Documentation

HiPath 4000 V5
IP Solutions - Signaling and Payload Encryption (SPE)

Service Documentation

A31003-H3150-S104-2-7620

Communication for the open minded

Siemens Enterprise Communications
www.siemens.com/open

SIEMENS

Communication for the open minded

Siemens Enterprise Communications
www.siemens.com/open

Reference No.: A31003-H3150-S104-2-7620

Service Manual HiPath 4000 V5 - IP Solutions - Signaling and Payload Encryption (SPE) - Contents

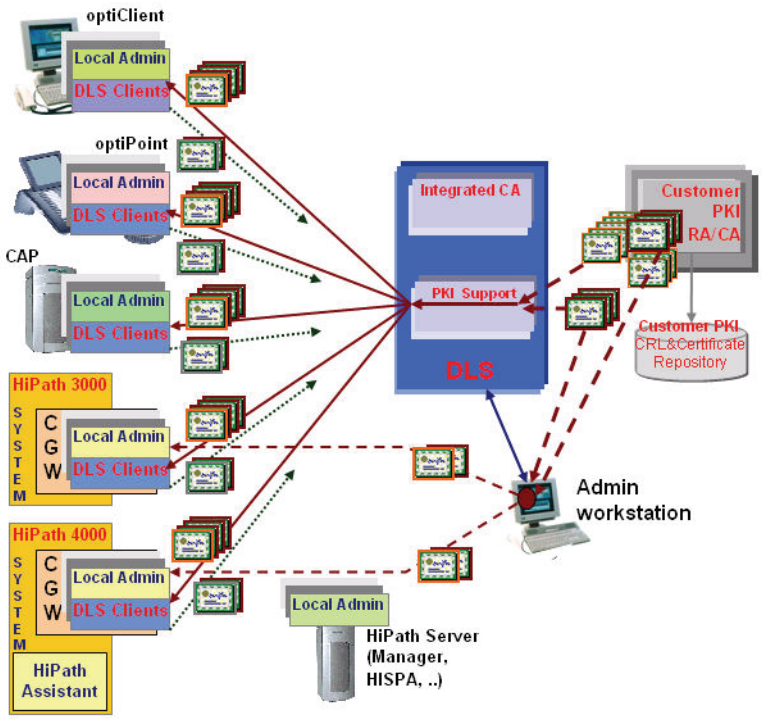
1 Feature Description

The "Signaling and Payload Encryption" feature encompasses the encryption of payload data and critical signaling data within HiPath 4000 V4 systems or between such systems and the associated endpoints. Calls are bundled and securely transferred with HiPath 3000 V7 and HiPath 8000 V3.1 R2.

A PKI (Pubic Key Infrastructure) is needed to use this feature. For more information, see Section 1.1.1, “Public Key Infrastructure (PKI)”.

1.1 Solution Concepts

1.1.1 Public Key Infrastructure (PKI)



A Public Key Infrastructure (PKI) is needed to use the "Signaling and Payload Encryption" feature. You can either use an existing customer PKI for this or apply a new PKI using Deployment Service DLS V2 R2.

The necessary certificates are centrally deployed to all HiPath 4000 gateways and terminals via DLS.

The PKI for HiPath 4000 included in DLS V2

- features a "lightweight PKI" solution for customers that do not have a PKI (certificate creation),
- supports the integration of an existing PKI (certificate provision for customer PKI),
- performs automatic certificate deployment.

Customer with PKI

If the customer already has a PKI, the following factors must be considered:

- The existing certificate must be allowed for encryption and signing.
- The existing certificate is an RSA certificate.
- Because of performance issues the existing certifcate has a maximum key length of **1024 bits**.
- The existing certificate is in PEM or PKCS #12 format.

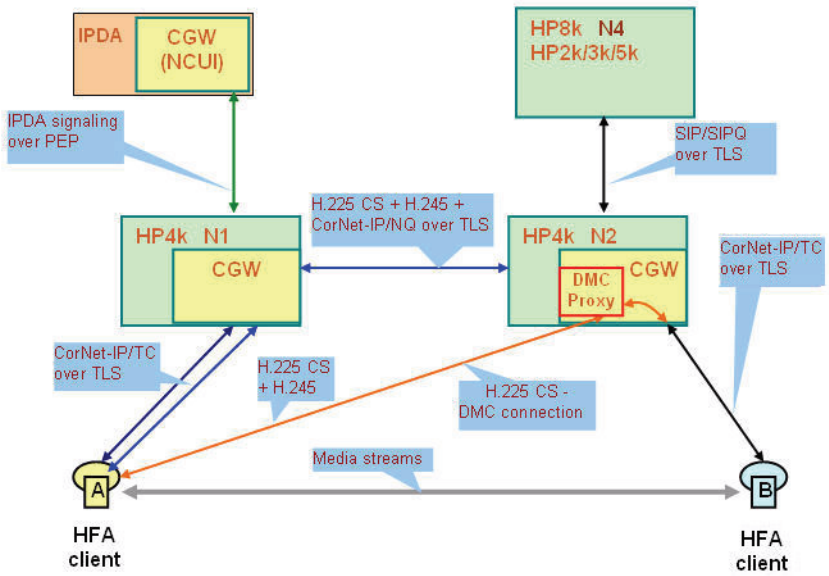
Customer without PKI

If the customer does not have a PKI, the necessary certificates can be created with DLS V2 R2. The **Automatic SPE Configuration** function in the **Administration** menu is used for this.

Detailed information on DLS

For more information on importing and deploying certioficates via DLS see Chapter 5, “Distribution of Certificates to a Common Gateway Board with DLS”.

1.1.2 Signaling Encryption



Signaling encryption is based on the TLS (Transport Layer Security) protocol for HFA telephones or IP trunking (H.323/SIP) and the PEP (Proprietary Encryption Protocol) protocol for IPDA.

In the case of VoIP signaling paths in a HiPath 4000 network or to partner systems (such as HiPath 8000), every connection is individually and independently encrypted. TLS/SSL encryption (SIP/H.323/HFA) and AES encryption based on pre-shared secrets (IPDA/DMC) is used for this. End-to-end encryption is based on an unbroken encrypted chain of partial signaling links.

The TLS/SSL connections remain permanently active and is renewed at regular intervals. The time interval for renegotiation is set in the WBM:

WBM > Explorers > Security > (right-click) **Signaling and Payload Encryption (SPE) > Edit Security Configuration > Minimum Re-Keying interval [hours]**

- HFA stations

  CorNet-TC/TS and H.323 signaling between HiPath gateways and HFA stations is secured by a "server-authenticated" TLS connection, that is, the HFA stations check the certificates supplied by the gateway.

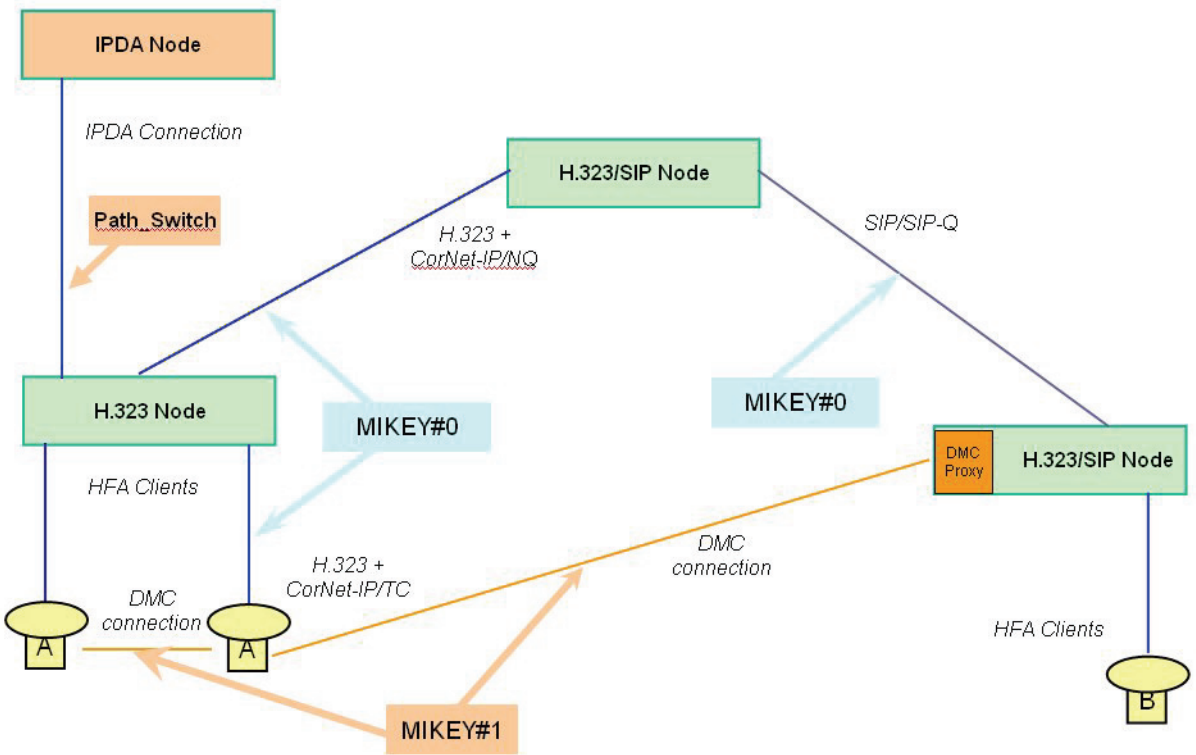
- CorNet-IP/SIP-Q trunking

  H.323/SIP signaling (including Cornet-NQ messages) between two gateways is secured by a "mutual-authenticated" TLS connection, that is, both gateways verify the identity of the partner based on the certificates delivered.

- DMC connections

  Signaling (H.225) is secured with H.235.1 (authentication and integrity) for the DMC connections. The "shared-secret" (key) needed is generated by the HiPath 4000 for every call and distributed to the DMC endpoints. This means that DMC connections are not encrypted, they are only authenticated.

1.1.3 Payload Encryption

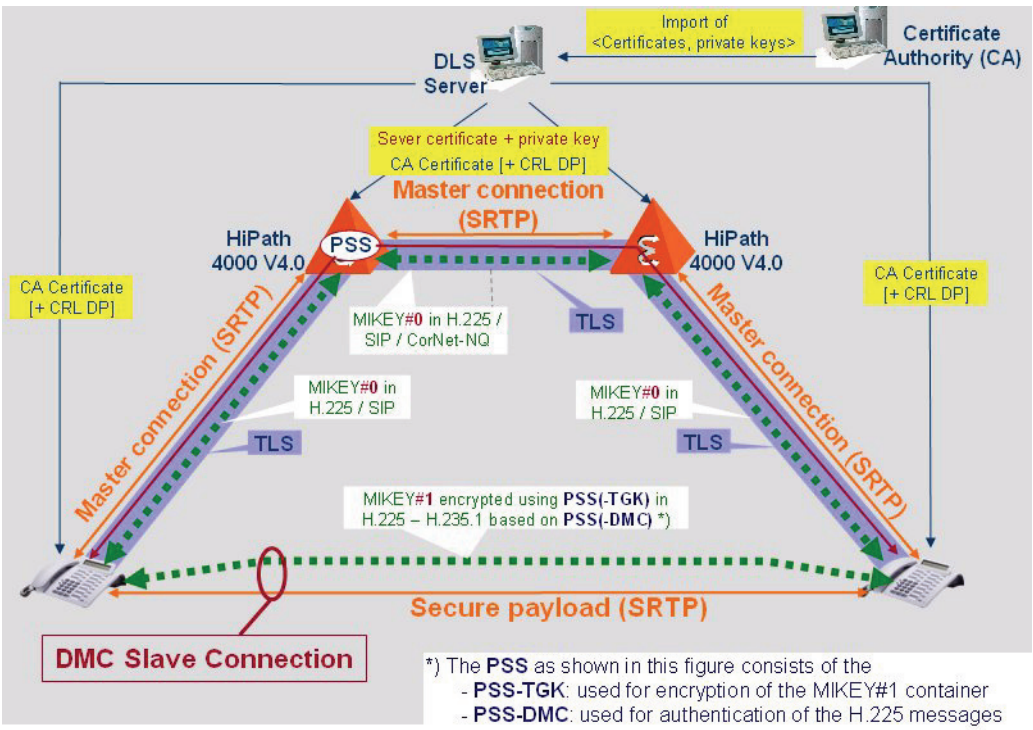


SRTP is used for all connections (HFA, SIP, IPDA) for payload encryption. The Advanced Encryption Standard (AES) is the encryption system used for this. **MIKEY** is used here as a key management protocol. **MIKEY Option 0** and **MIKEY Option 1** are used for encryption. For more information on MIKEY please refer to Section 1.2, “MIKEY”.

Each payload encryption operation uses a new, (cryptographically) random key generated at an endpoint and only used for the duration of this payload connection. This key is exchanged via (certificate-authenticated) signals between the two endpoints. The key here is a 128-bit key.

Stations receive a message about whether a call is end-to-end encrypted.

1.2 MIKEY



MIKEY is a form of key management for realtime multimedia communication and facilitates the exchange of keys and other security parameters between stations. In voice over IP, MIKEY can be used to exchange the master key and other security parameters to ensure secure SRTP transmission between terminals.

1.2.1 MIKEY Option 0

MIKEY Option 0 is used in case the signaling connection is secured via TLS (hop-by-hop), i.e.: for all end-to-end payload stream for the (DMC) Master connection of a HiPath 4000 node in which for subscriber interfaces Server authenticated TLS connections and for trunking interfaces mutual authenticated (Server and Client) TLS connections are requested.

Thus, no certificates are needed for MIKEY Option 0 itself but the HiPath systems respectively their gateways need an own (server) certificate plus private key for TLS purpose.

All involved entities need the certificate of that/these CAs that issue the certificates for the HiPath systems / gateways.

In case **CRL** (**C**ertificate **R**evocation **L**ist) checks are required by means of configuration, the **CRL DP** (**CRL D**istribution **P**oint - HTTP/LDAP URL) is required by every endpoint and has therefore distributed too.

1.2.2 MIKEY Option 1

MIKEY Option1 is used for DMC slave connections only (HiPath 4000, HiPath 2000/3000/5000 as passive DMC endpoints).

The required symmetric encryption key needed therefore is generated on a per call base by the HiPath system and distributed to the DMC endpoints via secured network links.

No certificates are required by MIKEY Option 1 itself.

2 Service Information

2.1 Restrictions

- IP connections to a CA4000 system are not encrypted, that is, the application data transmitted over this interface is unprotected but can be used without restriction.
- This feature is **not** compatible with "Signaling and Payload Encryption" in HiPath 4000 V3.0, that is, encrypted signaling and payload cannot be transmitted in a network with HiPath 4000 V3.0.

  In a network with HiPath 4000 V3.0, it is not possible to encrypt the trunking path between the two systems. HiPath 4000 V3.0's internal encryption can be activated, however, within HiPath 4000 V3.0.
- If encryption has been activated on an STMI2/NCUI2+ board, the number of configured channels must be 33% less than when encryption is deactivated.

  For the exact number of B channels, see "HiPath Gateways HG 3500 und HG 3575", Section 3.6, "B Channels".
- SIP subscribers do not support encryption. That means that you can't activate SPE for SIP subscribers. For a complete list of terminals that support "Signaling and Payload Encryption", see Section 3.4.1, "Supported IP Terminals".
- Encryption on native SIP trunks is not released.

2.2 Upgrade from HiPath 4000 V3.0 to HiPath 4000 V4

If the "Signaling and Payload Encryption (V3.0)" feature is active in the HiPath 4000 V3.0 systems you want to upgrade, you must deactivate it before you perform the upgrade. For more information, see "HiPath 4000 V4, Guide for the Conversion / Implementation of HiPath 4000 Networks".

2.3 Supported Certificates

DLS can import the following certificates:

- CA certificates (*.crt, *.cer) from the certification authority
- Certificates in the format **P**ublic **K**ey **C**ryptography **S**tandards #12 (PKCS #12) (*.p12)
- Certificates in the format X.509 PEM

An expired certificate cannot be reloaded. If a certificate expires in the course of implementation, a HISTA message is issued along with an Error message. The system continues to use the certificate, however.

Certificates should be replaced when their validity expires.

The certificate for Secure Trace features a number of unique characteristics (see Chapter 4, “Secure Trace”).

HISTA message

Error message

F5881 with Error Cause: CERTIFICATE EXPIRED

2.4 Board Replacement

If certificates are lost (for example, when loading a board following board replacement), they can be reloaded by means of the customary "Backup&Restore" mechanism (logical HBR Back-up). The same applies to the MEKs during IPDA encryption.

Only a valid certificate can be loaded on the board.

2.5 SPE in Connection with Mobile HFA

2.5.1 Terminology

SPEcapable client:	A client actually logged in as TRADITIONAL client but that is SPE capable and provided with all credential and configurations for connecting as **SECURE** or **CIPHER** client.
TRADITIONAL client:	A client actually logged in as TRADITIONAL client and **NOT SPE** capable at all (e.g. optiPoint 500).

	**SECURE** and **CIPHER** client

	**TRADITIONAL** client
	SPEcapable client

2.5.2 Prerequisite

The **same protocol** (TCP or TLS) must be used for the connection to the gateway **for** the **VISITED and** the **HOME station** in order to avoid that a VISITED station using TCP can disconnect a HOME station using TLS (Dos attacks).

A HOME station connected via TCP that is disconnected by a VISITED station connected via TLS, is unable to disconnect the VIISTED station and thereffore cannot re-connect to its gatewy again.

