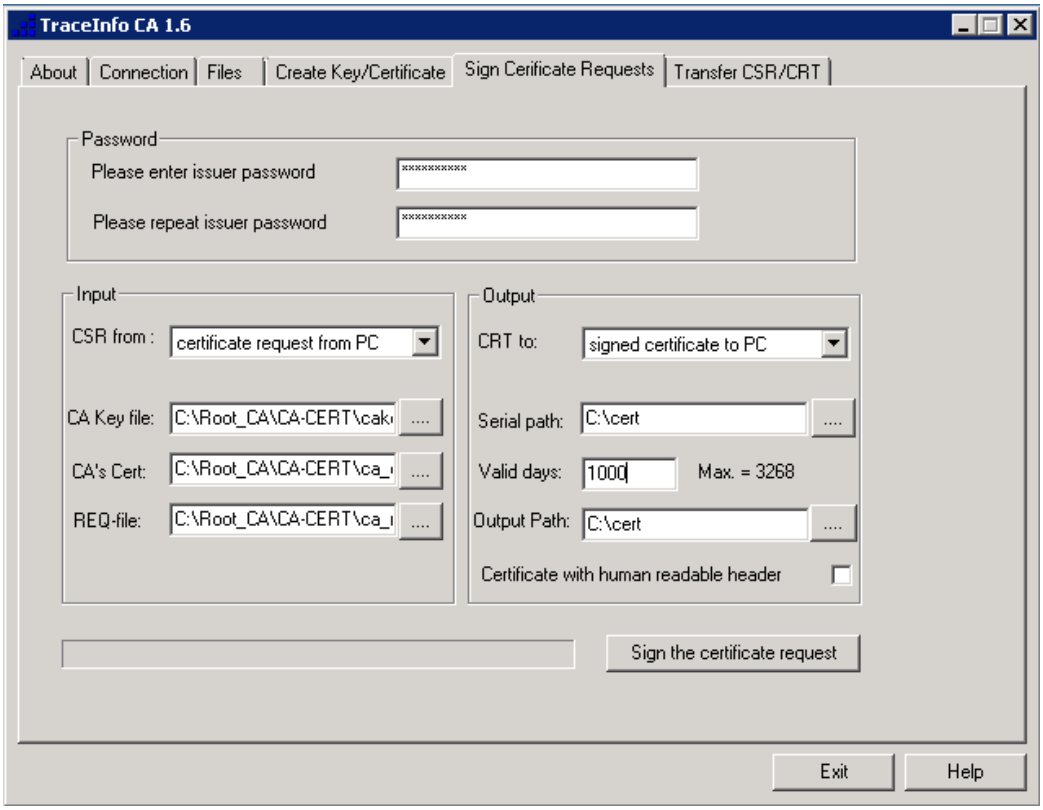


Abbildung 49 - TI-CA Sign Certificate Requests PC-to-PC

- In der Inputbox wählen Sie bitte folgendes aus:

  - Wählen Sie unter „CSR from:" „certificate request from PC" aus.
  - Wählen Sie für „CA Private Key" die private Schlüssel-Datei aus.
  - Wählen Sie das CA Zertifikat.
  - Unter „REQ-file" wählen Sie die Zertifizierungsanforderungs-Datei (hier: „Beispiel.csr") aus.

- In der Outputbox wählen Sie bitte folgendes aus:

  - Wählen Sie unter "CRT to:" "signed certificate to PC" aus.
  - Geben Sie den Pfad für die Seriennummer-Datei an.(1)
  - Geben Sie unter „Valid days" die Gültigkeit des Root-Zertifikates in Tagen an.
  - Geben Sie unter „Output Path" den lokalen Zielordner für die Sicherung der signierten Zertifikatsdatei an.

- Bitte deaktivieren Sie “Certificate with human readable header”.

- Wenn Sie die Einstellungen wie oben Beschrieben vorgenommen haben, drücken Sie den Button "Sign the certificate request".

Nachdem die CSR signiert wurde, befindet sich das Zertifikat „Beispiel.crt“ im angegebenen Zielordner.

Hinweis (1):

Die Seriennummer wird in einer Datei namens serial.txt gesichert. Wenn diese im angegebenen Pfad nicht auffindbar ist wird die Applikation eine neue Datei mit einer Default-Startnummer anlegen. Der Nutzer kann die Startnummer selbst bestimmen indem er eine Datei serial.txt mit einer 16-stelligen Hexadezimalzahl, z.B. 0123456789ABCDEF, anlegt. Die Applikation wird die aktuell in der serial.txt-Datei hinterlegte Seriennummer verwenden. Nachdem die aktuelle Seriennummer verwendet wurde, wird die Applikation die serial.txt-Datei hochzählen.

Zum 2.Fall) Die CSR von einem NovaTec System liegt lokal vor, das signierte Zertifikat wird anschließend auf das entsprechende NovaTec-System zurück-geschrieben. Diese Option bietet die TI-CA – allerdings z.Z. ohne praktische Anwendung.

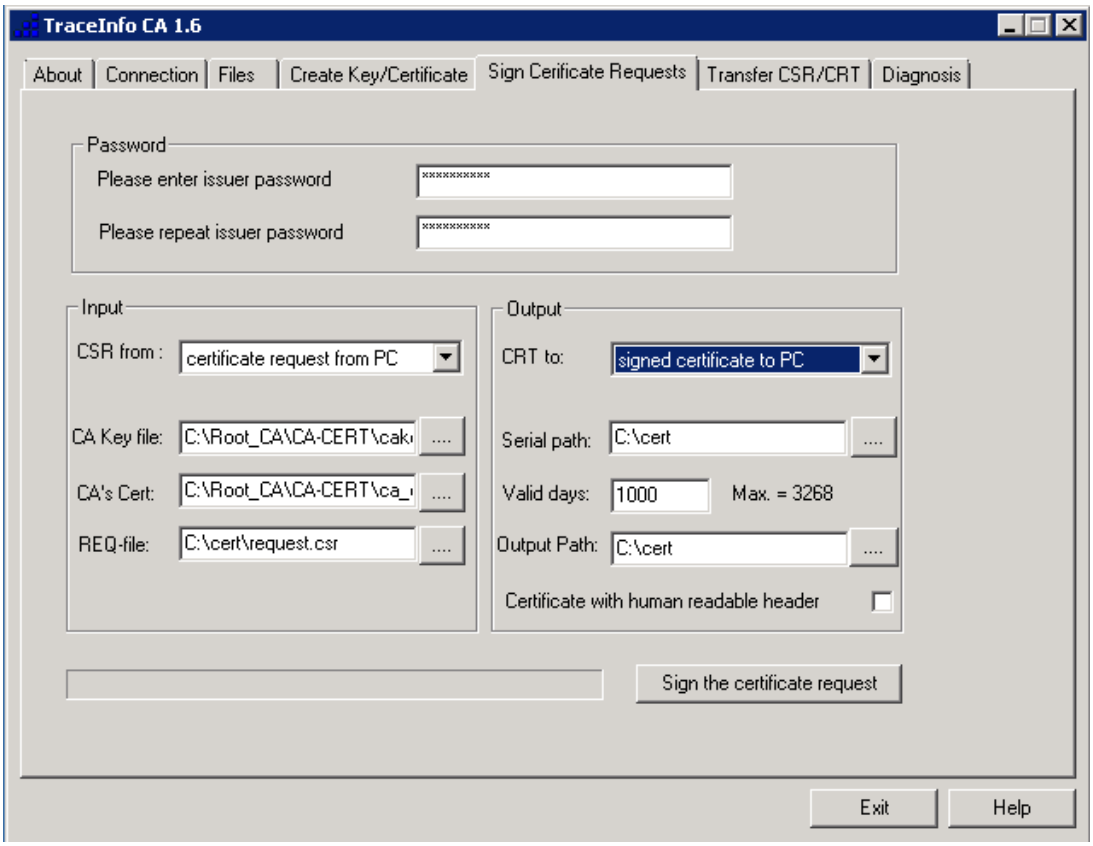


Abbildung 50 - TI-CA Sign Certificate Requests PC-to-Target

- Verbinden Sie die TI-CA mit dem Zielsystem. Tragen Sie unter dem Reiter „Connection" → „Settings" die IP-Adresse des Zielsystems ein (siehe Abbildung 48 - Zielsystem adressieren).
- Alle weiteren Einstellungen für das Signieren mit der TI-CA sind auf dem Reiter „Sign Certificate Requests" vorzunehmen.
- Geben Sie dort das CA Passwort ein, welches mit dem „CA private key" (cakey.pem) verknüpft ist.
- Wiederholen Sie die Passworteingabe. Sollte dieser Schritt fehlschlagen, erscheint eine Fehlermeldung in der unteren Zeile und der Button "Sign the certificate request" wird deaktiviert.

- In der Inputbox wählen Sie bitte folgendes aus:

- Wählen Sie unter „CSR from:" „certificate request from PC" aus.
- Wählen Sie für „CA Private Key" die private Schlüssel-Datei aus.
- Wählen Sie das CA Zertifikat.
- Unter „REQ-file" wählen Sie die Zertifikatsanfrage-Datei (Bsp: „sip_req.csr") aus.

- In der Outputbox wählen Sie bitte folgendes aus:

  - Wählen Sie unter "CRT to:" beispielsweise für SIP "sip_req.crt to target" aus.
  - Geben Sie den Pfad für die Seriennummer-Datei an.(1)
  - Geben Sie unter „Valid days" die Gültigkeit des Root-Zertifikates in Tagen an.
  - Geben Sie unter „Output Path" den lokalen Zielordner für die temporäre Sicherung der signierten Zertifikatsdatei an. Diese wird auf das Zielsystem übertragen und danach lokal gelöscht.
  - Bitte deaktivieren Sie "Certificate with human readable header".
  - Wenn Sie die Einstellungen wie oben Beschrieben vorgenommen haben, drücken Sie den Button "Sign the certificate request".

Nachdem die Zertifizierungsanforderung (CSR) signiert wurde, wird das hier als Beispiel verwendete SIP-Zertifikat „sip_req.crt" in das Zielsystem geschrieben.

Hinweis (1):

Die Seriennummer wird in einer Datei namens serial.txt gesichert. Wenn diese im angegebenen Pfad nicht auffindbar ist, wird die Applikation eine neue Datei mit einer Default-Startnummer anlegen. Der Nutzer kann die Startnummer selbst bestimmen indem er eine Datei serial.txt mit einer 16-stelligen Hexadezimalzahl, z.B. 0123456789ABCDEF, anlegt. Die Applikation wird die aktuell in der serial.txt-Datei hinterlegte Seriennummer verwenden. Nachdem die aktuelle Seriennummer verwendet wurde, wird die Applikation die serial.txt-Datei hochzählen.

Zum 3. und 4. Fall) Diese beiden Fälle können zusammen behandelt werden. Der einzige Unterschied besteht darin, dass im 3. Fall ein CSR, und im 4. Fall mehrere CSR zusammen in einem Durchlauf signiert werden. Die CSR-Dateien liegen auf einem NovaTec Gateway vor. Auch die ausgestellten Zertifikate werden nach dem Signieren auf diesem NovaTec-System abgelegt.