2.5.3 Scenarios with Homogenous HiPath 4000 V4 Network with SPE enabled

HOME = SPEcapable and VISITED = SPEcapable

no problems

HOME = TRADITIONAL or SPEcapable and VISITED = SECURE/CIPHER

No problems but **SECURE/CIPHER** clients have to use **TCP** when acting as VISITED stations for a **TRADIONAL/SPEcapable** client.

By the SPE Mobile HFA call flows the VISITED station already gets the protocol to be used for connecting to the HOME gateway.

HOME = TRADITIONAL or SPEcapable and VISITED = TRADITIONAL or SPEcapable

no problems

HOME = SECURE/CIPHER and VISITED = TRADITIONAL

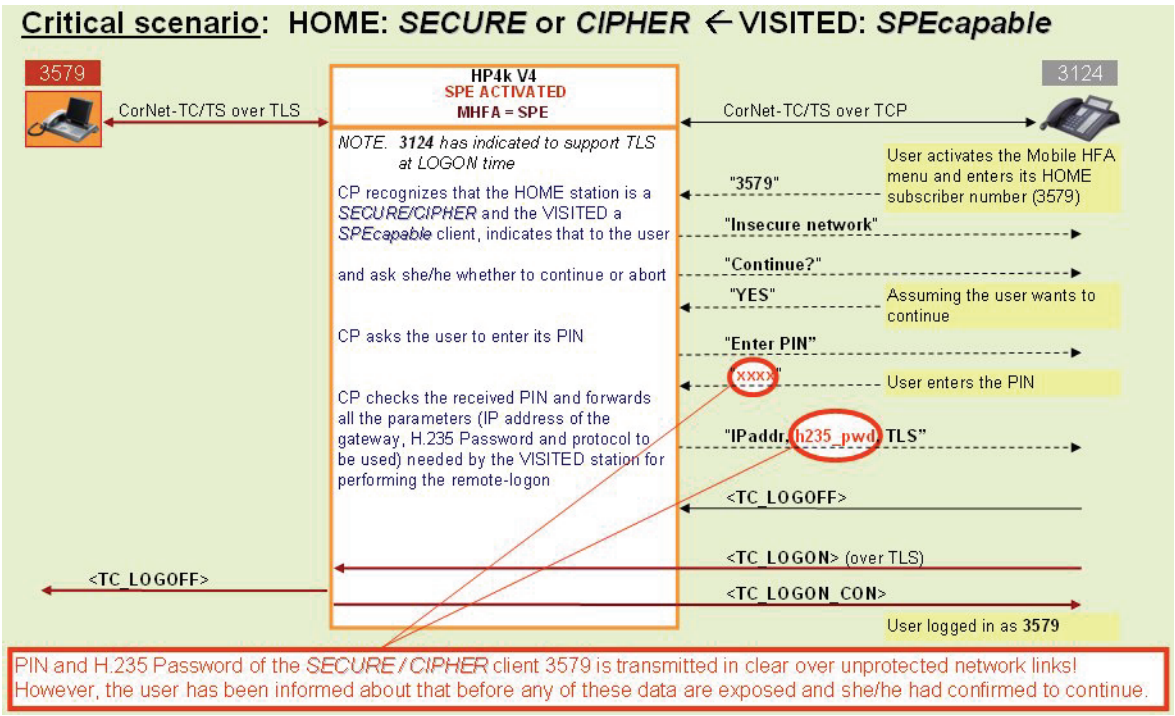
does not work

HOME = SECURE/CIPHER and VISITED = SPEcapable

Critical.

SPEcapable clients have to use **TLS** when acting as **VISITED** stations for a **SECURE/CIPHER** client.

This scenario is critical due to **PIN and H.235 password transfer over insecure network links**.



2.5.4 Scenarios within a Network with SPE activated Nodes and SPE deactivated Nodes

HOME and VISITED SPE deactivated and TRADITIONAL/SPEcapable

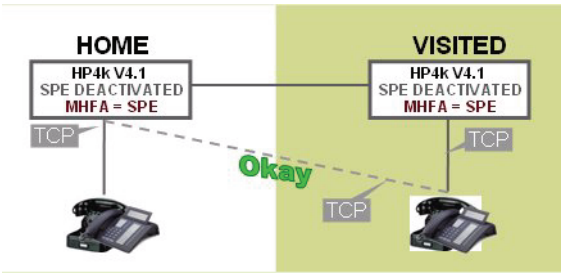
HOME:

- SPE deactivated

- phones: TRADITIONAL/SPEcapable

VISITED:

- SPE deactivated
- phones: TRADITIONAL/SPEcapable



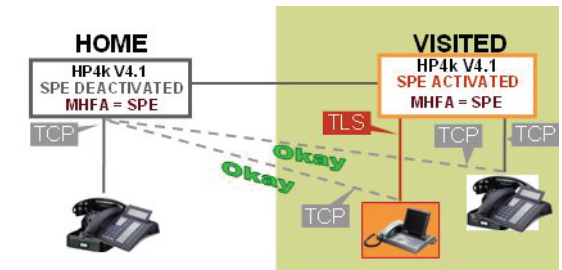
HOME: SPE deactivated and TRADITIONAL/SPEcapable, VISITED: SPE activated and TRADITIONAL/SPEcapable and SECURE/CIPHER

HOME:

- SPE deactivated
- phones: TRADITIONAL/SPEcapable

VISITED:

- SPE activated
- phones: TRADITIONAL/SPEcapable and SECURE/CIPHER



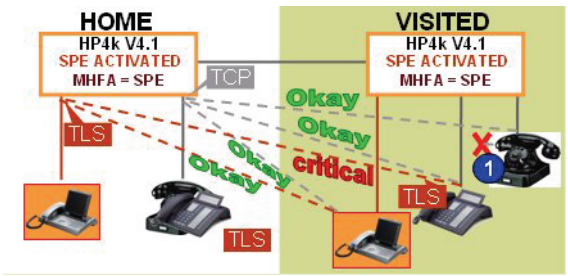
HOME: SPE activated and TRADITIONAL/SPEcapable and SECURE/CIPHER, VISITED: SPE activated and TRADITIONAL and SPEcapable and SECURE/CIPHER

HOME:

- SPE activated
- phones: TRADITIONAL/SPEcapable and SECURE/CIPHER

VISITED:

- SPE activated
- phones: TRADITIONAL and SPEcapable and SECURE/CIPHER



1	A **TRADITIONAL** client (without SPE support) is never accepted as VISITED station for a **SECURE** or **CIPHER** client. Call processing on the VISITED switch is aware about that and rejects the remote-login attempt with „Remote Login not possible“ (already before asking the user to enter its PIN).

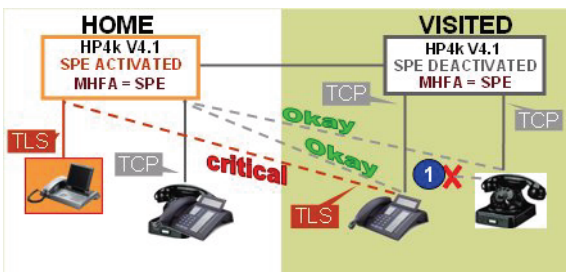
HOME: SPE activated and TRADITIONAL/SPEcapable and SECURE/CIPHER, VISITED: SPE activated and TRADITIONAL and SPEcapable

HOME:

- SPE activated
- phones: TRADITIONAL/SPEcapable and SECURE/CIPHER

VISITED:

- SPE activated
- phones: TRADITIONAL and SPEcapable



1	A **TRADITIONAL** client (without SPE support) is never accepted as VISITED station for a **SECURE** or **CIPHER** client. Call processing on the VISITED switch is aware about that and rejects the remote-login attempt with „Remote Login not possible“ (already before asking the user to enter its PIN).

2.5.5 Network Wide Usage of Mobile HFA

Accepting **TRADITIONAL** clients as HOME as well as VISITED station on a HiPath 4000 V4 with SPE activated has significant improvement concerning the usage of the Mobile HFA feature within homogenous HiPath 4000 V4 (with or without SPE activated) networks.

Mobile HFA **cannot** be used in networks between HiPath 4000 V4 systems with SPE activated and HiPath 4000 V2.0 / HiPath 4000 V3.0.

2.6 Scenarios

Signaling and payload encryption is supported in the following scenarios:

- IP/SIP trunking (see Section 3.3, “SPE for IP Trunking”)
  - Local-local gateway
  - Remote-local gateway
- HFA terminals (see Section 3.4, “SPE for IP Terminals”)
- IPDA (see Section 3.5, “SPE for IPDA”)
- Analog and TDM terminals (see Section 3.7, “SPE in Analog/TDM Endpoints”)
- Analog and TDM trunking connections (see Section 3.8, “SPE in Analog/TDM Trunks”)

3 Signaling and Payload Encryption (SPE) Configuration

Before you configure the **Signaling and Payload Encryption (SPE)** feature in a HiPath 4000 V4 system, make sure that all prerequisites are met (see Section 3.1, “Prerequisites”). Once this has been assured, you can configure the individual functions as required.

3.1 Prerequisites

The following prerequisites must be met before you can activate **SPE** in a system:

- All HG 3500 V4 common gateways in this system must be assigned SPE certificates and at least one CA certificate.
- All NCUI2 boards must be replaced by NCUI2+ or NCUI4.
- All NCUI boards must have Master Encryption Keys (MEKs) configured.
- All components must be timely synchronized via SNTP:
  - HiPath 4000 system: AMO DATE + HiPath 4000 Assistant
  - HG 3500 / HG 3575: automatic from the system
  - endpoints: WBM/DLS

  For more detailed information please refer to Feature Usage Examples, "Configuring the Time/Time Zone").

3.2 Default Security Level

A default security level that is used when configuring new trunks or stations can be defined with AMO ZANDE:

CHA-ZANDE:TYPE=SECURITY,**SECTDMSB=<sec_level_subs_TDM>**,
SECTDMTR=<sec_level_trunks TDM>,**SECIPSB=<sec_level_ip_subs>**,
SECIPTR=<sec_level_IP_trunks>;

Parameters:

SECTDMSB (TRADITIO/SECURE):	Security level for TDM subscribers. Devault value: **TRADITIO**
SECTDMTR (TRADITIO/EXTSECUR):	Security level for TDM Trunks Devault value: **TRADITIO**
SECIPSB (STANDARD/SECURE/CIPHER):	Security level for IP subscribers Devault value: **SECURE**
SECIPTR (TRADITIO/STANDARD/SECURE/EXTSECUR):	Security level for IP Trunks Devault value: **SECURE**

3.3 SPE for IP Trunking

The following steps have to be performed:

1. Configuring the Trunk

   The AMO TDCSU is used for basic trunk configuration:

   CHANGE-TDCSU:PEN=<port equipment number>,**SECLEVEL=<security_level>**;

   The security level (**SECLEVEL**) can feature the following values:

TRADITIO:	Nonsecure trunk Default value for TDM trunks.
STANDARD:	SRTP (payload encryption) is not supported, only signaling encryption (TLS-secured)
SECURE:	Full encryption (SRTP- + TLS-secured) Default value for IP trunks.
EXTSECUR:	This trunk is encrypted by a mechanism (such as VPN) that is different from this feature. This trunk is therefore treated by call processing as "fully encrypted" but not encrypted by HiPath 4000. The other side of the trunk must be also a HiPath 4000 V4 configured also as EXTSECUR.

NOTE: The same security level will be set for all trunks associated with a board.

2. Configuring the gateway

   a) External gateway in a local-local configuration

   The external gateway does not automatically register at this system (local-local configuration). Therefore the external gateway's security level must be configured:

   CHANGE-GKREG:GWNO:=<gateway_number>,**SECLEVEL=<security_level>**;

   b) Internal Gateway

   The security level of the internal gateway is set via AMO TDCSU (with the command CHANGE-TDCSU). With AMO GKREG you can only display the actual security level but can't modify it. To modify the security level use AMO TDCSU.

   If the security level configured with the AMO TDCSU is not displayed for the internal gateway in AMO GKREG, this could be because:

   - SPE is not active (check with AMO ZANDE) or
   - certificates are not available, faulty or expired (for more information, refer to the WBM/DLS and AMO HISTA, **AMO BCSU**, **AMO SDSU**).

3. Activating SPE

   The configurations described above take effect if SPE is activated for this system:

   `CHANGE-ZANDE:TYPE=SECURITY,`**`SPESUPP=YES`**`;`

   Parameter:

SPESUPP (YES/NO):	Activates/Deactivates SPE for this system.

NOTE: You must perform a hard restart on the system after you have activated SPE. If you have a duplex system you have to perform the following command on both processors simultaneously (at the same time). This means all LTUs and APs will restart!
`EXEC-REST:TYPE=UNIT,UNIT=BP,RSLEVEL=HARD;`

AMO BCSU

Detailed information can be found in the AMO BCSU with the command `DISPLAY-BCSU:TYPE=TBL,LTG=<ltg>,LTU=<ltu>,SLOT=<slot>`; in the **SECURITY STATUS** section.

AMO SDSU

Detailed information can be found in AMO SDSU with the command `DISP-SDSU`. Refer to **SECURITY LEVEL** in the output.

```
CCT  LINE          STNO  SI BUS TYPE
             000   1702                  OPTI ONLY     READY
               MULTLINE 8. . . . . . . . . . . . . .READY
               000 NO CONN
               001 SUBUNIT . . . . . DIGITE MAIN      TRS
               (ALT_ROUT: N)        (OPTIIP  )
                 LINE: 2859 STNO: 6701          SI:VCE
                    001 . . . . . . . . DIGITE SUB A   UNACH
                    002 . . . . . . . . DIGITE SUB A   UNACH
                    003 . . . . . . . . DIGITE SUB C   UNACH
               002 NO CONN
               003 NO CONN
               004 NO CONN
               005 NO CONN
               006 NO CONN
               007 NO CONN
               008 NO CONN
               SECURITY LEVEL  . . . . . . . (CONF.)  "SECURE"
```

```
                                        (ACT.)   "UNKNOWN"
CCT  LINE         STNO  SI BUS TYPE
004  1706                 OPTI ONLY     READY
  MULTLINE 8. . . . . . . . . . . . . .READY
  000 NO CONN
  001 SUBUNIT . . . . . DIGITE MAIN     READY
  (ALT_ROUT: N)       (OPTIIP  )
    LINE: 2866 STNO: 6709          SI:VCE
      001 . . . . . . . . DIGITE SUB A   READY
      002 . . . . . . . . DIGITE SUB A   READY
      003 . . . . . . . . DIGITE SUB C   READY
  002 NO CONN
  003 NO CONN
  004 NO CONN
  005 NO CONN
  006 NO CONN
  007 NO CONN
  008 NO CONN
  SECURITY LEVEL  . . . . . . . (CONF.)  "SECURE"
                                        (ACT.)   "TRADITIO"
CCT  LINE         STNO  SI BUS TYPE
008  1710                 OPTI ONLY     READY
  MULTLINE 8. . . . . . . . . . . . . .READY
  000 NO CONN
  001 SUBUNIT . . . . . DIGITE MAIN     READY
  (ALT_ROUT: N)       (OPTIIP  )
    LINE: 2870 STNO: 6713          SI:VCE
      001 . . . . . . . . DIGITE SUB A   READY
      002 . . . . . . . . DIGITE SUB A   READY
      003 . . . . . . . . DIGITE SUB C   READY
  002 NO CONN
  003 NO CONN
  004 NO CONN
  005 NO CONN
  006 NO CONN
  007 NO CONN
  008 NO CONN
  SECURITY LEVEL  . . . . . . . (CONF.)  "SECURE"
                                        (ACT.)   "SECURE"
```

```
CCT  LINE         STNO  SI BUS TYPE
014  1716                 OPTI ONLY     READY
  MULTLINE 8. . . . . . . . . . . . . .READY
  000 NO CONN
  001 SUBUNIT . . . . . DIGITE MAIN      READY
  (ALT_ROUT: N)       (OPTIIP  )
    LINE: 2800 STNO: 6980          SI:VCE
      001 . . . . . . . . DIGITE SUB A   READY
      002 . . . . . . . . DIGITE SUB A   READY
      003 . . . . . . . . DIGITE SUB C   READY
  002 NO CONN
  003 NO CONN
  004 NO CONN
  005 NO CONN
  006 NO CONN
  007 NO CONN
  008 NO CONN
  SECURITY LEVEL  . . . . . . . (CONF.)  "CIPHER"
                                (ACT.)   "CIPHER"
```

3.4 SPE for IP Terminals

Signaling and payload encryption does not work for IP terminals unless the terminal itself is configured and the appropriate configurations are performed in the system (see Section 3.4.2, “Configuration”).

3.4.1 Supported IP Terminals

The following IP terminals are supported:

NOTE: SIP subscribers do not supported SPE! Therefore do not activate SPE at SIP subscribers.