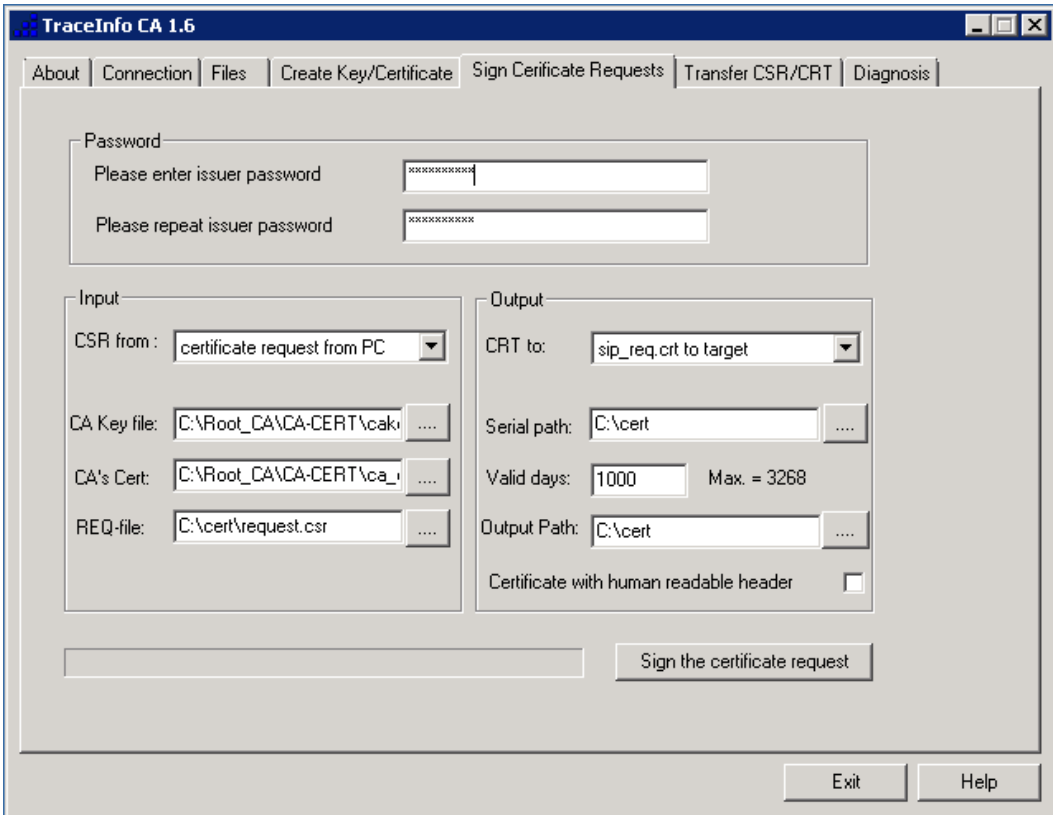


Abbildung 51 - TI-CA Sign Certificate Requests PC-to-Target

- Verbinden Sie die TI-CA mit dem Zielsystem. Tragen Sie unter dem Reiter „Connection" → „Settings" die IP-Adresse des Zielsystems ein (siehe Abbildung 48 - Zielsystem adressieren).
- Alle weiteren Einstellungen für das Signieren mit der TI-CA sind auf dem Reiter „Sign Certificate Requests" vorzunehmen.
- Geben Sie dort das CA Passwort ein, welches mit dem „CA private key" (cakey.pem) verknüpft ist.
- Wiederholen Sie die Passworteingabe. Sollte dieser Schritt fehlschlagen, erscheint eine Fehlermeldung in der unteren Zeile und der Button "Sign the certificate request" wird deaktiviert.

- In der Inputbox wählen Sie bitte folgendes aus:

- Wählen Sie unter „CSR from:" „certificate request from PC" aus.
- Wählen Sie für „CA Private Key" die private Schlüssel-Datei aus.
- Wählen Sie das CA Zertifikat.
- Unter „REQ-file" wählen Sie die Zertifizierungsanforderungs-Datei (Bsp: „sip_req.csr") aus.

- In der Outputbox wählen Sie bitte folgendes aus:

  - Wählen Sie unter "CRT to:" beispielsweise für SIP "sip_req.crt to target" aus.
  - Geben Sie den Pfad für die Seriennummer-Datei an.(1)
  - Geben Sie unter „Valid days" die Gültigkeit des Root-Zertifikates in Tagen an.
  - Geben Sie unter „Output Path" den lokalen Zielordner für die temporäre Sicherung der signierten Zertifikatsdatei an. Diese wird auf das Zielsystem übertragen und danach lokal gelöscht.
  - Bitte deaktivieren Sie "Certificate with human readable header".
  - Wenn Sie die Einstellungen wie oben Beschrieben vorgenommen haben, drücken Sie den Button "Sign the certificate request".

Nachdem die CSR signiert wurde, wird das hier als Beispiel verwendete SIP-Zertifikat „sip_req.crt" in das Zielsystem geschrieben.

Hinweis (1):

Die Seriennummer wird in einer Datei namens serial.txt gesichert. Wenn diese im angegebenen Pfad nicht auffindbar ist, wird die Applikation eine neue Datei mit einer Default-Startnummer anlegen. Der Nutzer kann die Startnummer selbst bestimmen indem er eine Datei serial.txt mit einer 16-stelligen Hexadezimalzahl, z.B. 0123456789ABCDEF, anlegt. Die Applikation wird die aktuell in der serial.txt-Datei hinterlegte Seriennummer verwenden. Nachdem die aktuelle Seriennummer verwendet wurde, wird die Applikation die serial.txt-Datei hochzählen.

5.2 Ablauf der Signierung mit SCEP

Die folgenden 8 Schritte werden während der Konfiguration von SCEP und der anschließenden Signierung mit SCEP durchlaufen:

1. Schritt: Public Zertifikate für alle drei Instanzen in die Konfiguration importieren.
2. Schritt: Enrollment und Encryption Zertifikat in die Konfiguration importieren.
3. Schritt: (Optional) „One Time Password" aus Web Browser in die Konfiguration importieren.
4. Schritt: Upload der Konfiguration auf die NovaTec Systeme mit Reset.
5. Schritt: SCEP Enrollment mit automatischem Reset.

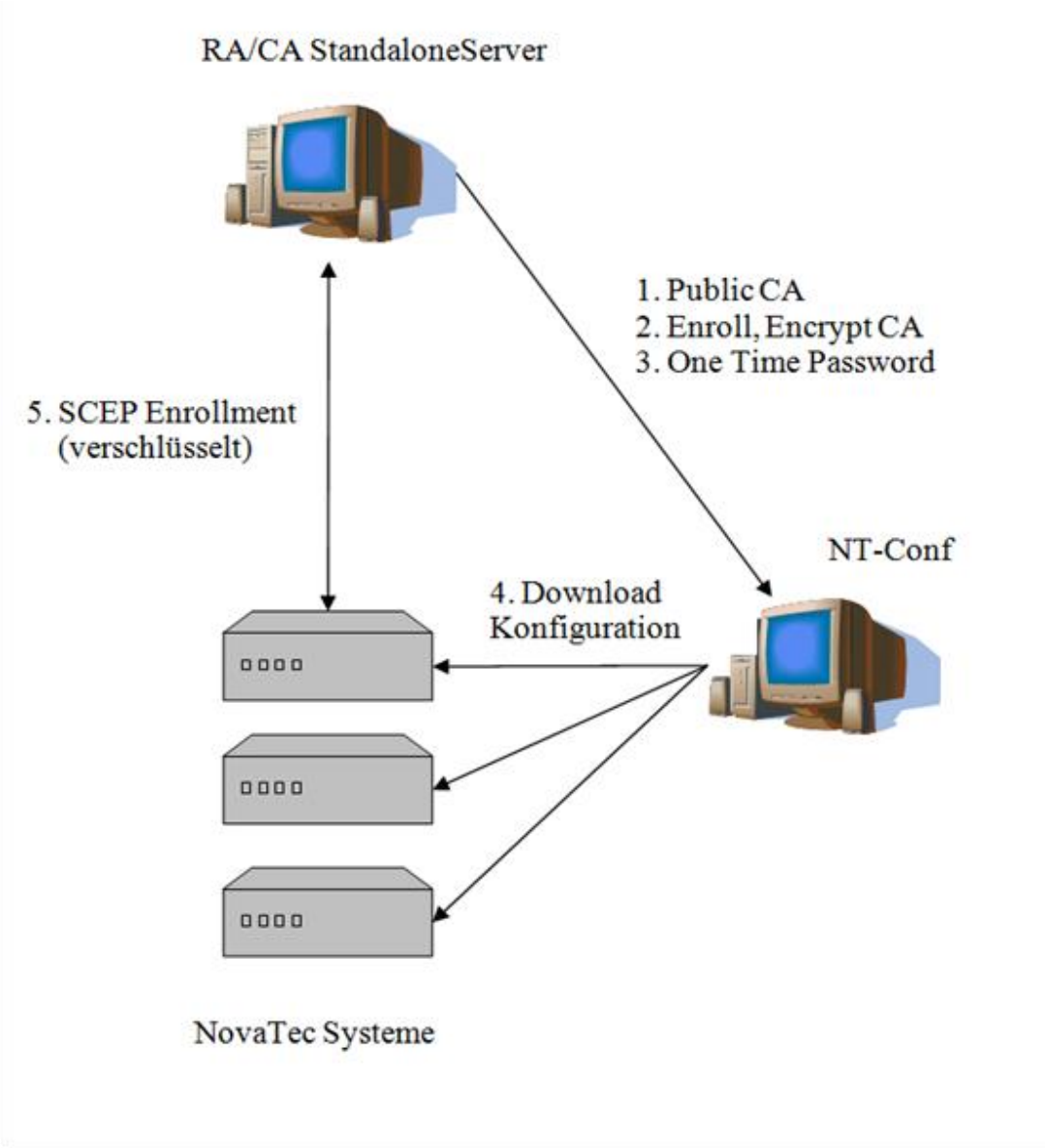


Abbildung 52 - SCEP Enrollment NovaTec Gateways

Nachdem jetzt die TLS-Zertifikate auf den NovaTec Gateways signiert sind und die für die Verifizierung der PKI-Kette notwendigen Zertifikate (hier nur das Public CA) in diese importiert sind, müssen auch der CallServer und die Workstation, mit der die Gateways überwacht werden, mit der vollständigen Zertifikatskette versorgt werden. Außerdem wird auf der Workstation durch die TI-CA das TLS-Zertifikat für NMT und NMS signiert.

6. Schritt: Public CA Zertifikat in den CallServer importieren (Bsp. CUCM, siehe Kapitel 6.3 Zertifikate Im- & Exportieren).
7. Schritt: Mit dem TI_CA aus Public CA Certifikat die NMT und NMS Zertifikate erzeugen (siehe 5.1).
8. Schritt: Funktionstest NMT, NMS und SIP mit TLS.

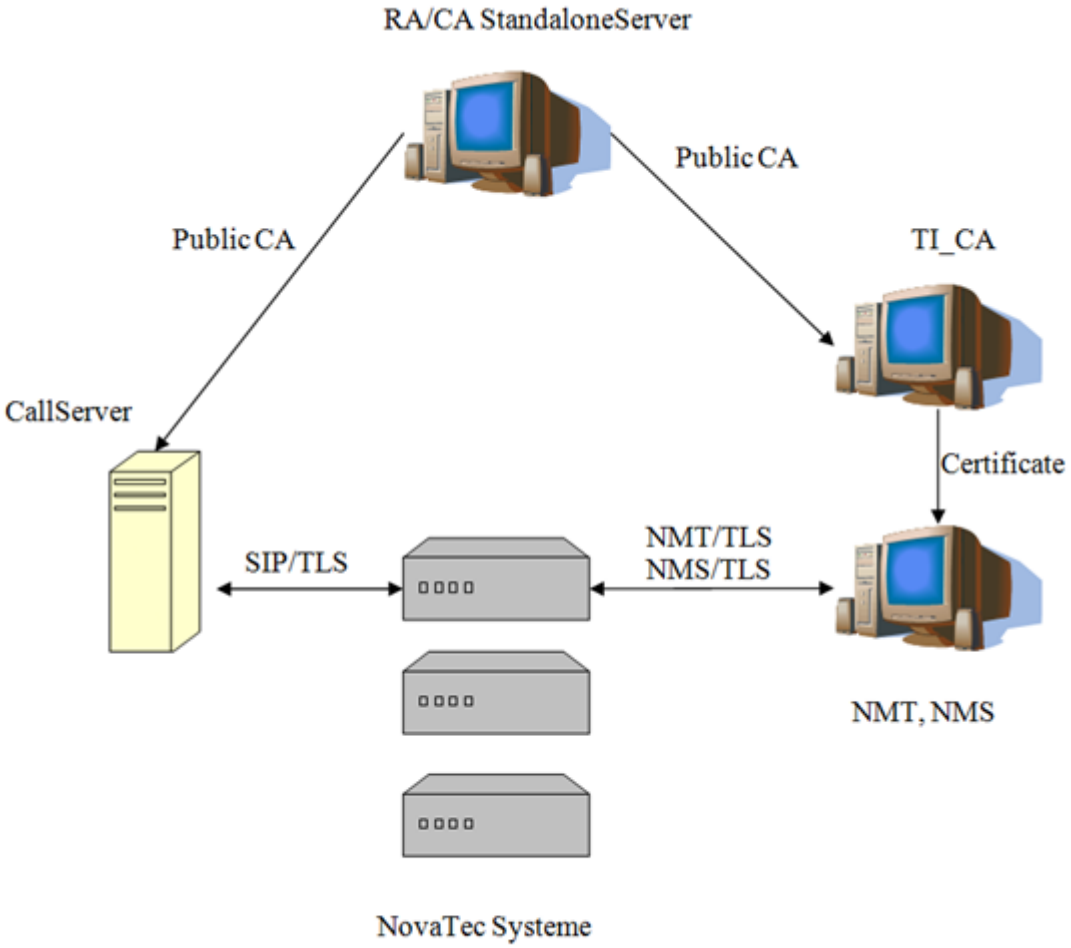


Abbildung 53 - SCEP Enrollment CallServer & NovaTec Management PC

5.3 Systeme mit NAMES signieren

Führen Sie die im NAMES Benutzerhandbuch aufgeführten Konfigurationsschritte aus. Danach kann NAMES das Signieren der Zertifikate automatisiert durchführen. Es werden alle 3 CSR Dateien auf den Gateways signiert, die vorher durch deren Konfiguration bestimmt angelegt worden sind.

6 Gesicherte Verbindungen im CUCM konfigurieren

Damit zwischen NovaTec Gateways und dem CISCO Call Manager mit TLS und sRTP gesicherte Verbindungen aufgebaut werden können, muss der Cisco Unified Communication Manager (CUCM)-Cluster-Sicherheits-Modus auf „mixed mode" gesetzt werden. Als Voraussetzung muss der CISCO CTL Client installiert werden, der eine Liste von Zertifikaten (Certificate Trust List) im CUCM erstellt. Es werden zwei Cisco Security Dongle/Token und deren Passwörter benötigt. Verbinden Sie diese Dongle nur auf Anforderung mit einem USB-Port.

Für detaillierte Informationen sondieren Sie bitte die CUCM Hilfeseiten oder Sie folgen der Kurzanleitung im nächsten Abschnitt.

6.1 CISCO CTL Client installieren

Führen Sie folgende Schritte aus um den Cisco CTL Client zu installieren:

1. Öffnen Sie die Cisco Unified Communications Manager Administration, wie im Cisco Unified Communications Manager Administration Guide beschrieben, auf einem Windows PC oder einem Windows Server, auf dem Sie den Client installieren möchten.

2. Wählen Sie im Cisco Unified Communications Manager Administration folgendes aus: "Application > Plugins**"**. Der "Find and List"-Plugin wird angezeigt.

3. In der Suche des Drop-Down-Menüs des Plugins „Installation" eingeben und „Find" anklicken.

4. Lokalisieren Sie den Cisco CTL Client.

5. Um die Datei herunterzuladen, drücken Sie auf „Download" rechts im Fenster in Höhe des Cisco-CTL-Client-Plugins.

6. Wählen Sie „Speichern" und geben Sie einen Pfad an. Merken Sie sich diesen.

7. Gehen Sie sicher, dass der Sicherheitsagent ausgeschaltet ist. Z.B.: Es läuft kein Unternehmens Sicherheitsagent auf diesem Server.

8. Um mit der Installation zu beginnen, doppel-klicken Sie „Cisco CTL Client" (Icon oder ausführbare Datei, je nachdem, wo der Download gespeichert wurde). Hinweis: Sie können auch über "Öffnen" in der "Download komplett"-Meldung gehen.

9. Die Version des Cisco CTL Clients wird angezeigt; drücken Sie den Button „Weiter".

10. Der Installations-Agent wird angezeigt. Drücken Sie auf „Weiter".

11. Nehmen Sie die Lizenzvereinbarung an und klicken Sie auf "Weiter".

12. Wählen Sie ein Verzeichnis, in das Sie den Client installieren wollen. Um die Defaulteinstellung zu ändern, wählen Sie „durchsuchen". Nachdem Sie den Installationsort gewählt haben, klicken Sie „Weiter".

13. Klicken Sie auf "Weiter", um mit der Installation zu beginnen.

14. Wenn die Installation komplett ist, drücken Sie auf "Fertig stellen".

Bitte überprüfen Sie folgende Punkte, bevor Sie beginnen den CTL Client mit dem CUCM zu verbinden:

1. Gehen Sie auf Cisco Unified Serviceability → Tools → Service Activation und versichern Sie sich, dass folgende Dienste aktiv sind:

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

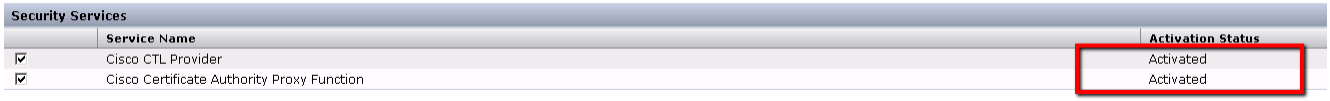


Abbildung 54 - CTL Provider Activated

2. Gehen Sie auf die CUCM Admin Seite → System → Service Parameter Configuration

   - Wählen Sie als Server den passenden CUCM aus.
   - Wählen Sie als Service den „Cisco CTL Provider Service".
   - Die Portnummer muss 2444 sein.

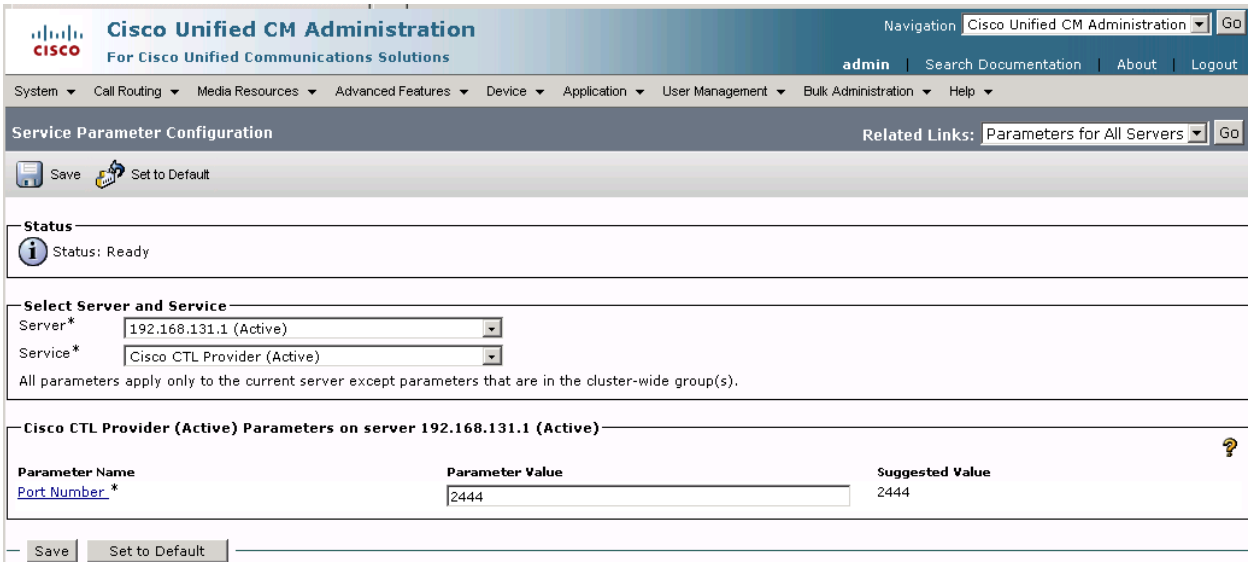


Abbildung 55 - CTL Service Parameter

Sicherheitszertifikate zum CUCM hinzufügen und den "Mixed Mode" freischalten

1. Starten Sie den CTL Client.

Abbildung 56 – CTL Client connect

- Benutzen Sie möglichst nicht den DNS-Namen des CUCM, sondern ausschließlich dessen IP-Adresse.
- Der Default-Port sollte 2444 sein.
- Username und Passwort sind CUCM Username und Passwort.

2. Der CTL-Client wird den User bestätigen und sich mit dem CUCM verbinden.
3. Die abgebildete Meldung wird angezeigt. An diesem Punkt wählen Sie bitte "Set Cisco Unified CallManger Cluster to Mixed Mode". Drücken Sie auf "Next" (Weiter).

Abbildung 57 - CTL Mixed Mode

4. Der CTL-Client wird Sie zum Hinzufügen eines Sicherheitsnachweises auffordern. Bitte schließen Sie nun den Dongle am USB-Port des PC/Servers an, auf dem aktuell der CTL-Client installiert wird.

5. Der CTL-Client wird nun das Passwort für den Dongle abfragen. Benutzen Sie das Passwort (z.B. "Cisco_xyz") auf dem Aufkleber. Seien Sie bei der Passworteingabe besonders aufmerksam, da zwei falsche Eingaben den Dongle unbrauchbar machen!

6. Wenn Sie dazu aufgefordert werden, entfernen Sie den ersten Dongle vom USB-Port und schließen den zweiten Dongle auf explizite Anforderung an.

7. Bei Prozessende wird eine "Fertig stellen"-Option angezeigt, aber auch die Möglichkeit, weitere Sicherheitszertifikate hinzuzufügen.

8. Befolgen Sie – bei Hinzufügen weiterer Zertifikate - die Schritte erneut und wählen Sie "Fertig stellen" oder fügen Sie weitere hinzu.

9. Nach Abschluss dieses Vorganges werden Sie neben den Einträgen CAPF und CCM TFTP die entsprechende Anzahl an Einträgen für Sicherheitsnachweise (security token), wie auch unten abgebildet, sehen. ACHTUNG: Das Bild zeigt vier Sicherheitsnachweise, je nachdem wie viele Sie geladen haben, wird die Anzahl abweichen.