- optiPoint 410 (HFA)
- optiPoint 420 (HFA)
- OpenStage 20 HFA
- OpenStage 40 HFA

- OpenStage 60 HFA
- OpenStage 80 HFA
- OpenStage 20 G HFA
- OpenStage 40 G HFA
- OpenStage 60 G HFA
- OpenStage 80 G HFA
- AC-Win IP
- optiClient 130

3.4.2 Configuration

1. Configuring the IP terminal in the system

   The AMO SDAT is used for basic terminal configuration:

   ```
   CHANGE-SDAT:STNO=<station
   number>,TYPE=DATA1,CLASSSEC=<security_level>;
   ```

   The security level (**CLASSSEC**) can feature the following values:

SECURE:	These terminals are allowed to connect to the HFA board with TLS or TCP depending on the terminal settings (WBM/DLS). That means that this terminal can be fully secure (SRTP+TLS) or traditional non-secure terminal, i.e. no signaling or payload encryption. This can be set via WBM/DLS of the terminal. The AMO SDAT configuration stays **SECURE** in both cases (setting of the terminal secure or non-secure). Deafult value.
CIPHER:	These terminals allow only complete encrypted direct connections. This means, that the connection to the system logged on and each DMC connection must be encrypted. This setting grants highest security but leads maybe to a lower connection quality. This setting is only applicable for HFA endpoints. For a terminal configured as **CIPHER** it is **not allowed to deactivate SPE** on the terminal (WBM/DLS).

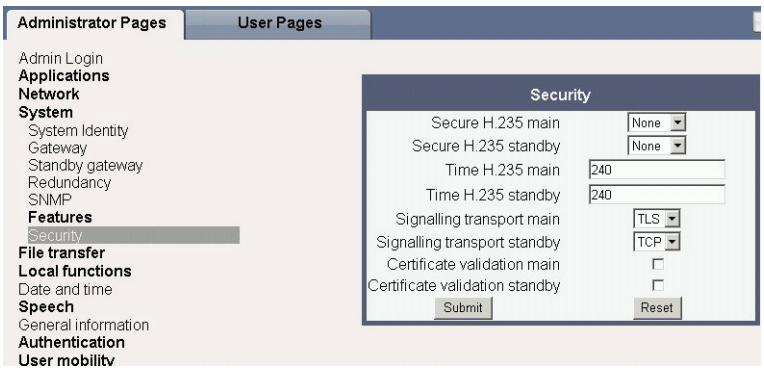
   NOTE: IP terminals can only be configured as SECURE or CIPHER in AMO SDAT. Other values are available in the AMO but cannot be meet for HFA IP terminals.

2. Configuring SPE at the terminal

   SPE settings are performed at the terminal either with DLS/WBM or via the terminal itself. Signaling and display settings can also be performed at the terminal.

OpenStage WBM

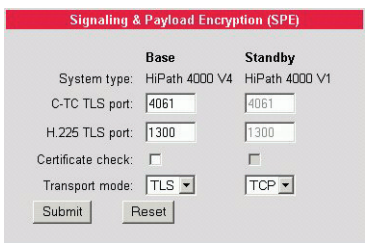
(Tab sheet) **Administrator Pages > System > Security**



optiPoint WBM

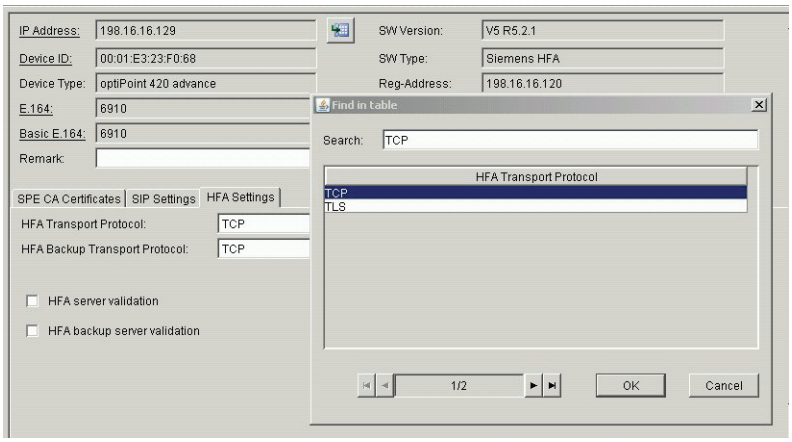
In this menu it can be defined whether the **Transport mode** TLS orTCP is used. Additionally the setting can be done that the SPE certificate will be check by the CA certificate (check box **Certificate check**).

Admin > System > Signaling & Payload Encryption (SPE)



DLS

IP Devices > IP Phone Configuration > Signaling and Payload Encryption (SPE)



Detailed Information / Documentation

For more information please refer to the relevant documentation:

Deployment Service

- Deployment Service V2

  http://apps.g-dms.com:8081/techdoc/de/P31003S2320M1000100A9/index.htm

Operating Manual for OpenStage Terminals

- OpenStage 40 HFA

  http://apps.g-dms.com:8081/techdoc/de/P31003S2000U105010019/index.htm

- OpenStage 60/80 HFA

  http://apps.g-dms.com:8081/techdoc/de/P31003S2000U108010019/index.htm

Administrator Manual for OpenStage Terminals

- OpenStage HFA

  http://apps.g-dms.com:8081/techdoc/en/P31003S2010M1000176A9/index.htm

optiPoint 410

- optiPoint 410 advance

  http://apps.g-dms.com:8081/techdoc/de/P31003H8400B413010019/index.htm

- optiPoint 410 economy/standard

http://apps.g-dms.com:8081/techdoc/de/P31003H8400B412010019/index.htm

- optiPoint 410 entry

  http://apps.g-dms.com:8081/techdoc/de/P31003H8400B411010019/index.htm

optiPoint 420 Operating Manual

- optiPoint 420 advance

  http://apps.g-dms.com:8081/techdoc/de/P31003H8400B423010019/index.htm

- optiPoint 420 economy/standard

  http://apps.g-dms.com:8081/techdoc/de/P31003H8400B422010019/index.htm

optiPoint 410/420 Administrator Manual

- optiPoint 410/420 Administrator Manual

  http://apps.g-dms.com:8081/techdoc/de/P31003A2056B4150100A9/index.htm

3. Activating SPE

   The configurations described above take effect if SPE is activated for this system:

   `CHANGE-ZANDE:TYPE=SECURITY,`**`SPESUPP=YES`**`;`

   Parameter:

SPESUPP (YES/NO):	Activates/Deactivates SPE for this system.

NOTE: You must perform a hard restart on the system after you have activated SPE. If you have a duplex system you have to perform the following command on both processors simultaneously (at the same time). This means all LTUs and APs will restart!
`EXEC-REST:TYPE=UNIT,UNIT=BP,RSLEVEL=HARD;`

3.4.3 Signaling at the Display

A connection is displayed as "encrypted" if all sections (signaling & payload) and the DMC path (signaling & payload) between all terminals involved in this call are encrypted.

3.4.3.1 Display in Call State

If you want the terminal's display to indicate whether or not a call is encrypted, you must first enable the parameter **SECLVDSP** in the AMO ZANDE for the entire system.

```
CHANGE-ZANDE:TYPE=SECURITY,SECLVDSP=YES;
```

The **SECLVDSP** attribute must also be activated in AMO SDAT on the terminals where the display is to appear.

```
CHA-SDAT:STNO=<station number>,TYPE=ATTRIBUT,AATTR=SECLVDSP;
```

NOTE: If you want a display to appear, the parameter **SECLVDSP** must be activated in both AMO ZANDE and AMO SDAT.
The status of the call is only displayed for 5 seconds. Then the display doesn't show wether the call is secure or non secure.

You can use the AMO SDAT, parameter **AATTR=SECLVTON** to make sure that the secure station also receives an advisory tone if the call is not encrypted.

```
CHANGE-SDAT:STNO=<station number>,TYPE=ATTRIBUT,AATTR=SECLVTON;
```

3.4.3.2 Display in Idle State

The terminal's idle display does not indicate whether the station is secure or not.

Display via key

You can configure a key in AMO TAPRO to display the status of the station:

e.g.: `CHANGE-TAPRO:STNO=<station number>,KY09=SECURE;`

Please note that the first eight keys are preprogrammed in OpenStage terminals.

Display via SPE entry in menu

You can also check the security status of the terminal in idle call state using the terminals menu.

- **Voice encryption not enabled**
  - The subscriber is connected to the switch via TLS but SPE is not activated for this terminal or
  - The subscriber is connected to the switch via TCP. In this case terminal configuration at the switch is not relevant.

  In this case encryption is always disabled (**Voice encryption not enabled**).
- **Voice encryption enabled**

The subscriber is connected to the switch via TLS and the subscriber is configured as a **SECURE** client.

In this case encryption is enabled (**Voice encryption enabled**).

- **Voice encryption always active**

  The subscriber is connected to the switch via TLS and the subscriber is configured as a **CIPHER** client.

  – Logon via TCP not possible.

  – All media streams are encrypted (at least to the gateway).

  In this case encryption is always active (**Voice encryption always active**).

3.4.3.3 Scenarios

- Client A - Standard client

  The subscriber is connected to the switch via TLS but SPE is not activated for this terminal or the subscriber is connected to the switch via TCP (terminal configuration at the switch is not relevant).

- Client B - Secure client

  The subscriber is connected to the switch via TLS and the subscriber is configured in the system as a **SECURE** client.

- Client C - Cipher client

  The subscriber is connected to the switch via TLS and the subscriber is configured in the system as a **CIPHER** client.

Secure call: B calls C

Both subscribers have a secure connection to the gateway. Therefore the DMC connection is also secure. The displays of both subscribers show **encrypted call** for 5 seconds. During the call both subscribers are able to check the security status in there menus (status will be displayed for 5 seconds).

Non Secure Call: A calls B

The connection from A to the gateway is not secure. Only the connection from the gateway to client B is secure. Therefore the DMC connection is not secure. The display of both subscribers show **call not encrypted** for 5 seconds. During the call both subscribers are able to check the security status in there menus (status will be displayed for 5 seconds).

Non Secure Call: A calls C

The connection from A to the gateway is not secure. Only the connection from the gateway to client C is secure. Therefore the DMC connection if it is established is not secure. The DMC connection ends in the HiPath 4000 because all

connections to client c (CIPHER) must be secure. The display of both subscribers show **call not encrypted** for 5 seconds. During the call both subscribers are able to check the security status in there menus (status will be displayed for 5 seconds).

3.5 SPE for IPDA

The following steps have to be performed for activating SPE for IPDA:

1. Distribute **M**aster **E**ncryption **K**ey (**MEK**) via HiPath 4000 Assistant to **all** APs configured in the system (states **Ready**, **NPR** (not present) and **UNACH** (hierarchically blocked)).

   This will

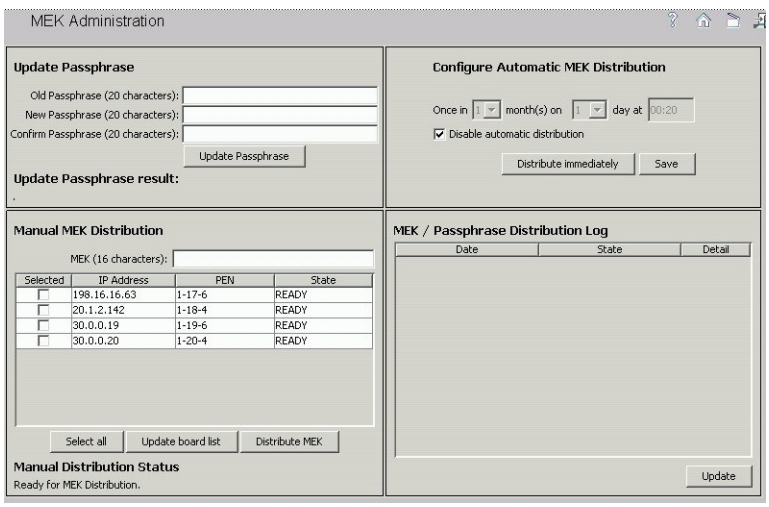
   - configure the MEK in the RMX for all APs regardless of their state and
   - transmit the MEK to all APs in **Ready** state.

   The **M**aster **E**ncryption **K**ey (MEK is used to encrypt the signaling data between the HiPath host system and an IPDA access point.

   The MEK must be set first on the NCUI boards and then on the HiPath host system.

   The MEK is configured via HiPath Assistant:

   Expert Mode > MEK Administration > sections **Configure Automatic MEK Distribution** and **Manual MEK Distribution**



   For more information on MEK administration, refer to the administration manual „HiPath 4000 Assistant V5, MEK Administration“ (http://apps.g-dms.com:8081/techdoc/de/P31003H3450M1440100A9/index.htm).

2. Check the Log from MEK client and see if any AP failed.

Expert Mode > MEK Administration > section **MEK / Passphrase Distribution Log**

3. For APs with state **NPR** and **UNACH** you need to enter the MEK manually via CLI on the AP using command `Set new MEK XXXXXXXX`.
4. After MEKs are configured for all APs successfully you can activate SPE.

   The IPDA encryption is activated with AMO SIPCO, parameter **IPDAENCR**:

   ```
   CHANGE-SIPCO:TYPE=SECURITY,IPDAENCR=YES;
   ```

   IPDAENCR (YES/NO): Signaling and voice encryption for IPDA connections.

   SPE activation for IPDA fails when MEKs are not configured for all APs (refer to point 1 to 3).
5. After the activation with AMO SIPCO you need to hard restart the system.

IMPORTANT: If you have a duplex system you have to perform the hard restart command on both processors simultaneously (at the same time). This means all LTUs and APs will restart!

```
EXEC-REST:TYPE=UNIT,UNIT=BP,RSLEVEL=HARD;
```

Exception

A soft restart is enough, if

- no common gateways inside the IPDA
- no HFA terminals inside the IPDA
- only TDM terminals inside the IPDA
- common gateways inside the IPDA need no encryption
- HFA terminals inside the IPDA need no encryption

Example: Soft restart of the active BP

```
EXEC-REST:TYPE=UNIT,UNIT=BP,RSLEVEL=SOFT;
```

6. If you have common gateway boards and HFA terminals in the IPDA shelf and they should act as secure you have to perform all steps that are necessary as if the common gateway board and the HFA terminals are in the host system (activate SPE with AMO ZANDE parameter **SPESUPP**, import certificates and so on).

   Related topics:

   - SPE for IP Trunking
   - SPE for IP Terminals
   - Distribution of Certificates to a Common Gateway Board with DLS

- Distribution of Certificates to a Common Gateway Board with the WBM of the Board
- Distribution of a CA Certificat to Terminals with DLS

7. If you need to add a new AP while IPDA security is already active, you need to do the following:
   - Configure the AP in the system normally with AMO UCSU, AMO APRT.
   - Don't connect the AP now because it will fail.
   - Use the MEK client administration in HiPath 4000 Assistant and update the board list to see your new AP.

     Expert Mode > MEK Administration > section **Manual MEK Distribution >** button **Update board list**
   - Configure a MEK manually for this AP. This will transmit the MEK to the RMX.
   - Use the CLI to configure the same MEK on the NCUI.
   - Now you can connect the AP to the LAN and activate the connection to the system via `EXEC-USSU:MODE=CONFAP,LTU=<ltu_number>;`.

3.6 SPE for HiPath 4000 SoftGate

See section HiPath 4000 SoftGate, Chapter 10, “Signalling and Payload Separation (SPE) for HiPath 4000 SoftGate”.

3.7 SPE in Analog/TDM Endpoints

IMPORTANT: The configuration of analog and TDM endpoints has no effect on their behavior. The only purpose of this configuration is the determination of end-to-end encryption. Then the connection will be treated by call processing as encrypted but it isn’t really encrypted.

```
CHA-SDAT:STNO=<station
number>,TYPE=DATA1,CLASSSEC=<security_level>;
```

The security level (**CLASSESEC**) can feature the following values:

TRADITIO: Nonsecure endpoint
Devault value.

SECURE: Full encryption (SRTP- + TLS-secured)
The phone is secured by external means but not encrypted by HiPath 4000. Call processing will consider this phone as a full secure phone.

3.8 SPE in Analog/TDM Trunks

NOTE: The configuration of analog and TDM trunks has no effect on their behavior. The only purpose of this configuration is the determination of end-to-end encryption. Then the connection will be treated by call processing as encrypted but it isn't really encrypted.

`CHA-TDCSU:PEN=<port equipment number>,SECLEVEL=<security_level>;`

The security level (**SECLEVEL**) can feature the following values:

TRADITIO: Nonsecure trunk

EXTSECUR: This trunk is encrypted by a mechanism (such as VPN) that is different from this feature. This trunk is therefore treated by call processing as "fully encrypted" but not encrypted by HiPath 4000. The other side of the trunk must be also a HiPath 4000 V4 configured also as EXTSECUR.

3.9 Activating/Deactivating the SPE Feature for Subfunctions in the System

SPE subfunctions can be deactivated - and in some cases even reactivated - without a restart. This allows service personnel to deactivate specific SPE subfunctions in problem situations, on the one hand, to verify if the problem is caused by SPE and, on the other hand, to pinpoint the cause of the fault.

IP terminals

Deactivating SPE

You can use DLS/WBM to deactivate SPE for all IP terminals (HFA terminals) (see Section 3.4.2, "Configuring SPE at the terminal"). This causes all terminals to logoff and then logon via TCP.

The common gateway boards themselves remain in secure mode, but **no** encryption is used as long as all clients are connected via TCP.

Cipher clients will not work correctly unless they are modified in AMO SDAT to **SECURE**.

Activating SPE

As for deactivation, again using DLS/WBM (see Section 3.4.2, “Configuring SPE at the terminal”).

Terminals will logoff and logon when SPE is activated or deactivated.

NOTE: The common gateway boards must already be in secure mode as otherwise the clients are unable to register.

SIP-Q/IP trunking in local-local configuration

Deactivating SPE

SPE can be deactivated without reboots.