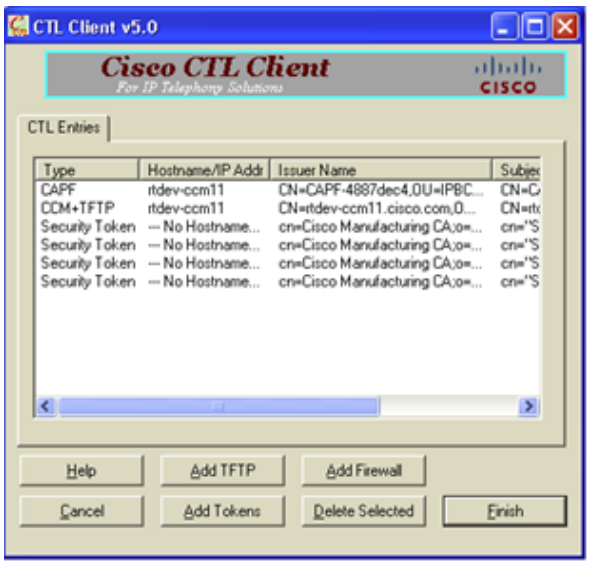


Abbildung 58 - CTL Entries

10. Entfernen Sie sämtliche Dongles von den USB-Ports und verwahren Sie diese sicher auf.

11. Schließen Sie den CTL Client.

12. Starten Sie den CUCM und TFTP Dienst über die CUCM Administration Seite neu.

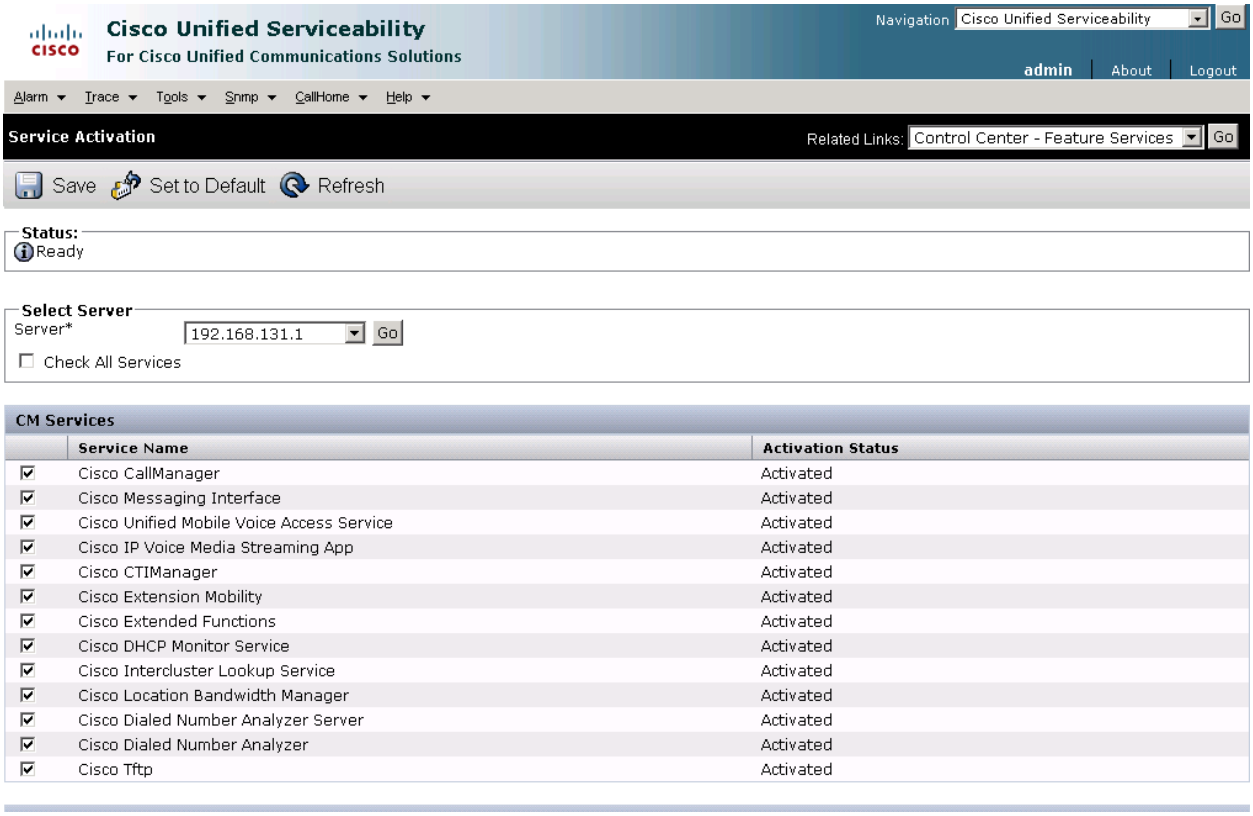


Abbildung 59 - CUCM Service Activation

6.2 Aktivierung in Konfiguration

6.2.1 NovaTec am TRUNK-Anschluss

Wählen Sie → CM Administration → Security → Sip Trunk Security Profile

- Der X.509 Subject Name muss mit dem „Common Name" identisch sein, der in der Konfiguration des angeschlossenen NovaTec Gateways für dessen SIP-CSR gesetzt ist.

- Setzen Sie den "Incoming Port:" auf 5061.

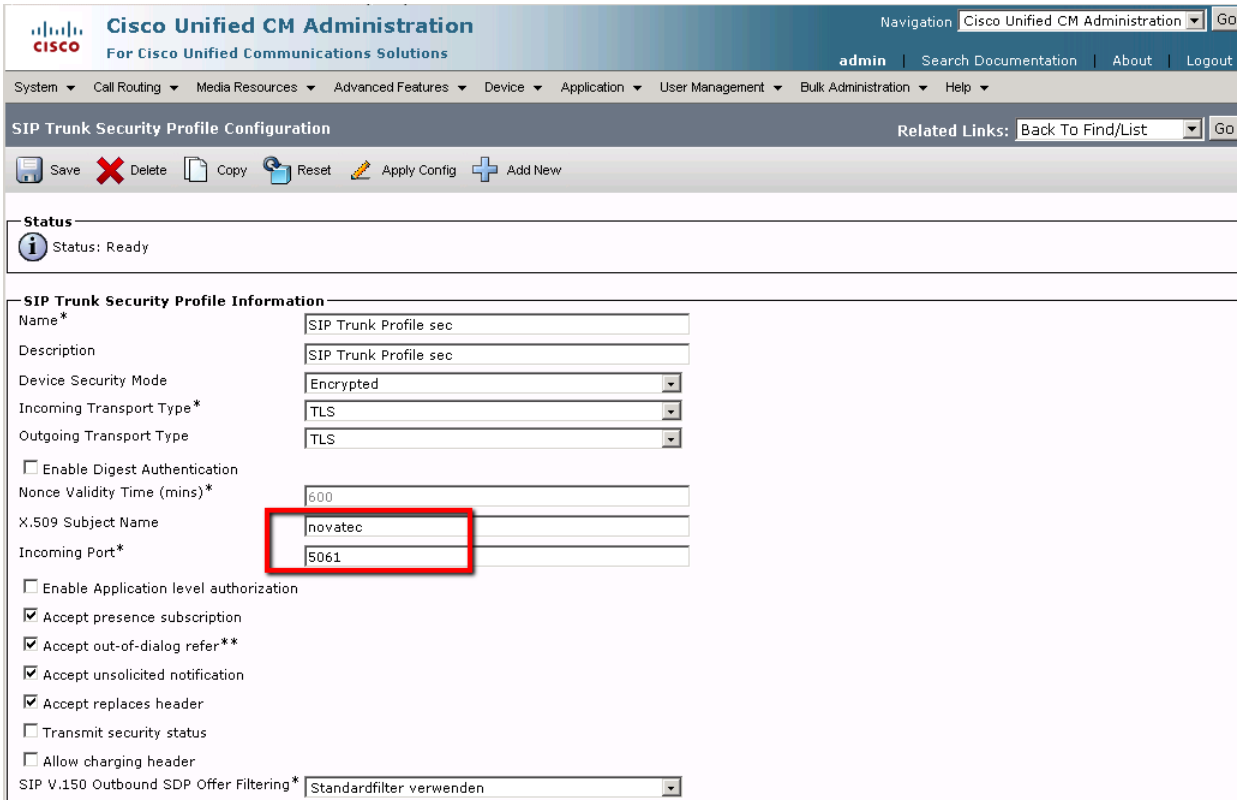


Abbildung 60 - CUCM Trunk Security Profile

Setzten Sie auch in der Tunk-Konfiguration den “Destination Port” auf 5061 und wählen Sie das zutreffende Trunk-Sicherheitsprofil aus.

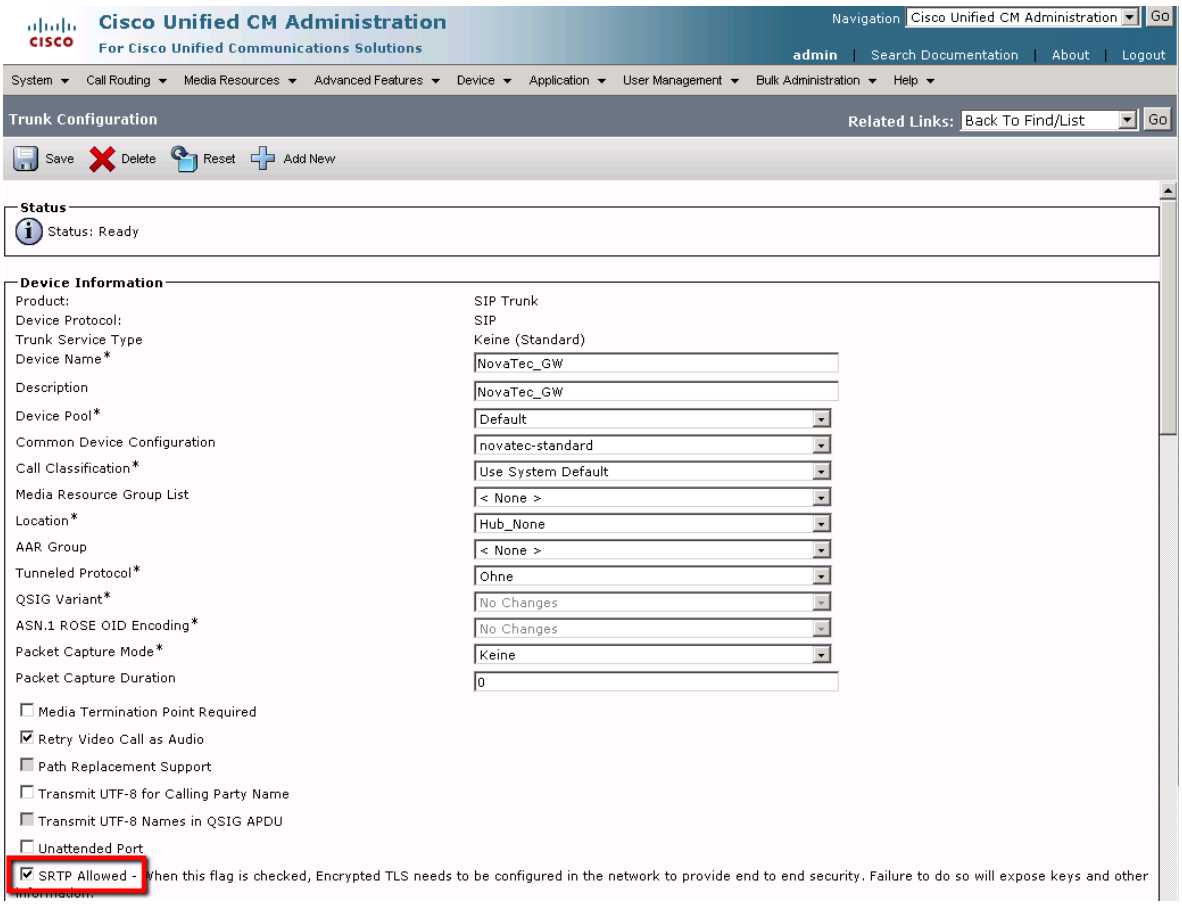


Abbildung 61 - CUCM Trunk sRTP allowed

In der Trunk-Konfiguration wird „SRTP Allowed" gesetzt, damit, neben dem mit TLS gesicherten Verbindungsaufbau via SIP, auch der eigentliche Sprach- bzw. Datenstrom mit sRTP gesichert übertragen wird.

Als „Destination Port" wird die Nummer 5061 für TLS eingestellt.