The reduction of the security level from **SECURE** to **TRADITIO** for a partner gateway (**AMO GKREG**, parameter **SECLEVEL**) means that all subsequent calls are set up via TCP or UDP. SPE is therefore deactivated for all subsequent calls to the relevant partner gateway.

The ongoing calls are maintained on TLS just as the TLS connection is maintained, even if all associated calls are ended. The common gateway itself also remains in secure mode.

NOTE: If you want to deactivate SPE for incoming calls from this partner gateway, you must also reconfigure the AMO GKREG at the partner system (parameter **SECLEVEL=TRADITIO**).

Activating SPE

SPE can be activated without reboots.

As for deactivation, again with the AMO-GKREG.

NOTE: The common gateway boards must already be in secure mode. Do not overlook possible changes in the partner system when performing activation (AMO GKREG, **SECLEVEL=SECURE**).

IP/SIP-Q trunking in local-remote configuration

Deactivating SPE

Reset the LEGK local common gateway or gateways (also known as LEGK server nodes) to **TRADITIO** (AMO TDCSU, **SECLEVEL=TRADITIO**) and perform a reboot.

NOTE: This causes all remote common gateways (also known as LEGK client nodes) to reregister and therefore fall back to **TRADITIO**. In addition, each of these remote common gateways generates an alarm (because of the fall back) that is deleted once the remote common gateway returns to secure mode (**SECLEVEL=SECURE**).

Activating SPE

As for deactivation, with the AMO TDCSU

NOTE: Like deactivation, this action also causes all remote common gateways (also known as LEGK client nodes) to reregister, meaning they are once again able to support secure trunks.
If a remote common gateway generated an ALARM during SPE fall back, it is now deleted.

IPDA

Deactivating SPE

IPDA encryption (signaling and payload) is deactivated with the AMO SIPCO and followed by a soft restart. In a duplex system, you also only have to perform **one** soft restart on the active CC.

NOTE: The deactivation of IPDA encryption causes every call and the associated DMC connections with IPDA reference (subscriber or trunk in AP shelf) to be executed and signaled as non-secure calls from an end-to-end perspective. The connections between the common gateway in the AP shelf and the HFA terminals or the partner gateway, however, remain encrypted, i.e. in IPDA shelves TLS terminals will still run on TLS and trunking gateways which have already estabiled TLS connection will continue haveing TLS connections.

Activating SPE

Like deactivation, with the AMO SIPCO and soft restart.

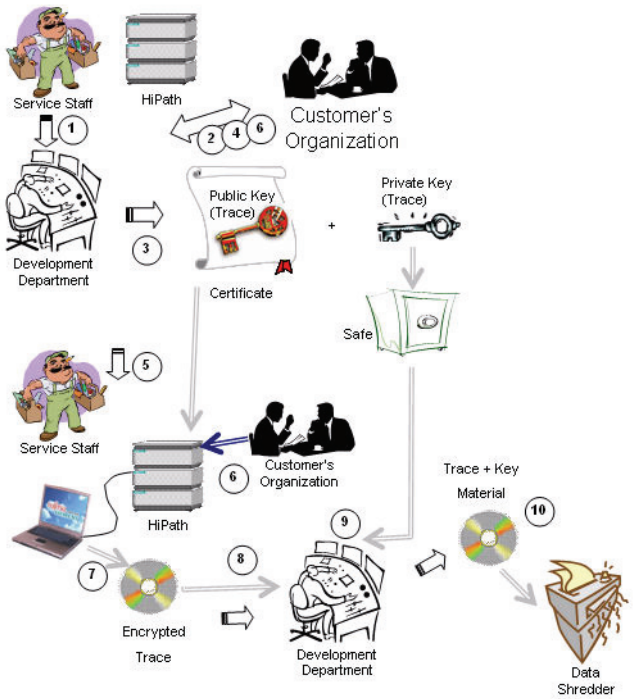
Note

The AMO SIPCO prompts the administrator to perform a hard restart after activating/deactivating SPE. This advisory is not modified for the following reasons:

- When SPE is already activated on the system for HFA terminals and IP trunking and IPDA encryption is activated for the first time a hard restart must be performed before the feature works correctly on the common gateways that are configured in AP shelves..
- If a customer would like to deactivate SPE completely for IPDA and the relevant common gateway a hard restart must be performed for this.

4 Secure Trace

Following an error, secure trace is used to let a service technician access conventional analysis options even though SPE is active.



Important note:
The right to evaluate trace information is reserved solely for service personnel and is subject to customer approval.

4.1 Configuration

Siemens Security Office CA produces a new secure trace pair of keys (public & private) every 15 days. These keys are valid for one month.

Public Key

The public key of this pair is published on the following intranet pages in X509 certificat format.

- https://sectels.mchh1.siemens.de/SecureTrace/
- http://prodsu.mch4.siemens.de/secure/index.htm
- https://sectels.mchh1.siemens.de/wiki/index.php/SecureTrace

This key (public key of the secure trace certificate) will be imported on the gateways when secure trace needs to be activated.

The Publich Certificate of Siemens Security Office CA is included in the loadware. This certificate is used to authenticate the Secure Trace Public certificate imported to the baord, i.e. verify that it is signed by Siemens Security Office.

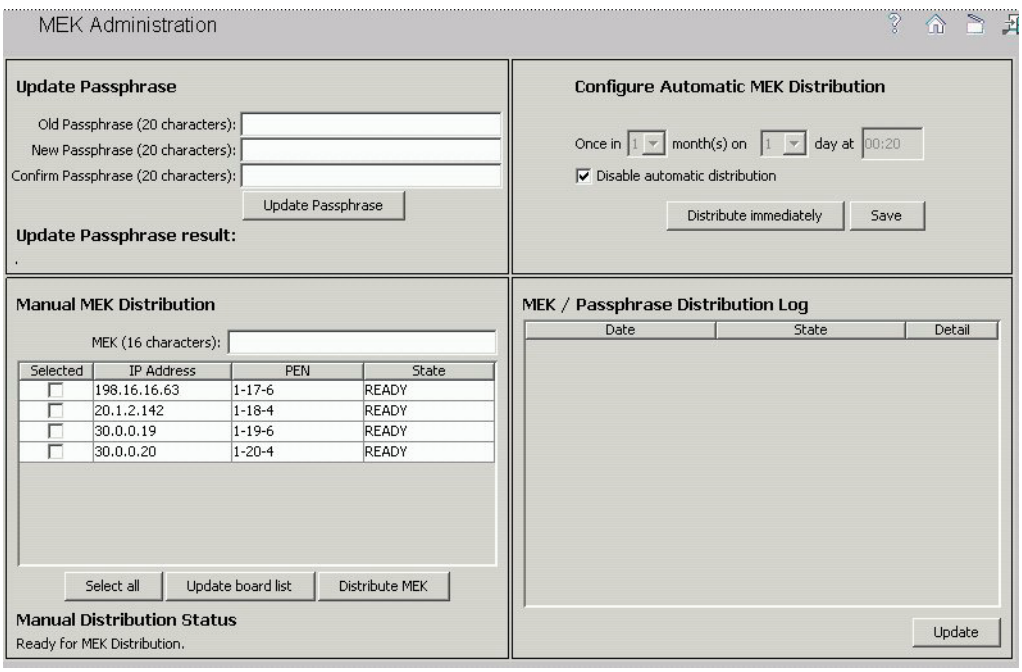
Private Key

Beside the secure trace public certificat / key the customer must set a confidential password (**Passphrase**) when installing a system. This passphrase is needed to activate secure trace.

If the passphrase is lost new system generation is mandatory. The old passphrase can't be retrieved by any means.

The passphrase is configured by HiPath 4000 Assisatnt:

Expert Mode > MEK Administration Client > Section **Update Passphrase**



4.2 Recording

The following prerequisites must be satisfied to activate secure trace:

- You must have a valid secure trace certificate:
  - signature check ok

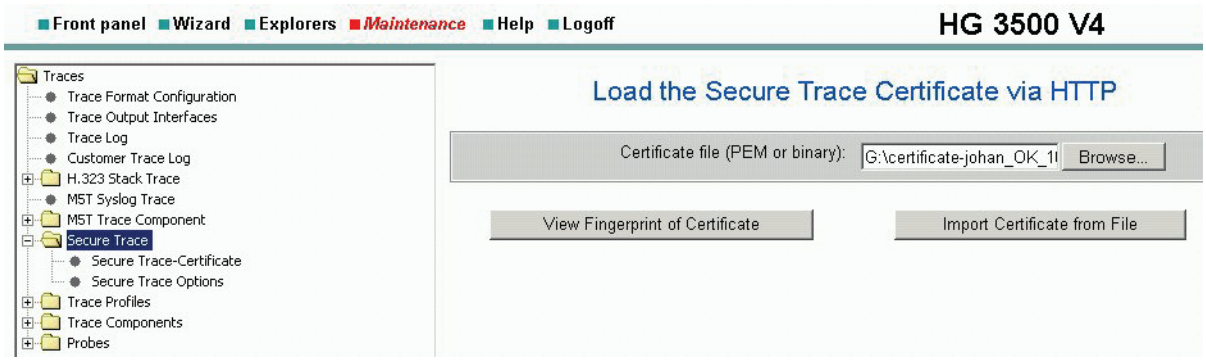
  - expiry date ok
  - format in X509
- the passphrase set for initial installation must be provided by the customer.
- SPE must be activated.

4.2.1 Loading a Secure Trace Certificate

The secure trace certificate is loaded via WBM.

Maintenance > Traces > Secure Trace > (right click) **Import Secure Trace certificates (.cer)**

The **Load the Secure Trace Certificate via HTTP** mask is displayed. Browse for the .cer file. **Press View Fingerprint of Certificate**. Now import the certificate with the **Import Certificate from File** button.

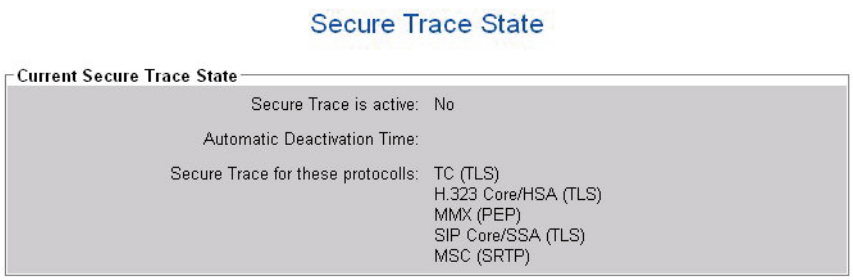


4.2.2 Secure Trace State

To determine the current status of a secure trace (activated or deactivated), select

Maintenance > Traces > Secure Trace > Secure Trace Options.

The **Secure Trace State** mask is displayed.



4.2.3 Activating a Secure Trace

Secure trace beacons are inserted in the IP current and are recorded with a network trace tool (such as Wireshark). This recording tool should be connected before you activate secure trace and must run for the entire duration of the trace.

Maintenance > Traces > Secure Trace > Secure Trace Options > (right-click) **Start Secure Trace**

The passphrase (**Secure Trace Activation Passphrase**) must be entered in this mask along with the trace duration in seconds (**Duration of Secure Trace (s)**).

You can select the required trace content under **Secure Trace protocols**:

- HFA endpoints:
  - **TC (TLS)**
  - **H.323 Core/HSA (TLS)**
- H.323 trunking signaling -> **H.323 Core/HSA (TLS)**
- IPDA signaling -> **MMX (PEP)**
- SIP trunking signaling -> **SIP Core/SSA (TLS)**
- Payload data (SRTP) -> **MSC (SRTP)**

Click **Start Secure Trace** to start secure trace.

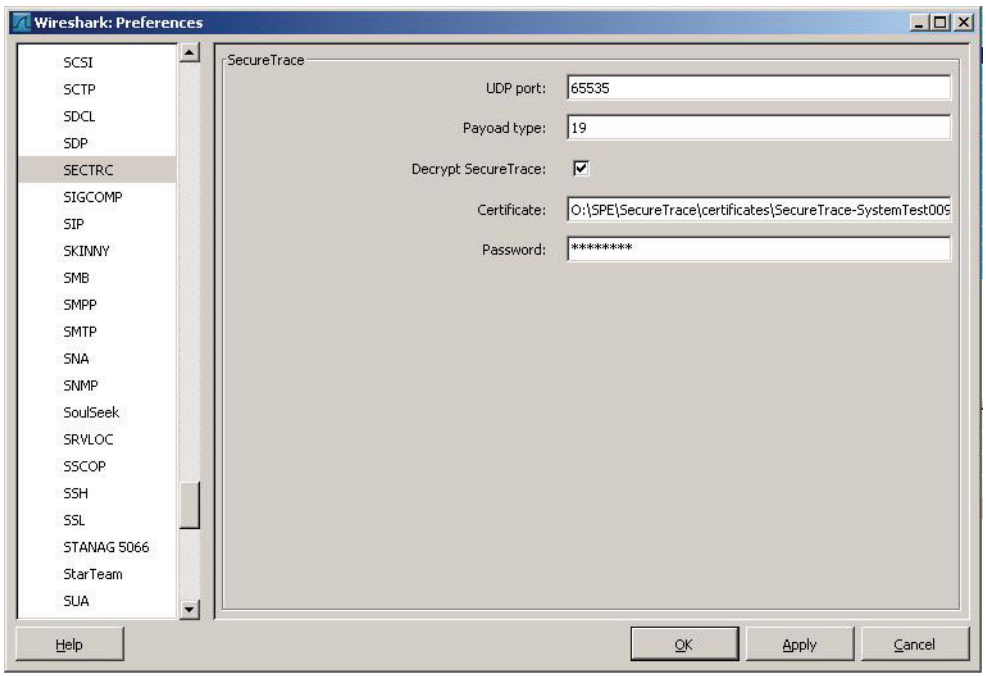
4.3 Decryption of Traces

To be able to read secure trace, you will need:

1. Wireshark HiPath plug-in (available on the GVS home page)
2. Secure trace "Private key" file (.p12 file)
3. Secure trace "Private key" password (.p12 file password)

Configuring secure trace in Wireshark

Before you load the trace file, you must enter the secure trace "Private key" file (**Certificate**) and the secure trace "Private key" password (**Password**) in Wireshark under **Edit > Preferences ... > Protocols > SECTRC**.



The signaling packets are automatically displayed in unencrypted format if all previous step were performed correctly.

With Wireshark you are able to unencrypt the signaling information.
To read the encrypted payload only development has the necessary tools.

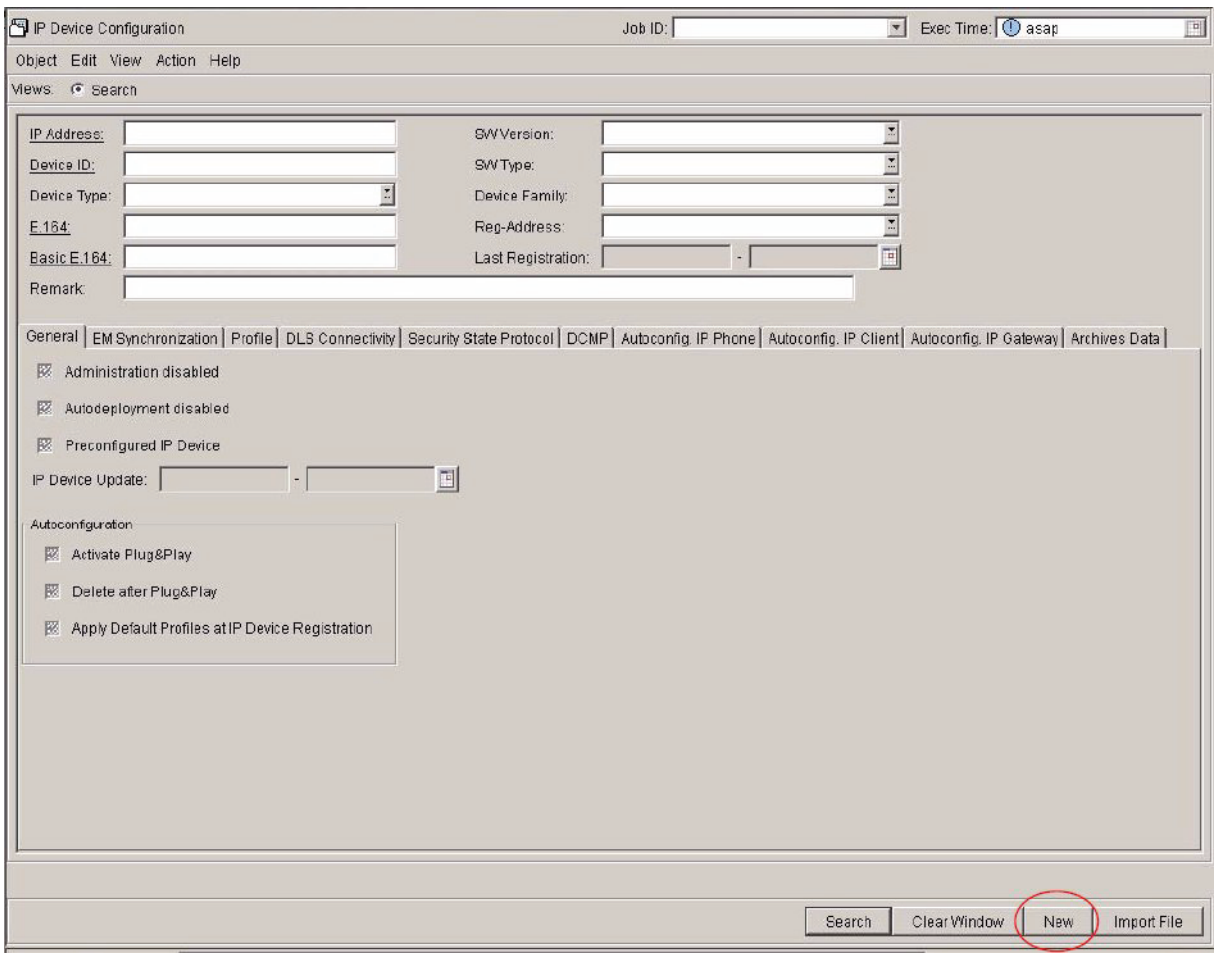
5 Distribution of Certificates to a Common Gateway Board with DLS

This chapter is only intended as a brief overview of the necessary steps in DLS. For a detailed description, refer to the DLS V2 Administrator Manual: (http://apps.g-dms.com:8081/techdoc/de/P31003S2320M1000100A9/index.htm).

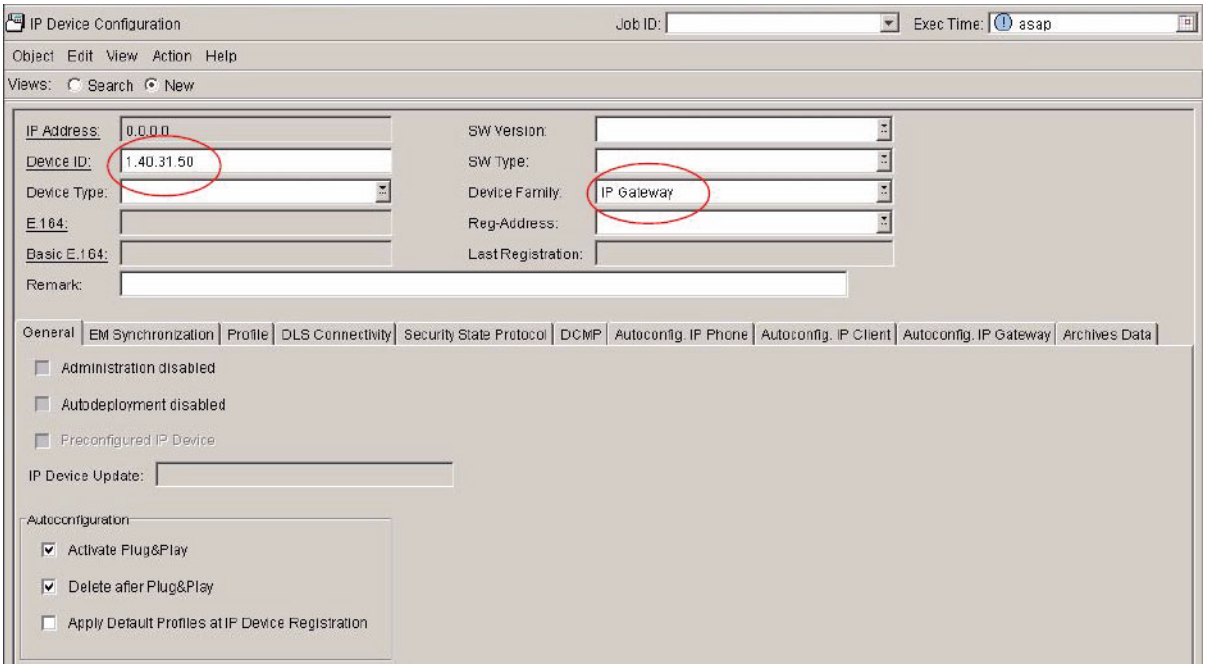
5.1 Create Virtual IP Device

IP Devices > IP Device Management > IP Device Configuration

Press button **New** to create a new virtual IP device.



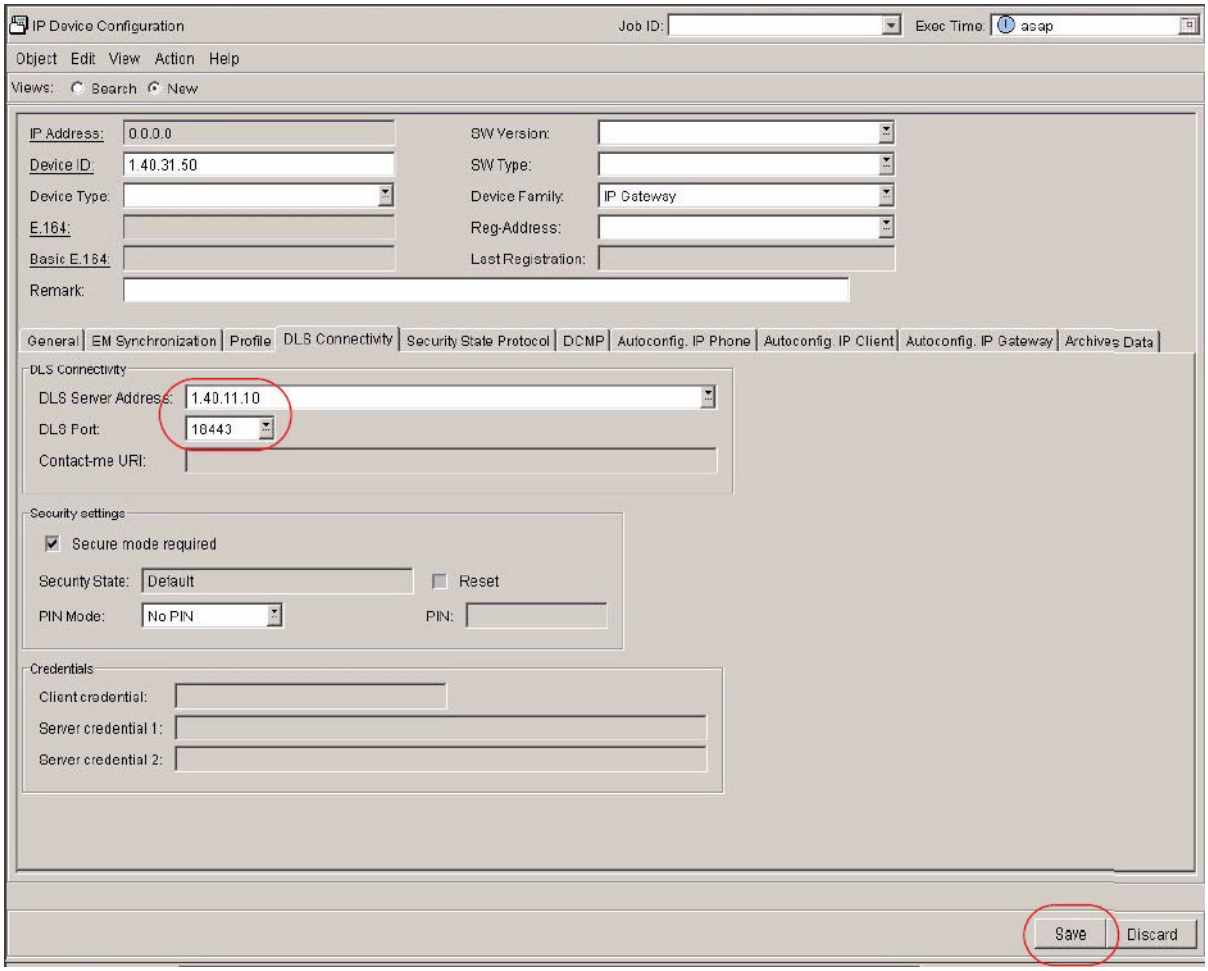
General tab: Set **Device Family** (IP gateway) and **Device ID** (IP address of common gateway board)



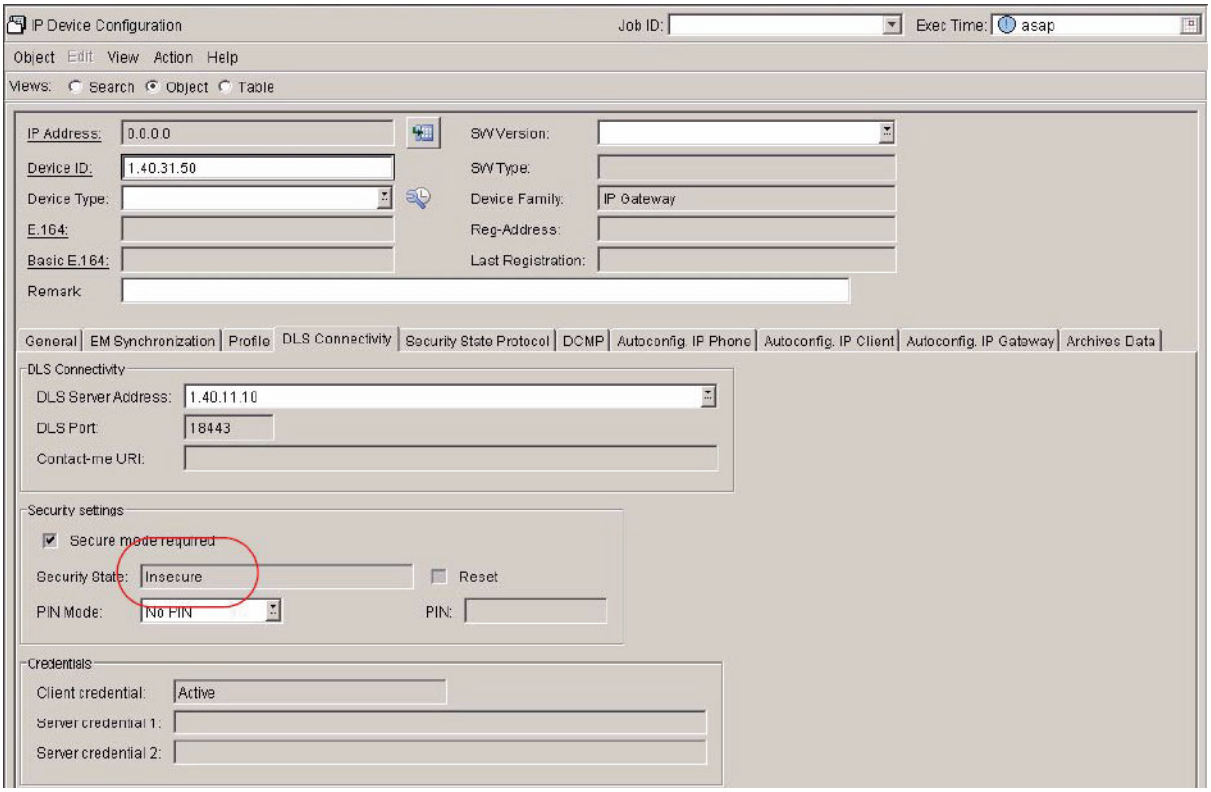
DLS Connectivity tab: **DLS Server Address** (DLS IP address) and **DLS Port** (18443) must be set.

The DLS port must also be set in AMO ZANDE parameter **DLSPORT**:

```
CHANGE-ZANDE:TYPE=DLS,DLSPORT=18443;
```



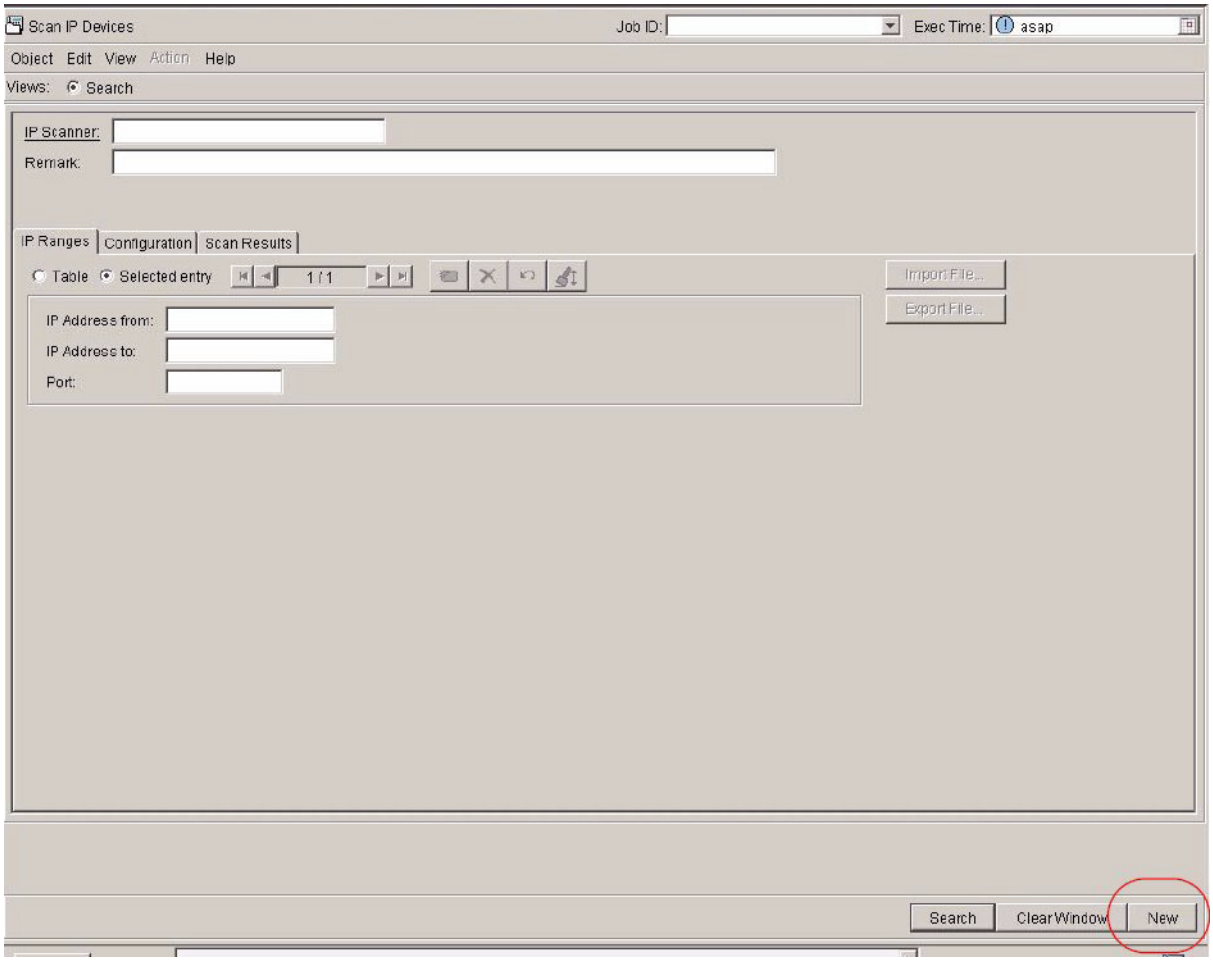
After saving the **Security State** changes from **Default** to **Insecure**.



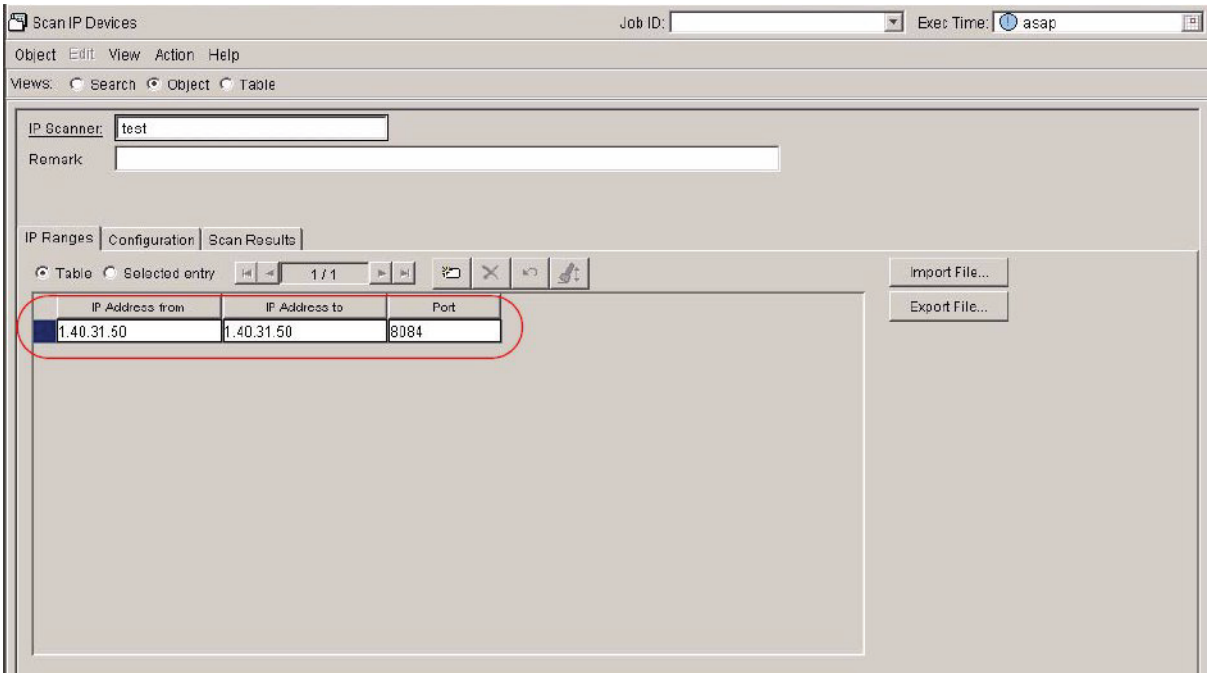
5.2 Scanning the IP Devices (IP gateways)

Bootstrapping: By scanning the IP devices (common gateways) the DLS sends a certificate to the gateway to prepare a secure connection for imporitng the „customer certificates“ (CA and certificate).