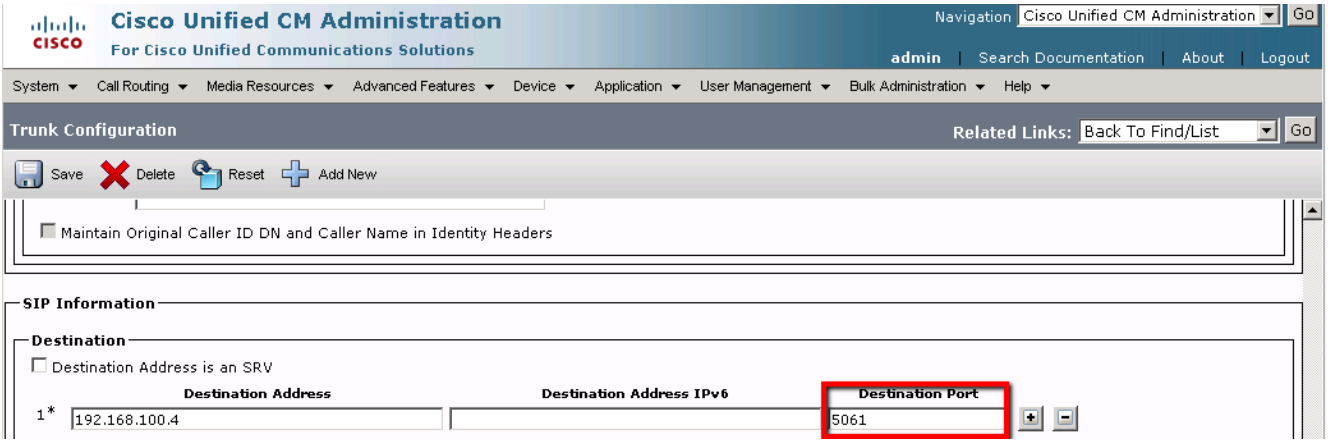


Abbildung 62 - CUCM Trunk Port 5061

6.2.2 NovaTec am Phone-Anschluss

An dem Phone-Anschluss eines CUCM kann eine NovaTec S3 angeschlossen werden. Um diesen Anschluss mit TLS und sRTP zu sichern, gehen Sie wie folgt vor.

Falls kein Security Profile existiert, wird dieses erstellt indem ein „Transnova S3 – Standard SIP Non-Secure Profile" kopiert wird, und als „Transnova S3 – SIP Secure Profile" gespeichert wird.

In diesem werden folgende Sicherheitseinstellungen gemacht.

Wählen Sie → Device → Phone → Security Profile

- Setzen des "Device Security Mode" auf "Encrypted"
- Als "Transport Type" wird "TLS" gewählt
- Als „SIP Phone Port" wird auf 5061 eingetragen

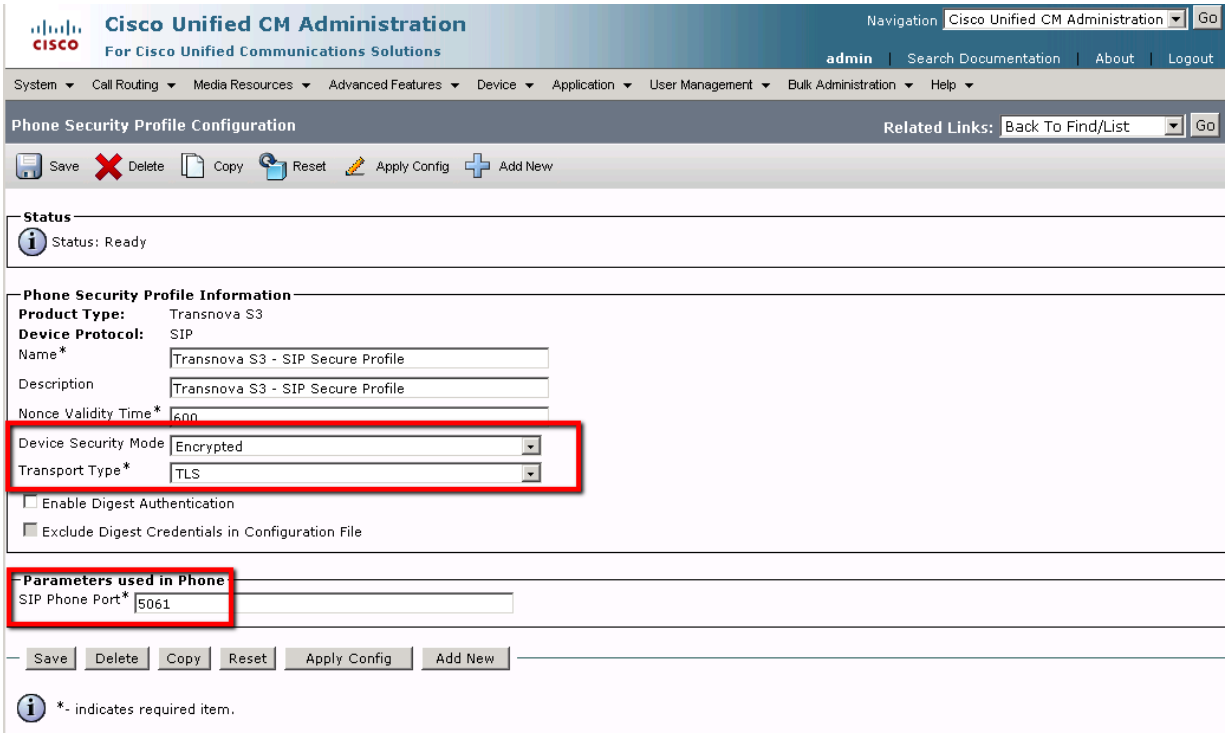


Abbildung 63 - Modify Transnova S3 - Non-Security Profile

Dieses neue „Transnova S3 – SIP Security Profile" wird nun in der „Phone Configuration" dem „Device Security Profile" zugewiesen.

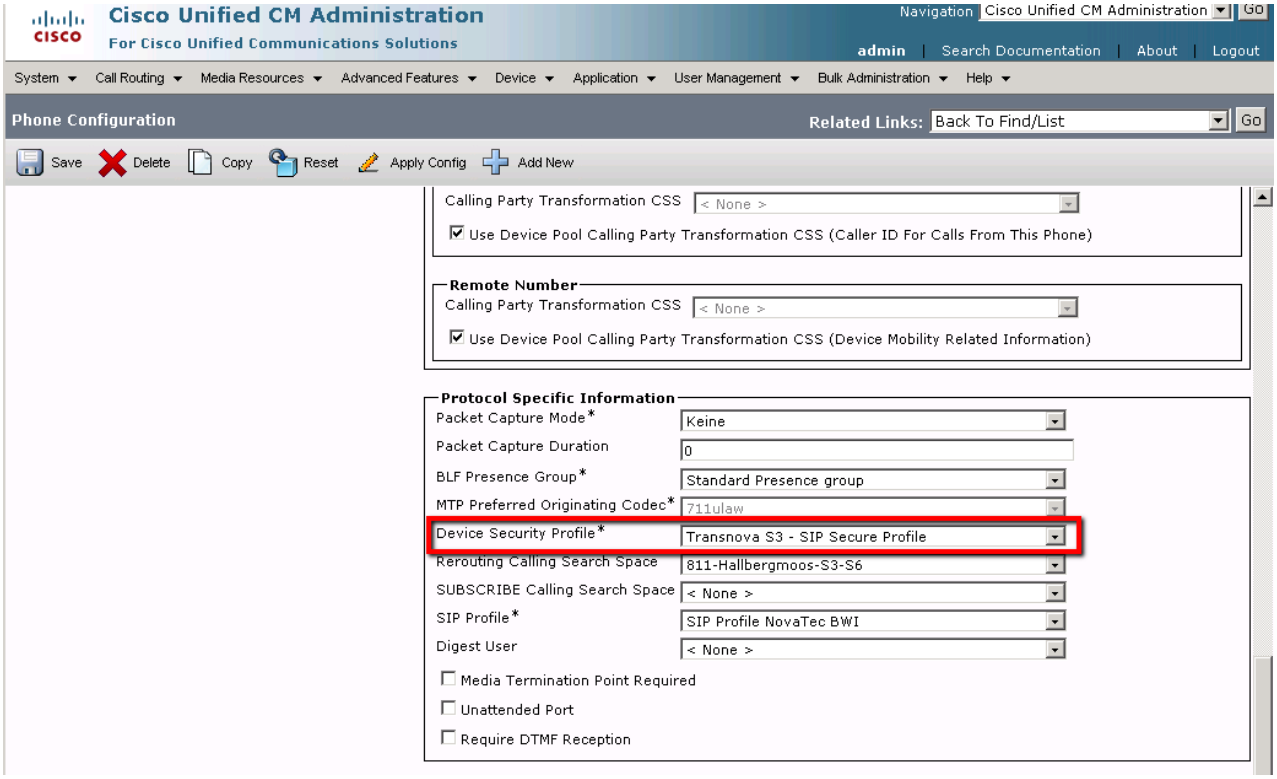


Abbildung 64 - Transnova S3 - Security Profile

6.3 Zertifikate Im- & Exportieren

Falls keine gemeinsame Zertifizierungsstelle (CA) für einen CUCM und ein NovaTec Gateway existiert, ist ein gegenseitiger Austausch der SIP-TLS-Zertifikate notwendig. Zum Beispiel könnte der CUCM nur ein selbstsigniertes SIP-TLS-Zertifikat besitzen und das NovaTec Gateway wird mit einem SIP-TLS-Zertifikat betrieben, das mit der TI-CA oder von einer externen CA signiert worden ist. In diesem Fall müssen die Zertifikate aus den Systemen exportiert und in die Gegenstelle importiert werden.

6.3.1 CUCM Zertifikate auf ein NovaTec-System exportieren

6.3.1.1 Herunterladen eines Zertifikats aus einem CUCM

Um ein Zertifikat aus einem CUCM auf Ihren PC herunterzuladen, gehen Sie bitte wie folgt vor:

1. Gehen Sie im CUCM auf OS-Administration → Security → Certifikate Management. Die Liste der Zertifikate wird angezeigt.

2. Sie können die Suchfunktion nutzen, um die Zertifikatsliste zu filtern.

3. Klicken Sie auf den Namen des Zertifikats „CallManager.pem". Die Zertifikats-Konfiguration wird als Fenster angezeigt.

4. Drücken Sie den Button "Download".

5. Öffnen Sie den Download-Dialog und speichern Sie die exportierte Datei.

6. Die auf dem PC gespeicherten CUCM Zertifikate können, wie im Kapitel 4.2.3 „CA-Zertifikat in Trust Liste laden" beschrieben, in die Trust Liste eines NovaTec Gateways importiert werden.