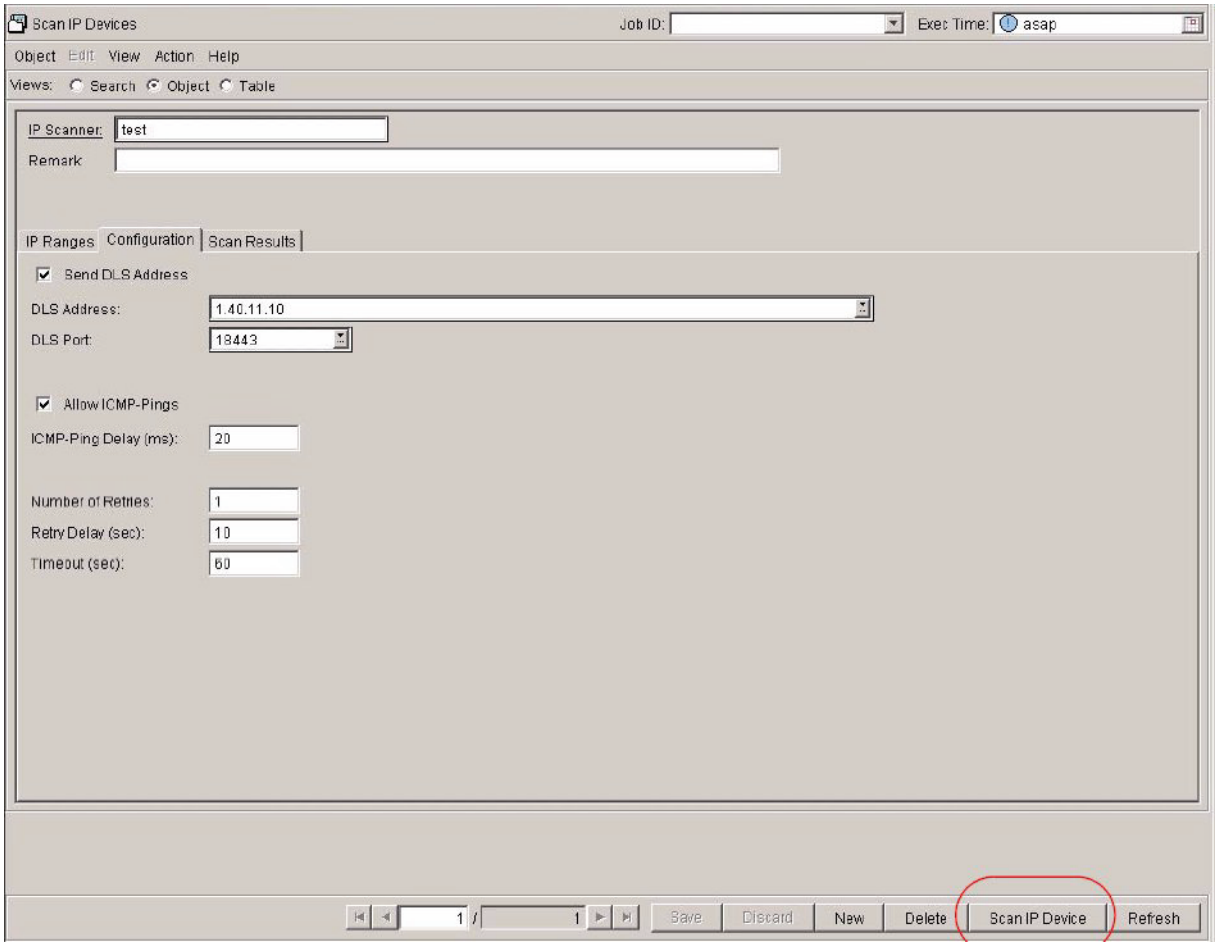
IP Device > IP Device Interaction > Scan IP Device



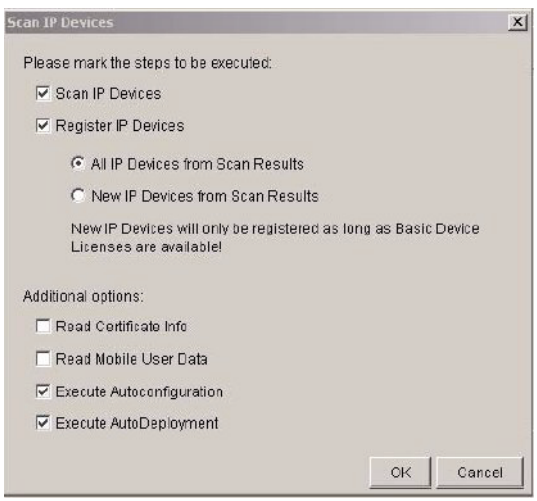
IP Ranges tab: Set name for the **IP Scanner**, IP address range (**IP Address from**, **IP Address to**) and **Port 8084**.



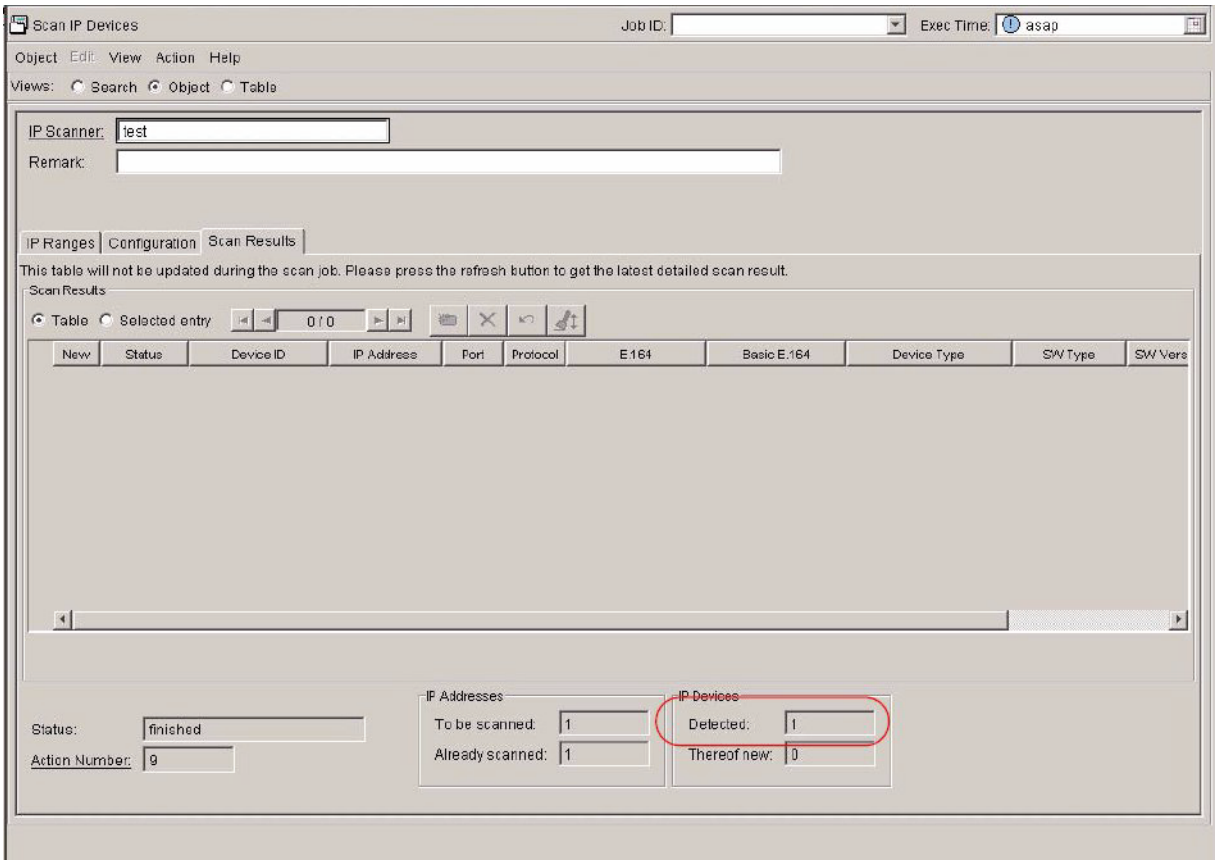
Configuration tab: Set IP Address of DLS (**DLS Address**) and **DLS Port** and select check box **Send DLS Address**. Start the scan with the button **Scan IP Devices**.



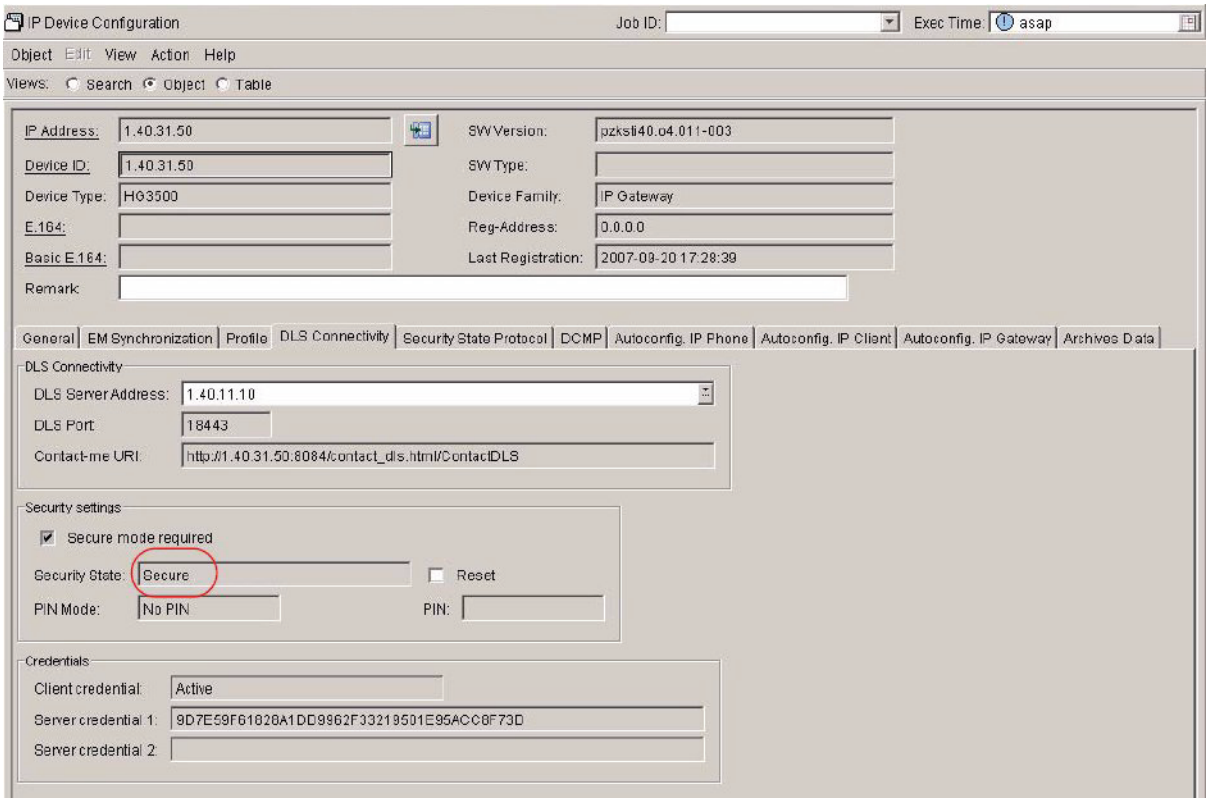
Select **Scan IP Devices**, **Register IP Devices** and **All IP Devices from Scan** and then select **OK**.



Scan Results tab: Number of detected gateways (**IP Devices > Detected**) will be shown.



DLS Connectivity tab: Status of the gateway (**Security State**) is now **Secure**.

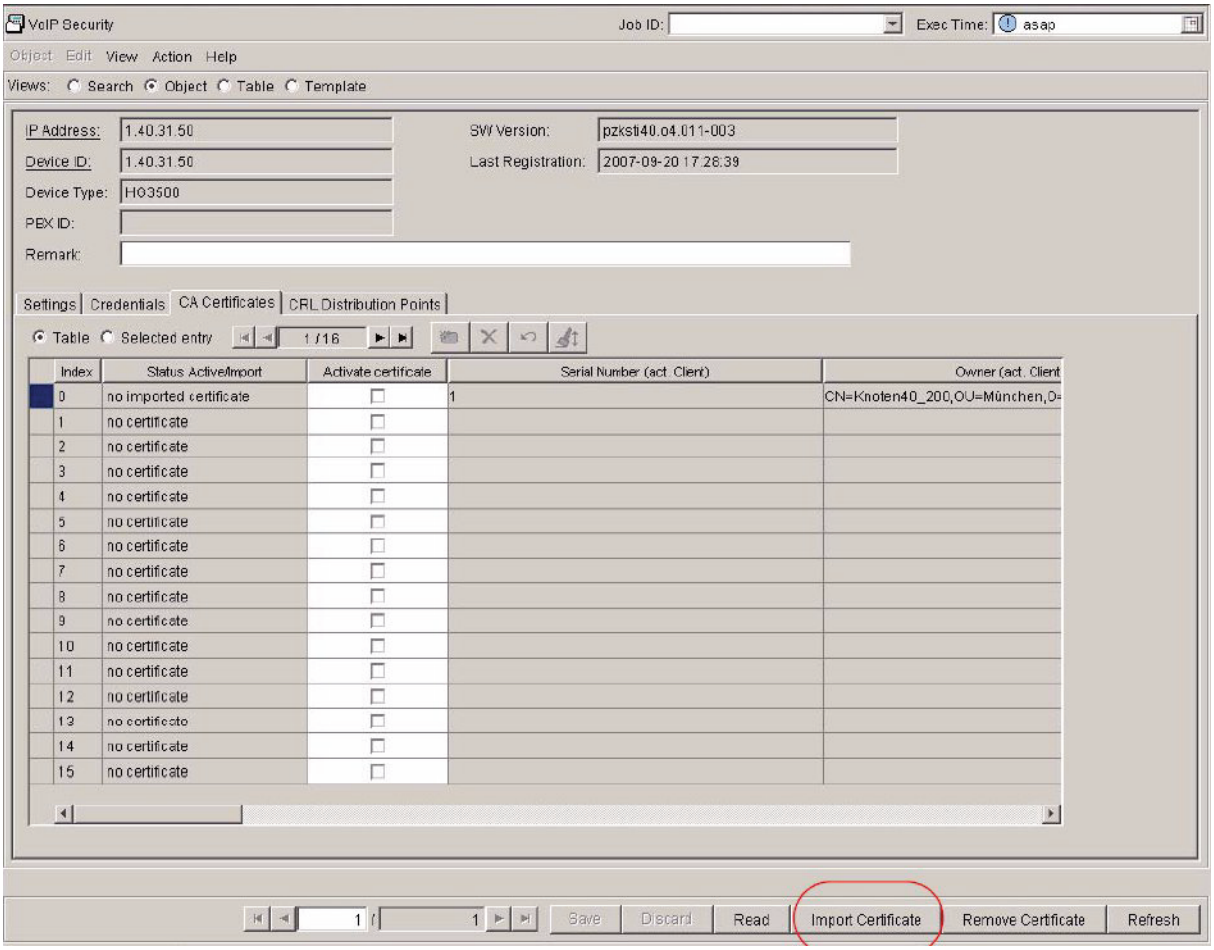


5.3 Distribution of the CA Certifcate

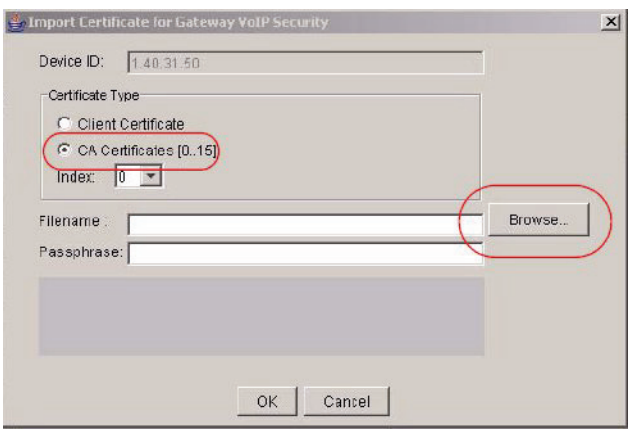
Import CA certificate: **IP Devices > IP Gateway Configuration > VoIP Security**

All detected boards will be shown by using the radio button **Search**.

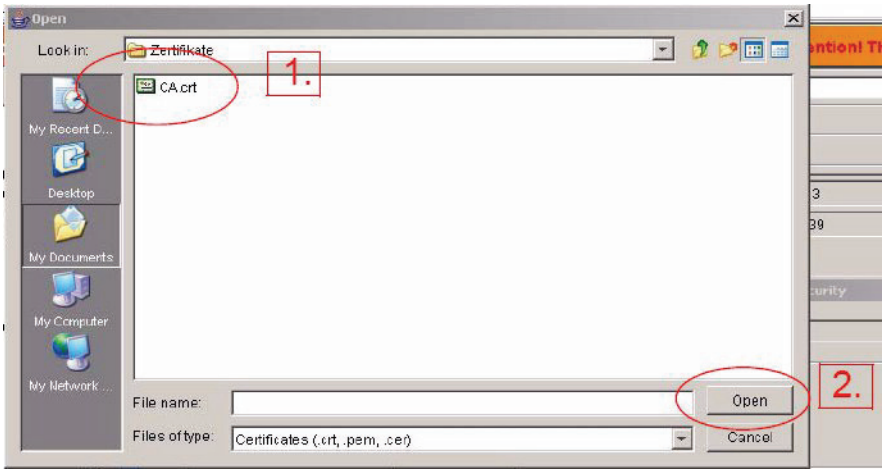
Press button **Import Certificate**.



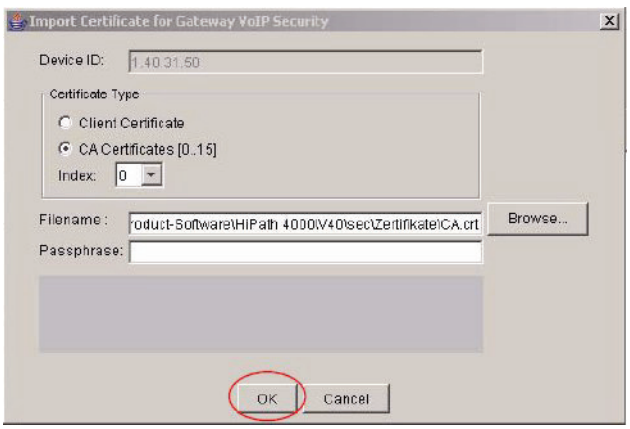
No a new window appears where you can browse for the CA certificate. Up to 16 CA certificates can be imported.



Select CA certiicate



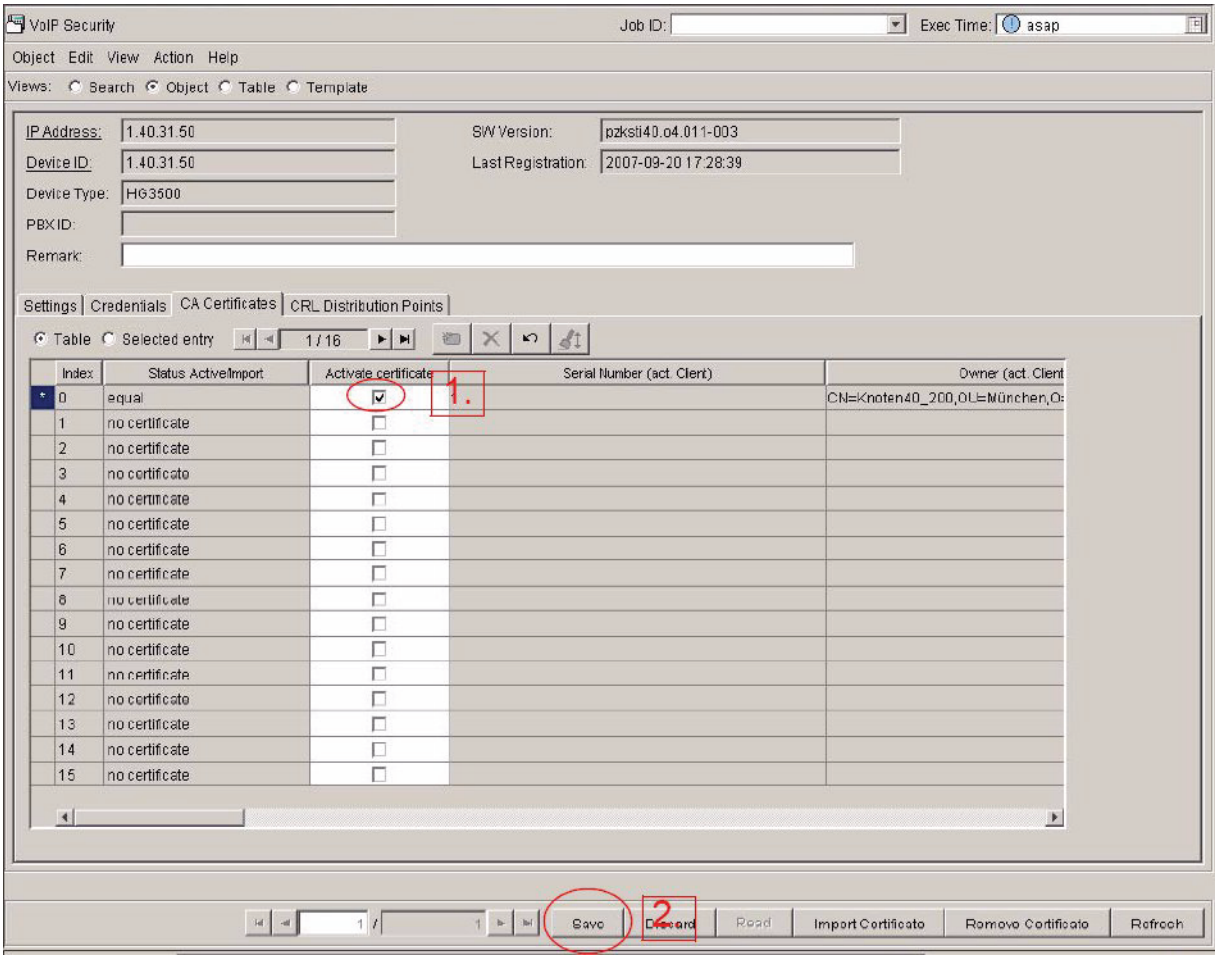
Confirm CA certificate.



Activate CA certificate.

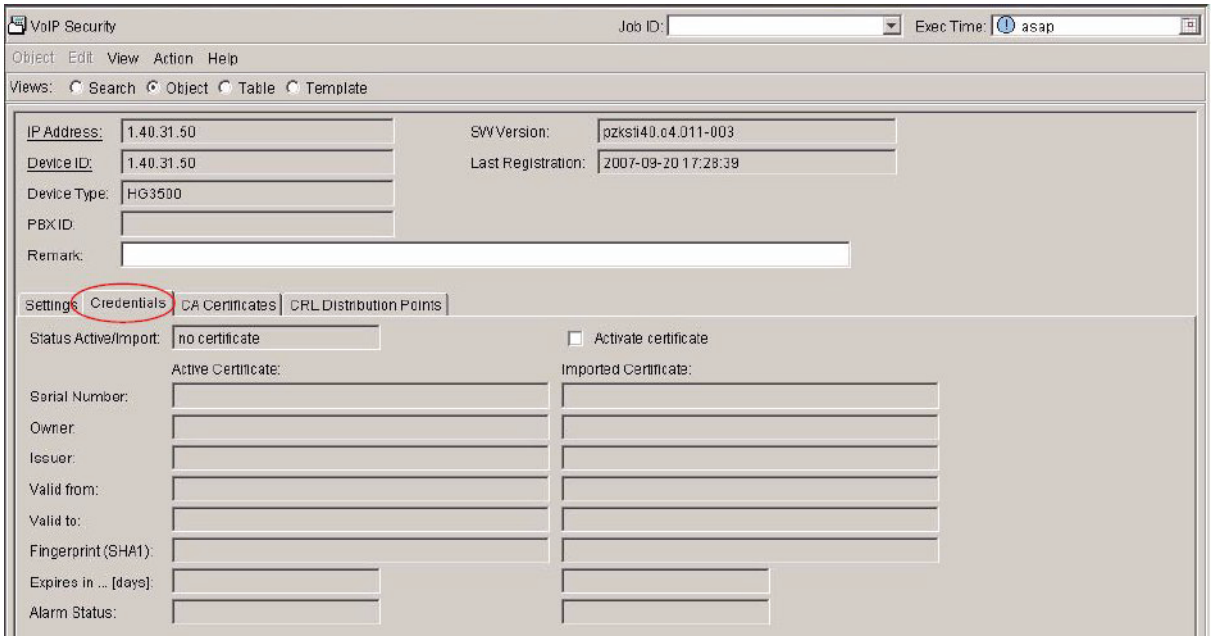
Activate the check box **Activate certificate** and with **Save** the certificate can be activated.

The status of the imported certificate will change from **no active certificate** to **equal** if the certificate is valid. Additionally some data will be read by the DLS e.g. CN, OU.

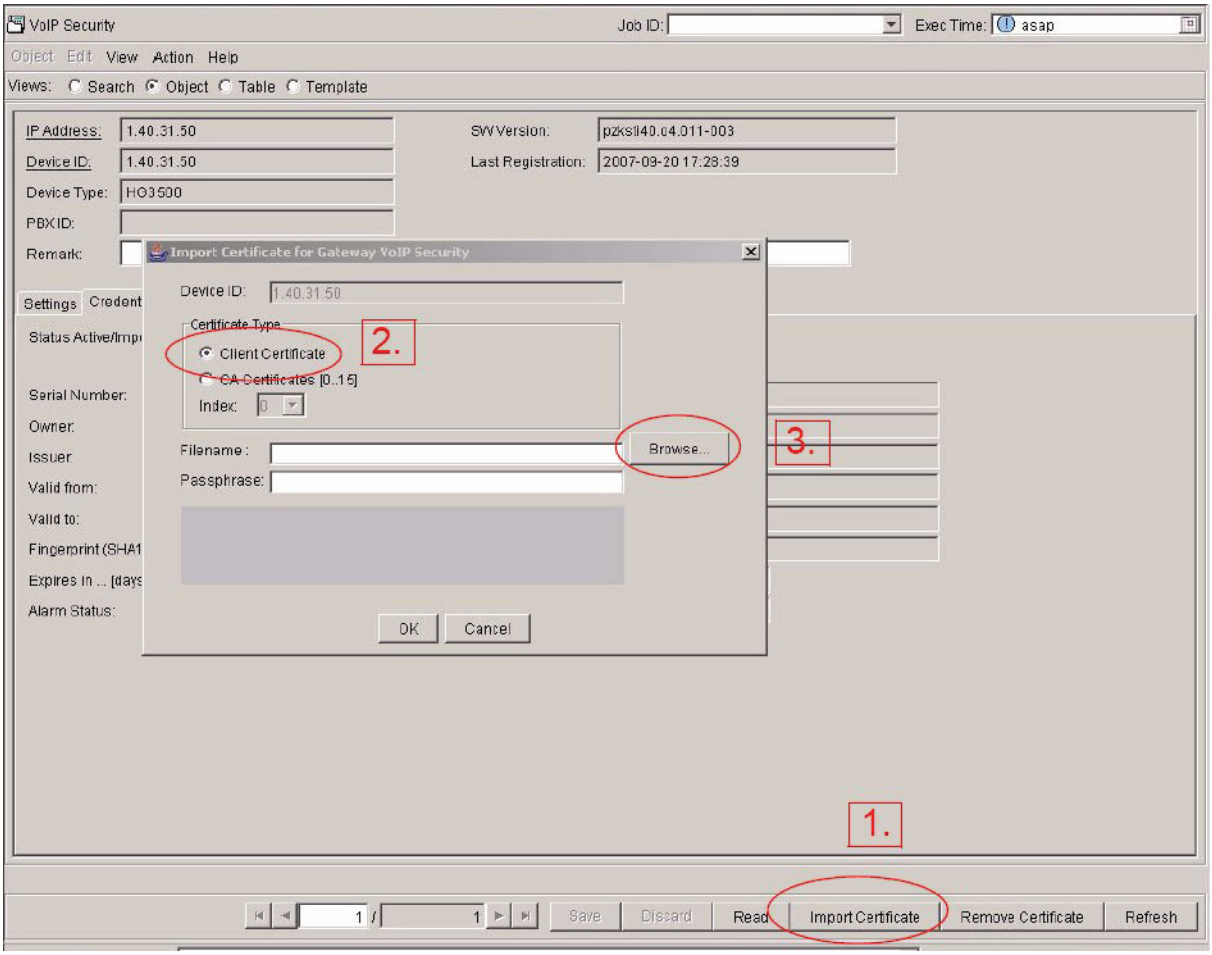


5.4 Distribution of the SPE Certificate

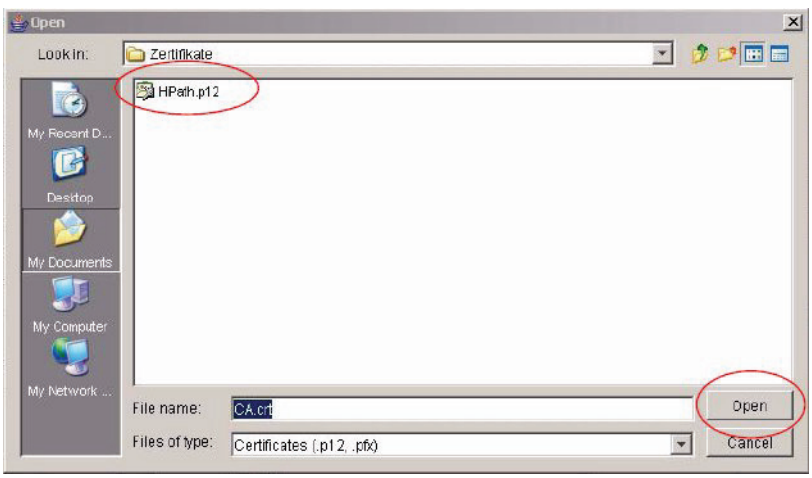
Import SPE certificate: **IP Devices > IP Gateway Configurtaion > VoIP Security >** tab **Credentials**



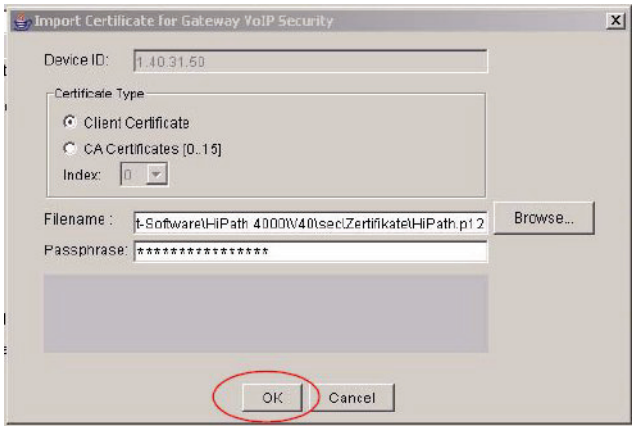
Browse for the certificate. **Passphrase** is the passwordm which was used creating the certificate.



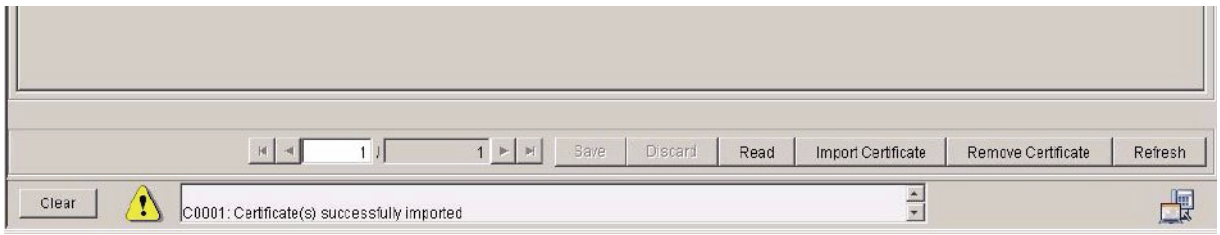
Select the certificate.



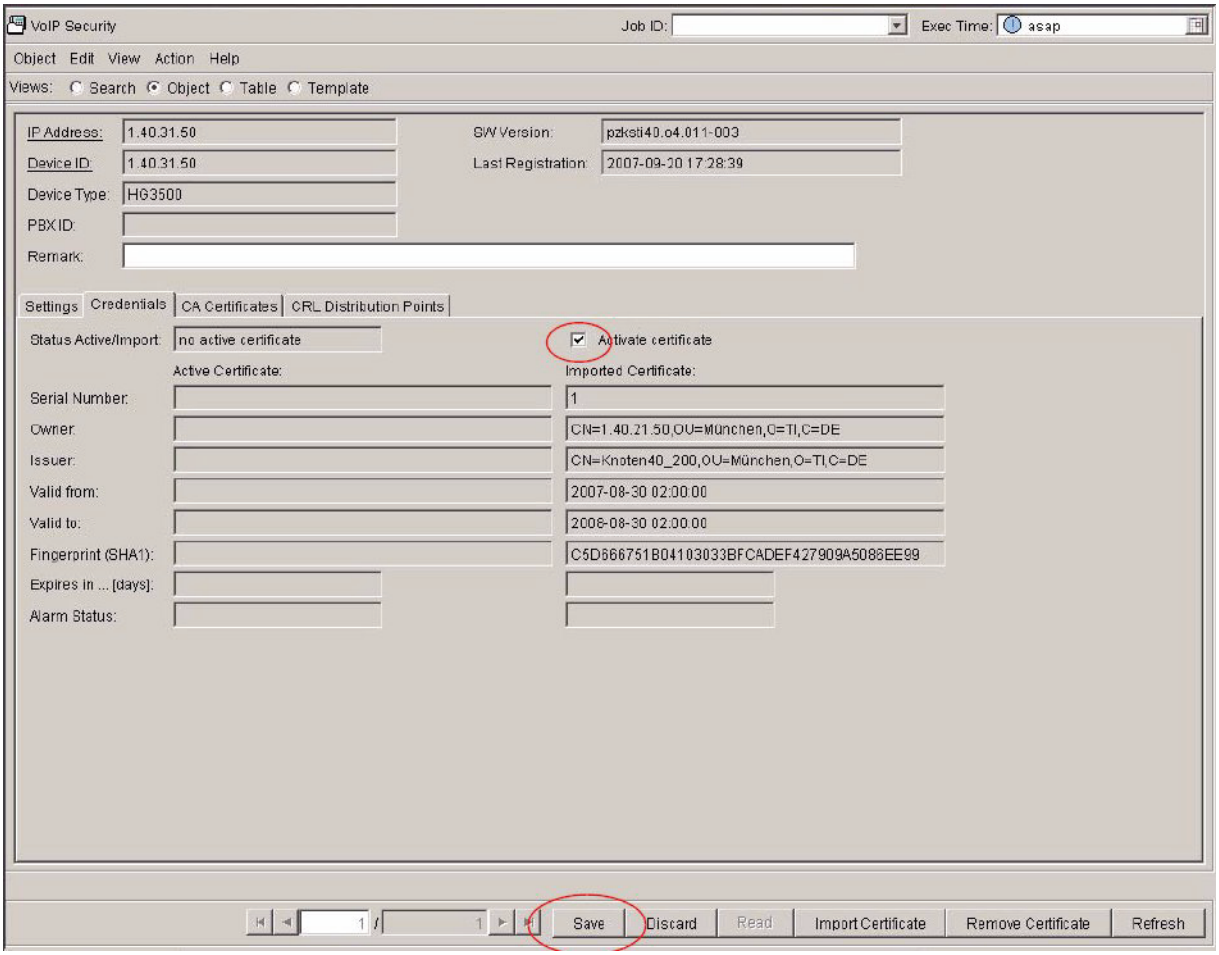
Confirm with **OK**.