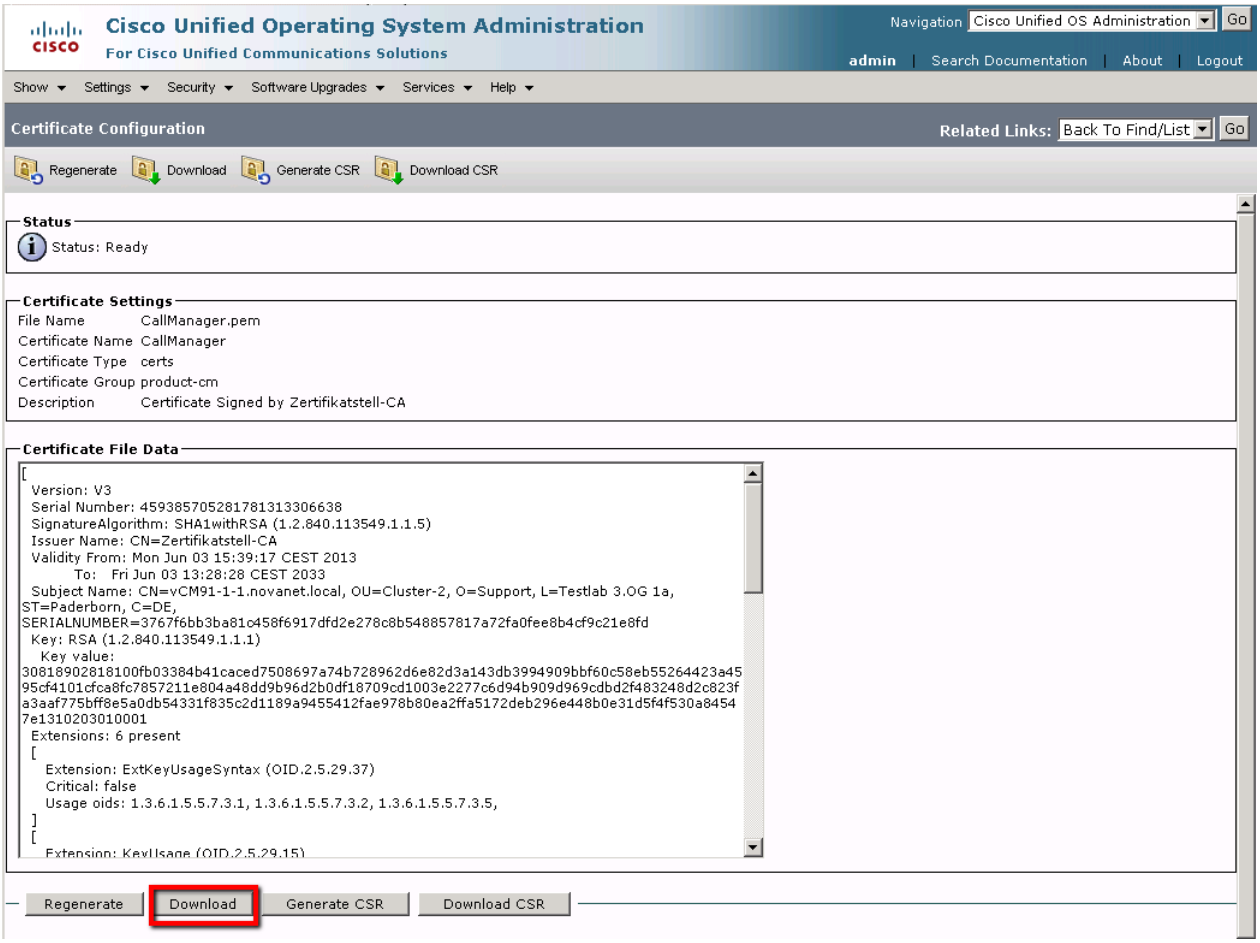


Abbildung 65 - Download CallManager Zertifikat

6.3.2 Importieren eines NovaTec Zertifikates in den CUCM

Um ein Zertifikat von Ihrem PC in den Trust Store eines CUCM zu laden, gehen Sie bitte wie folgt vor.

Das CA-Zertifikat, mit dem das SIP-TLS-Zertifikat eines NovaTec Gateways signiert wurde, muss in den CUCM Trust Store geladen werden. Hierzu berücksichtigen Sie bitte auch den Sicherheitsabsatz im CUCM OS Admin Guide, um herauszufinden, wie ein Zertifikat in den CUCM Trust Store geladen werden kann.

- Das CA-Zertifikat „xxxxx" sollte in den Call-Manager hochgeladen und als vertrauenswürdiges Zertifikat klassifiziert werden.
- OS Administration → Security → Certificate Management →Upload Certificate
- Certificate Name: Callmanager-trust
- Root Certificate (kann leer gelassen werden)
- Upload File: Beispiel „siptcl_ca_cert.pem"

Wenn mehrere Call-Manager in einem Cluster konfiguriert sind, muss "xxxxx" auf alle Call-Manger im Cluster geladen werden.

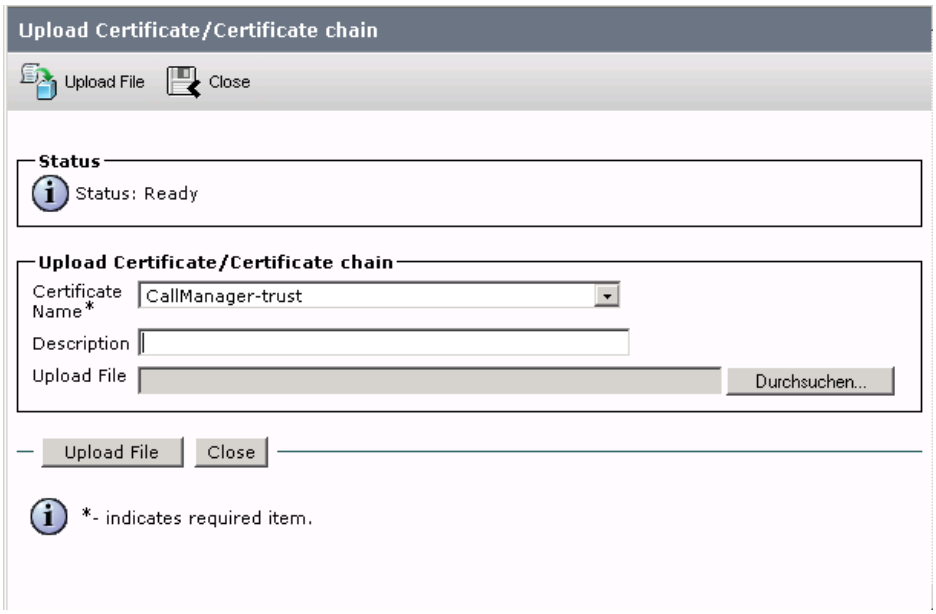


Abbildung 66 - Upload CA-Zertifikat in CUCM Trust List

6.4 Externe CA signiert CallManager

Wenn nicht das selbstsignierte CallManager-Zertifikat in einer PKI verwendet werden soll, sondern eine externen CA den CallManager-CSR signiert, werden folgende Schritte notwendig.

- Der CallManager stellt eine Zertifizierungsanforderung (CSR).
- OS Administration → Security → Certificate List → Schaltfläche „Generate CSR"

Abbildung 67 - Generate CSR

- Diese wird exportiert und zur Signierung an eine CA gegeben.
- OS Administration → Security → Certificate List → Schaltfläche „Download CSR"

Abbildung 68 - Download CSR

- Das CA-Zertifikat der externen CA wird in den CallManager geladen.
- OS Administration → Security → Certificate List → Schaltfläche „Upload Certificate"
- Als "Certificate Name" wählen Sie "CallManager-trust"

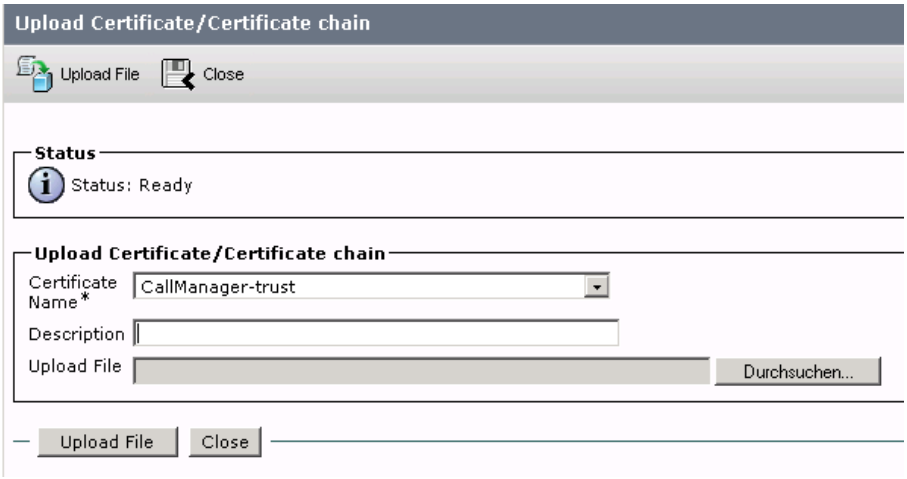


Abbildung 69 - CA-Zertifikat in Trust Liste laden

- Das signierte Zertifikat wird in den CallManager geladen.
- OS Administration → Security → Certificate List → Schaltfläche „Upload Certificate"
- Als "Certificate Name" wählen Sie "CallManager"

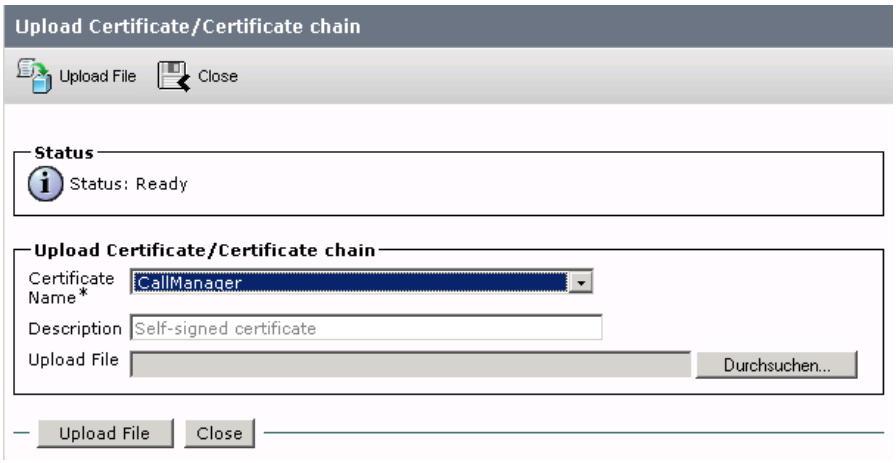


Abbildung 70 - Neues CallManager-Zertifikat laden

6.5 In Konfiguration deaktivieren

6.5.1 TLS und sRTP für CUCM Trunk deaktivieren

- Im Trunk-Konfigurationsfenster nehmen Sie die Häkchen im "SRTP Allowed..."-Kästchen raus. Setzen Sie den "Destination Port" auf 5060 und wählen das gewünschte Trunk-„non security"-Profil aus.

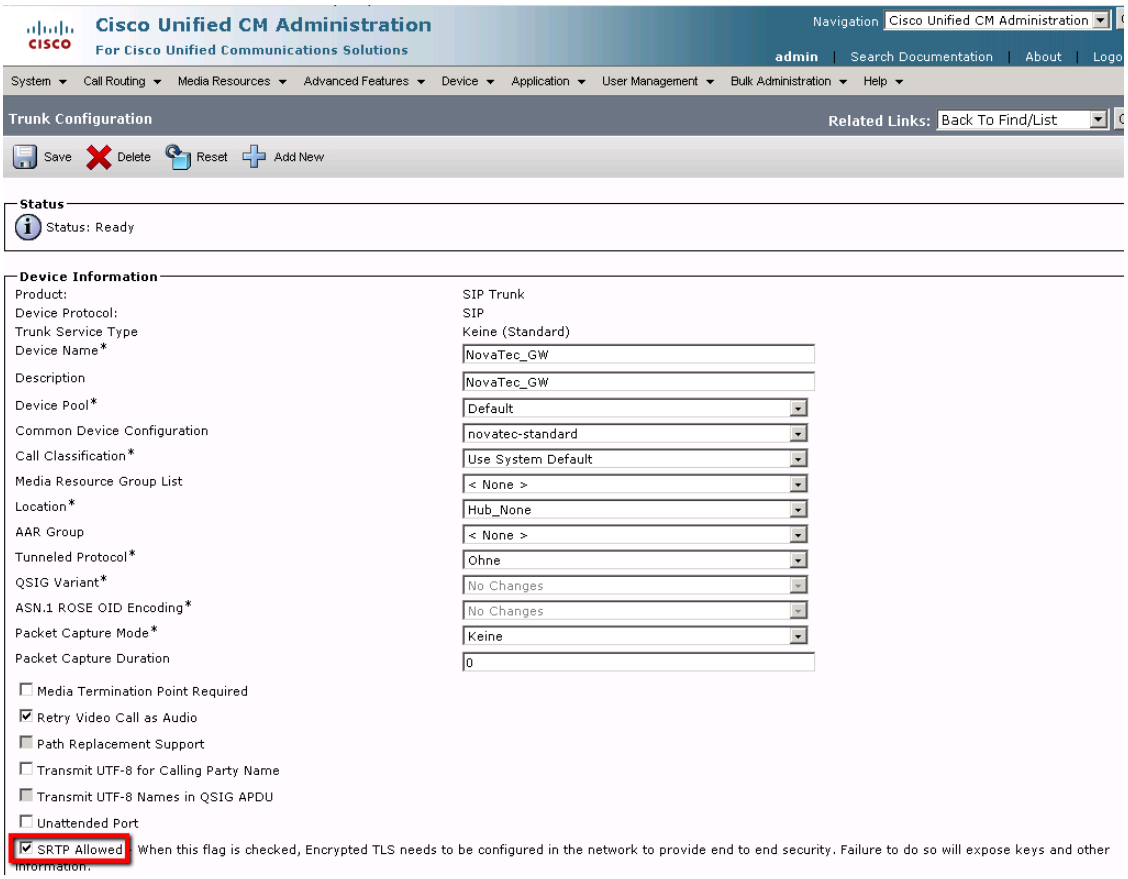


Abbildung 71 - Trunk Configuration – sRTP

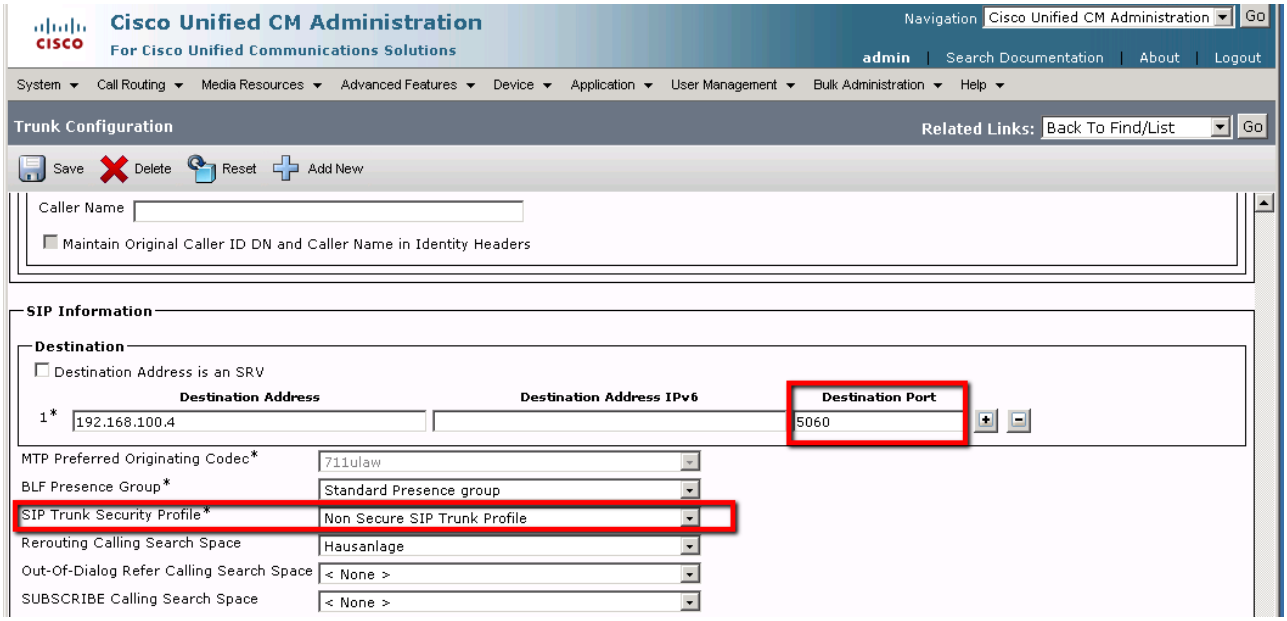
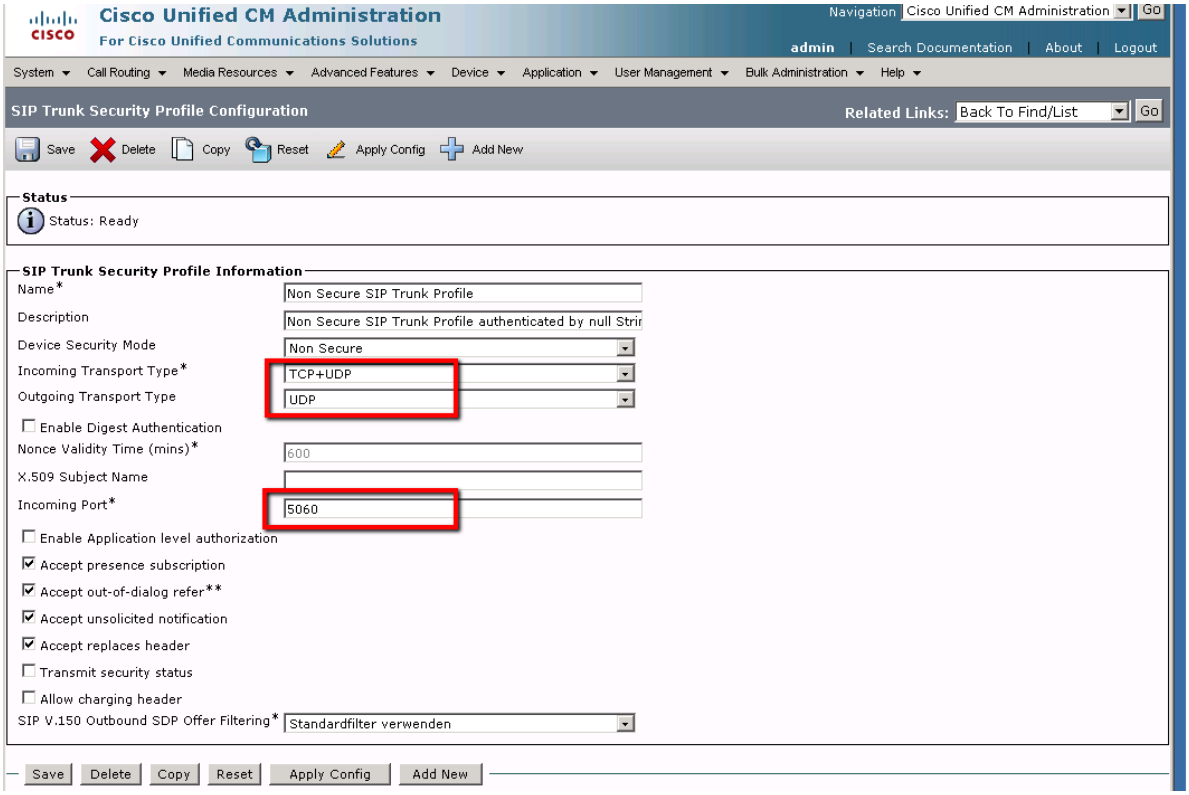


Abbildung 72 - Trunk Configuration Security Profile

- Die Einstellungen des Trunk-"non security"-Profils sollten wie die im Beispiel unten aussehen. "Incoming Port:" 5060.



6.5.2 TLS und sRTP für eine CUCM-Line deaktivieren

- Ändern Sie das Profil von einem "crypto security"-Profil auf ein „non security phone"-Profil.
- Die Einstellungen des Line-Devices im "non security"-Profil sollte wie folgt sein: "Incoming Port:" 5060.

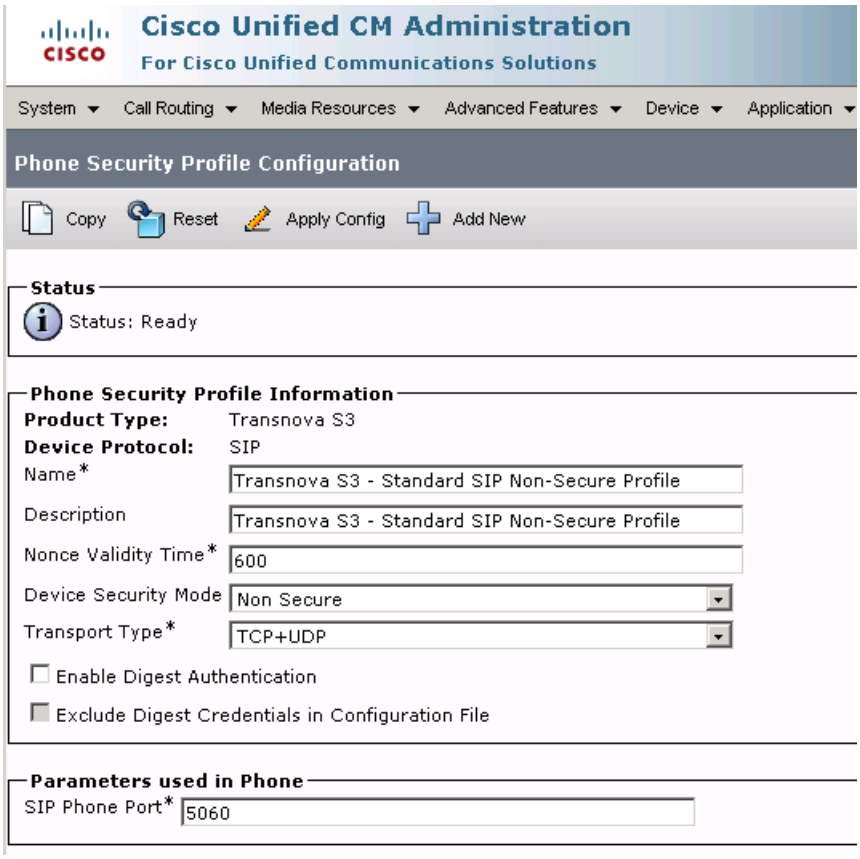


Abbildung 73 - CUCM Line disable security

7 Anhang

7.1 Status LED Signalisierung während der Signierung

Die Status LEDs auf der Frontplatte der NovaTec Systeme signalisieren folgende Zustände.

1. Keine Bedeutung.
2. Das System generiert einen 1024/2048 Key mit anschließendem Reset.
3. SCEP Mode: System sucht per DNS die IP Adresse des CA Server.
4. SCEP Mode: CA-Server gefunden. Enrollment wird durchgeführt mit anschließendem Reset.

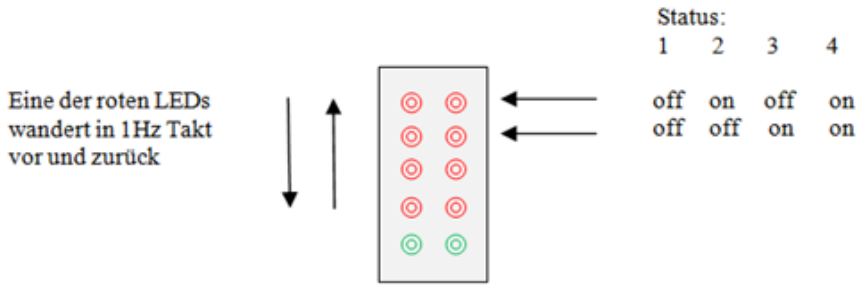


Abbildung 74 - LED Feld der CCU3

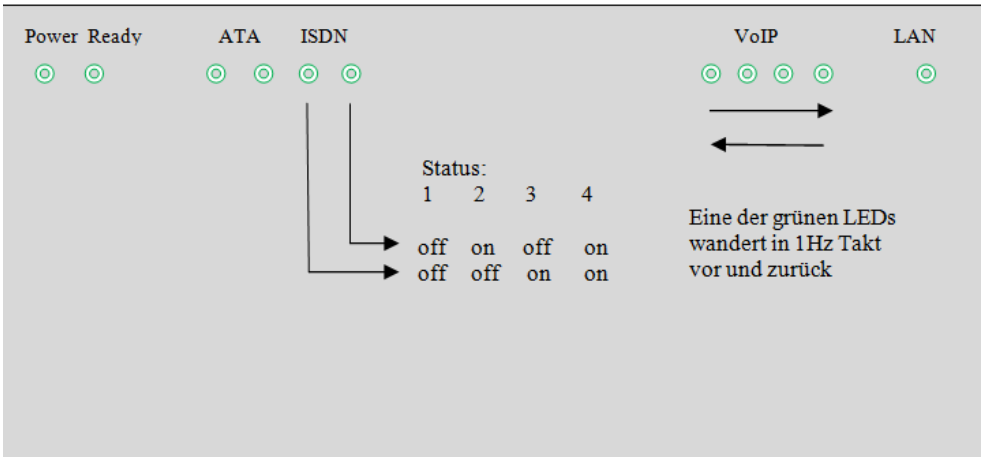


Abbildung 75 - LED Feld der S3

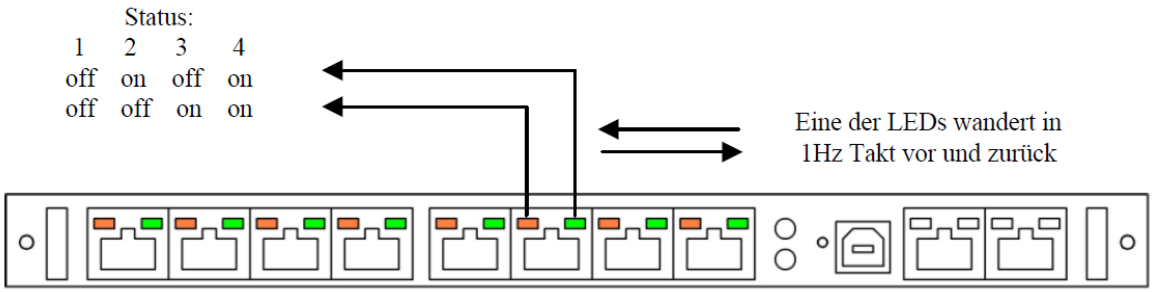


Abbildung 76 - LED Feld der CCU4

7.2 Wechsel 1024/2048 bit RSA Key

Im TraceInfo-Client wird unter „System-Security" die Länge des aktuellen privaten RSA Schlüssels angezeigt.

RSA key version: 00.00.00.01 → 1024 bit key

00.00.00.02 → 2048 bit key

Ein neuer Schlüssel wird nur im Fall eines Wechsels der Schlüssellänge erzeugt! Es kann direkt kein neuer Schlüssel mit der im System schon vorhandenen Schlüssellänge generiert werden.

War vor der Initiierung des Schlüsselwechsels ein 1024 bit Schlüssel hinterlegt, wird nach dem nächsten Reset ein 2048 bit Schlüssel generiert und vice versa. Dieser private RSA Schlüssel ist gesichert im Gateway hinterlegt und kann von außen nicht ausgelesen werden.

Durch die LEDs auf der Frontplatte wird das Erzeugen eines neuen Schlüssels angezeigt (siehe Abschnitt 7.1). Der Vorgang kann einige Minuten dauern (CCU3/S3: 4min/1024bit, 10min/2048bit – CCU4: 0,5min/1024bit, 1min/2048bit). Das Ende der Schlüsselgenerierung, wird mit einem Systemreset angezeigt.

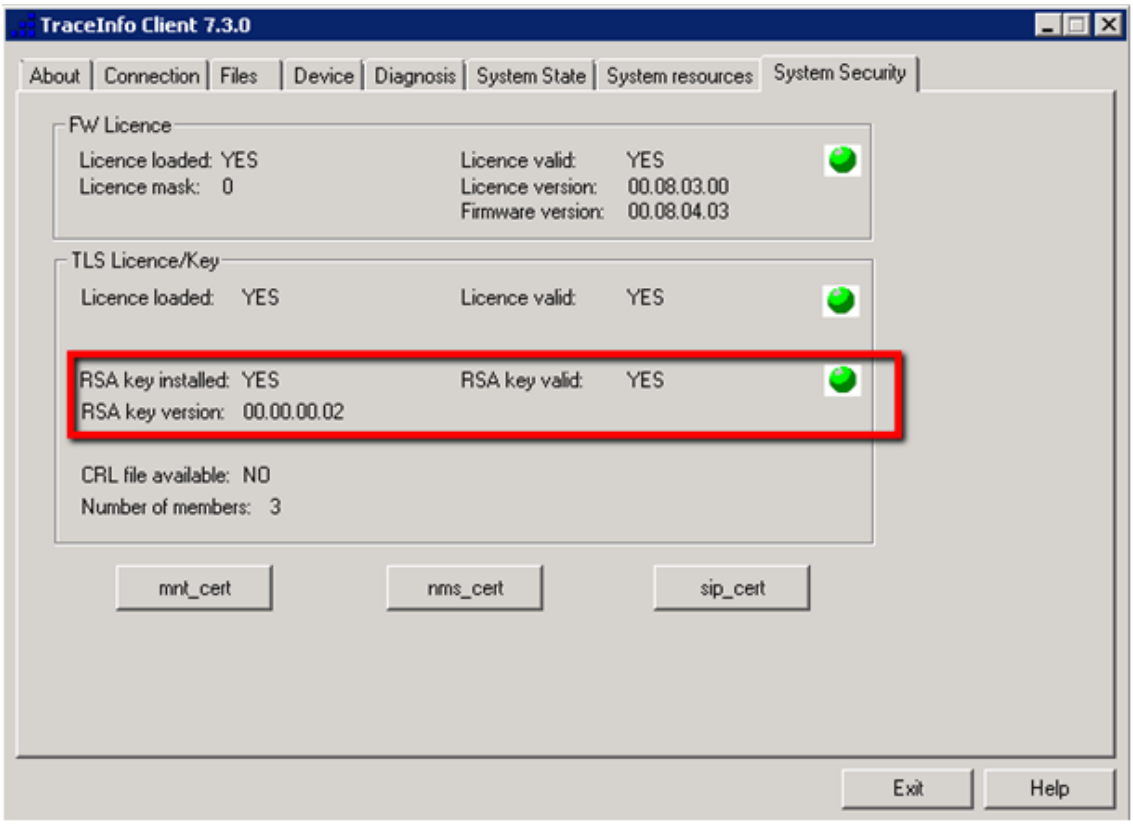


Abbildung 77 - Anzeige aktuelle Schlüssellänge

Um die Schlüssellänge im System zu ändern, werden folgende Schritte durchlaufen:

1. Die erforderliche Wechsellizenz, eine besondere FW-Lizenz, erhalten Sie von NovaTec. Diese wird wie eine normale FW-Lizenz auf das System geladen.

2. Außerdem wird in der Konfiguration unter „Operating parameters" → „RSA-key Settings" die neue Schlüssellänge angegeben.

3. Laden Sie diese Konfiguration in das System.

4. Das System generiert einen neuen Schlüssel mit geänderter Länge.

5. Laden Sie jetzt bitte erneut die originale NovaTec FW-Linzenz in das System und aktivieren diese mit einem anschließenden Reset des Gateways.

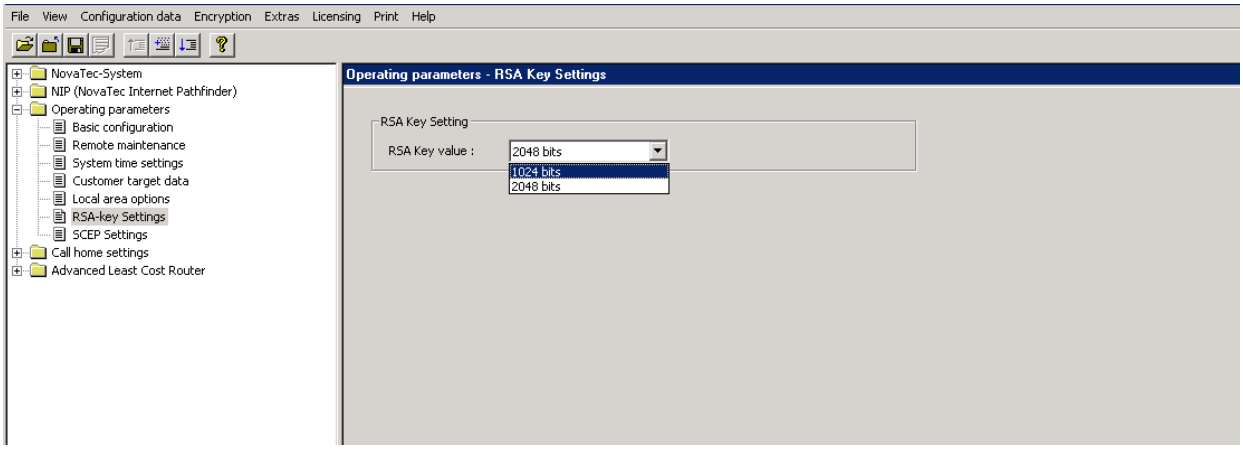


Abbildung 78 - Konfiguration Schlüssellänge

7.3 SCEP Applikation

7.3.1 NovaTec SCEP Implementierung

Das Protokoll ist nach der quasi Norm der Internet Engineering Task Force "Cisco Systems Simple Certificate Enrollment Protocol draft-nourse-scep-20" entworfen worden:

Die quasi Norm beschreibt 4 Funktionen

1. Get CA/RA certificate (Anforderung Public Certificate Kette und Enroll-Zertifikat)
2. Enroll certificate (Signieren des Zertifikat-Request)
3. Query certificate (Anfragen eines signierten Zertifikats)
4. Query CRL (Laden der "Certificate Revocation List".)

Die Funktion 1:

Die Funktion „Get CA/RA certificate" passt nicht in das heutige Konfigurationskonzept, da das Public Zertifikat bzw. die Zertifikatskette mit der Konfiguration den NovaTec Systemen zur Verfügung gestellt werden. Dieser unverschlüsselte Zugriff auf den Zertifikat-Server ist ein sicherheitsrelevanter Punkt. Die Norm verlangt, dass der Fingerprint des Zertifikats manuell vom Operator auf Glaubwürdigkeit überprüft wird.

Die Funktion 2:

„Enroll certificate" beschreibt das eigentliche „Signieren des Zertifikat-Request". Hierzu muss der Client (NovaTec System) in den Request seine IP Adresse in die „X.509v3 extensions" eintragen:

Beispiel:

[x509v3_IPAddr]

subjectAltName=critical,IP: "192.168.1.1"

Kann der Server "automatisches Enrollment", so muss der Zertifikat-Request zusätzlich mit einem Passwort gesichert werden:

Beispiel:

[req_attributes]

challengePassword = "A challenge password"

challengePassword_min = 4

challengePassword_max = 20

Die Funktion 3:

„Query certificate“ erlaubt das Anfragen eines signierten Zertifikats. Wird zurzeit nicht genutzt da optional und PKI abhängig.

Die Funktion 4:

„Query CRL“ Laden und Überprüfen der CRL-Liste “Certificate Revocation List”. Wird zurzeit nicht genutzt da optional und PKI abhängig.

7.3.2 SCEP Traceausgaben

Das Modul „SCEPD" der Firmware führt Traceausgaben in Klartext durch.

Beispiel:

```
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 Abkürzungsverzeichnis

Abkürzung	Bedeutung	Übersetzung
CA	Certificate Authority	Zertifizierungsstelle
CCU3	Central Control Unit Model 3	
CCU4	Central Control Unit Model 4	
CRT	Certificate	Zertifikat
CSR	Certificate Signing Request	Zertifizierungsanforderung
CTL	Certificate Trust List / CUCM	
CUCM	Cisco Unified Communications Manager	
DHCP	Dynamic Host Konfiguration Protocol	
FW	Firmware	
IP	Internet Protocol	
MNT	Maintenace Task in den NovaTec	
NAMES	NovaTec Administration & Management Element Server	
NMS	NovaTec Management Server	
PKI	Public Key Infrastructure	
Root-CA	Root Certification Authority	Oberste Zertifizierungsstelle
Root-CRT	Root-Certificate / CA-Certificate	Stammzertifikat/sebst signiert
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		Liste vertrauenswürdiger CAs
VoIP	Voice over IP	

7.5 Abbildungsverzeichnis