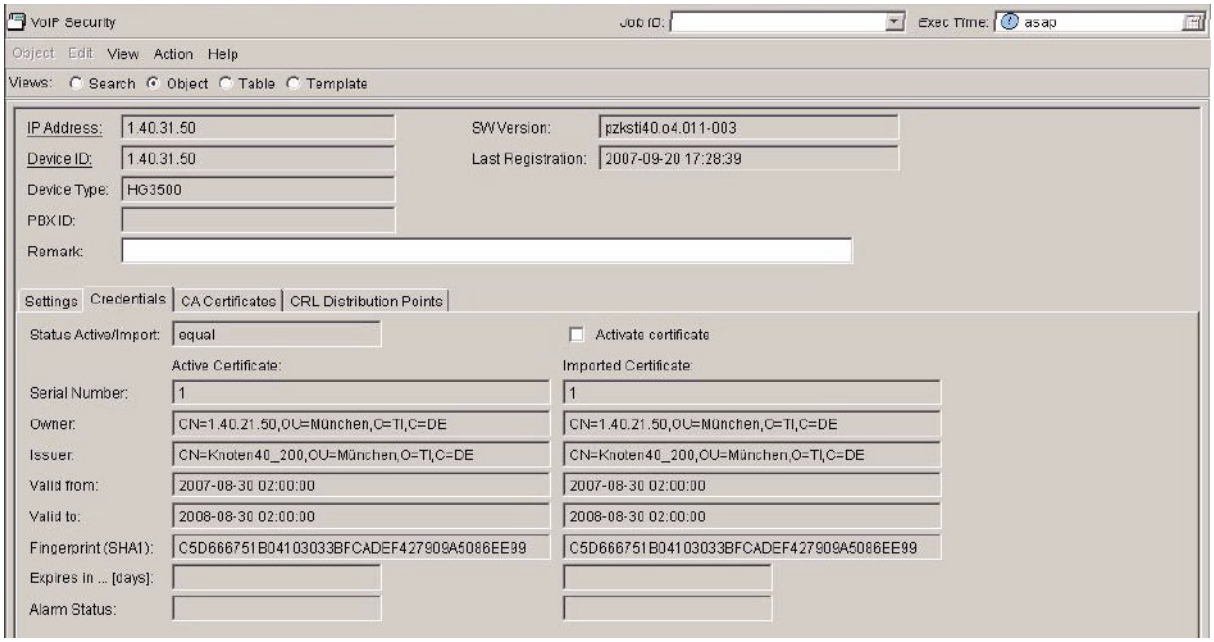
The certificate has been successfully imported.



Activate the certificate.



Certificate is active. Status (**Status active/Import**) is **equal**.



You can use the WBM application in HG 3500/3575 V4 to check if the import operations worked properly and the certificates were activated. Access is possible with the HiPath 4000 Assistant.

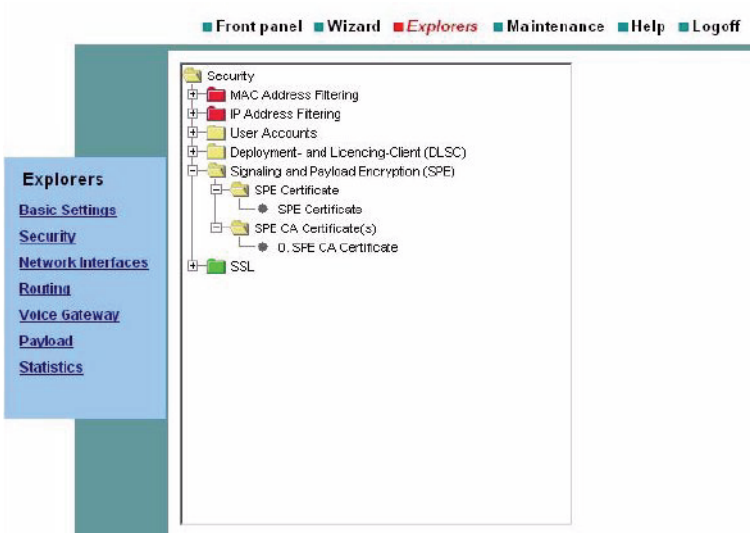
Menu: **Expert Access > HiPath4000 > HG35xx Web Based Management**

In the WBM you can have a look to the certificates in the following directory:

Explorers > Security > Signaling and Payload Encryption (SPE)

There should be two entries:

- SPE Certificate
- SPE CA Certificate(s)


Front panel
Wizard
Explorers
Maintenance
Help
Logoff
Explorers
Basic Settings
Security
Network Interfaces
Routing
Voice Gateway
Payload
Statistics
Security
MAC Address Filtering
IP Address Filtering
User Accounts
Deployment- and Licencing-Client (DLSC)
Signaling and Payload Encryption (SPE)
SPE Certificate
SPE Certificate
SPE CA Certificate(s)
0. SPE CA Certificate
SSL

6 Distribution of Certificates to a Common Gateway Board with the WBM of the Board

This chapter is only intended as a brief overview of the necessary steps in WBM. For a detailed description, refer to the WBM Administrator Manual: (http://apps.g-dms.com:8081/techdoc/de/P31003H3140M1010100A9/index.htm).

Certificates can be imported directly via WBM (Web-Based Management) of the common gateway board if DLS is not available in the customer network.

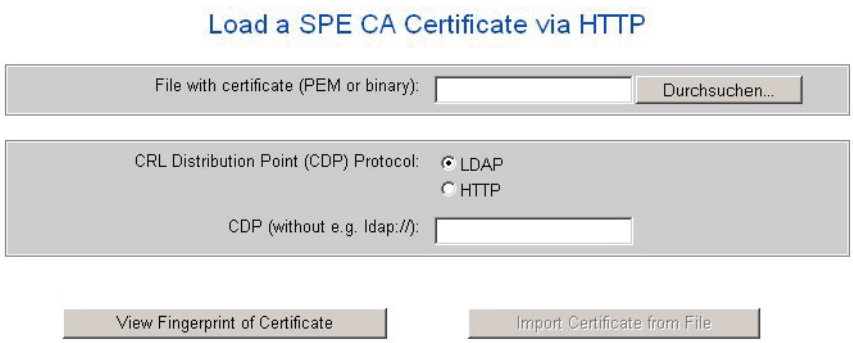
You can access the common gateway's WBM via HiPath 4000 Assistant: **Expert Mode > HG35xx Web Based Management**.

6.1 Importing CA certificates

Explorers > Security > Signaling and Payload Encryption (SPE) > SPE CA Certificate(s) > (right-click) **Import trusted CA Certificate (PEM or Binary)**

The **Load a SPE CA Certificate via HTPP** mask is displayed. Browse for the certificate. **Press View Fingerprint of Certificate**. Now import the certificate with the **Import Certificate from File** button.

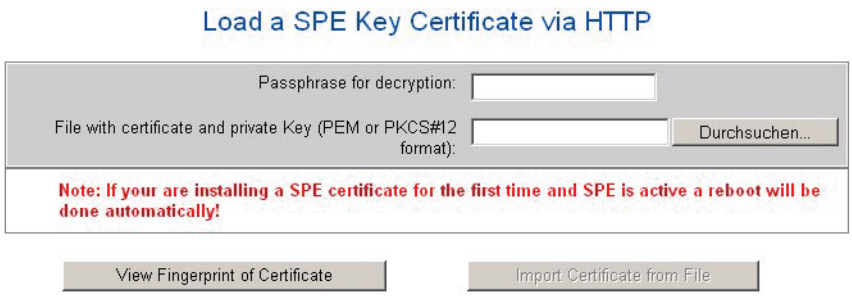
An appropriate message is output if the import operation was successful.



6.2 Importing an SPE certificate

Explorers > Security > Signaling and Payload Encryption (SPE) > SPE Certificate > (right-click) **Import SPE certificate plus private key (PEM or PKCS#12)**

The **Load a SPE Key Certificate via HTPP** mask is displayed. Enter the passphrase („private key") and then browse for the certificate. **Press View Fingerprint of Certificate**. Now import the certificate with the **Import Certificate from File** button.


Load a SPE Key Certificate via HTTP
Passphrase for decryption:
File with certificate and private Key (PEM or PKCS#12 format):
Durchsuchen...
Note: If your are installing a SPE certificate for the first time and SPE is active a reboot will be done automatically!
View Fingerprint of Certificate
Import Certificate from File

7 Distribution of a CA Certificat to Terminals with DLS

This chapter is only intended as a brief overview of the necessary steps in DLS. For a detailed description, refer to the DLS V2 Administrator Manual: (http://apps.g-dms.com:8081/techdoc/de/P31003S2320M1000100A9/index.htm).

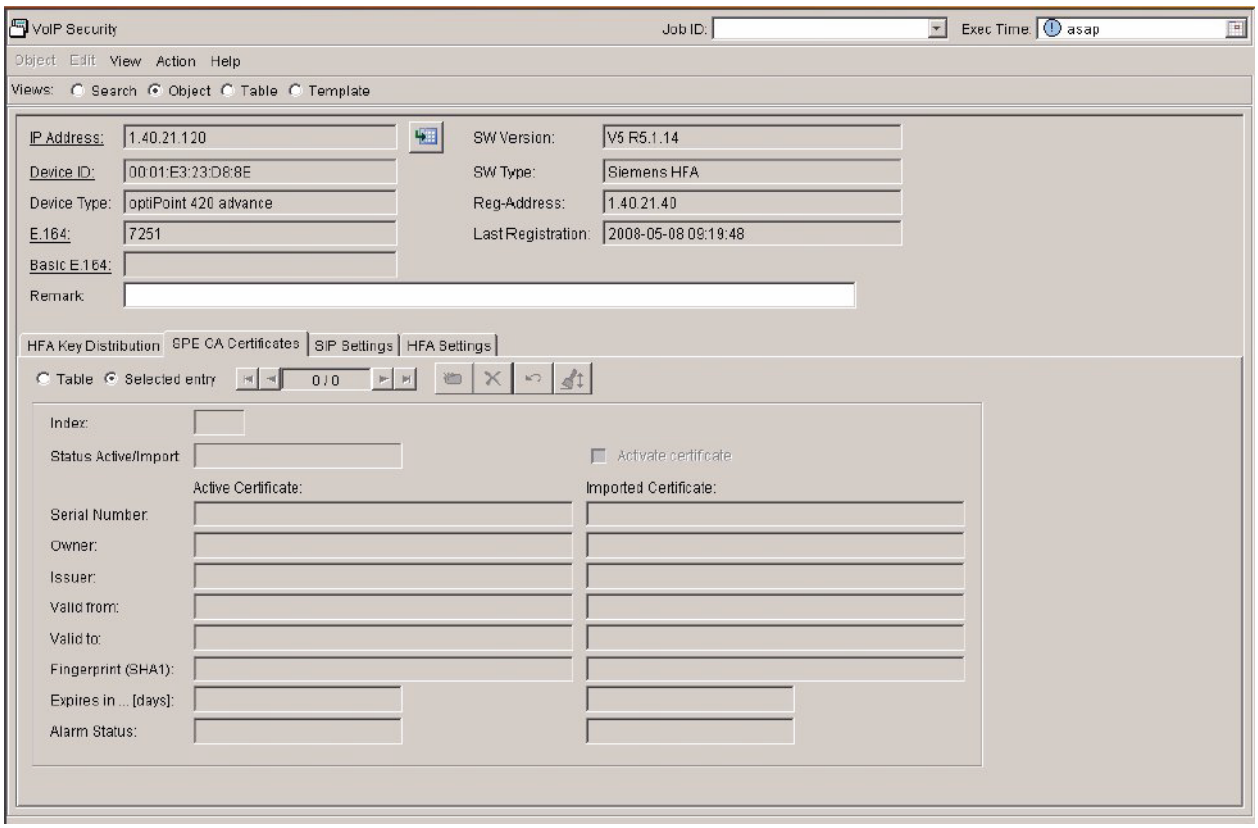
In the terminal the transport protocol can be set to TCP or TLS (via menu, WBM of the terminal or DLS). If **encryption** is used the protocol **TLS** must be used for the terminal.

An IP terminal only gets a CA certificate. The SPE certificate will be sent, if the terminal is working with the TLS protocol, directly from the common gateway to the IP terminal .

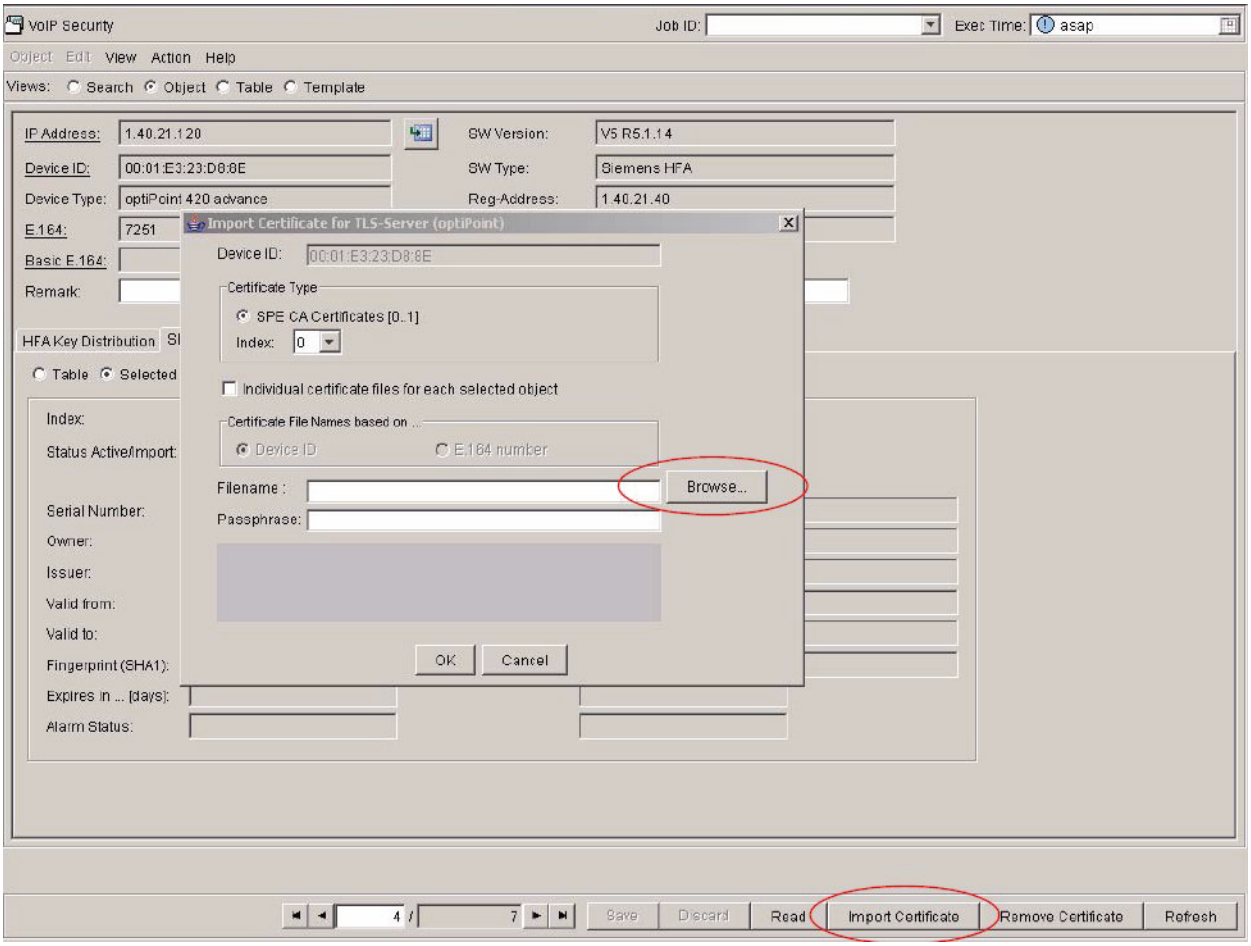
The CA certificate can be distributed to the phone only via the DLS. A manual distribution as for the common gateway board is not possible.

Distribution of the certificate to the terminal via DLS.

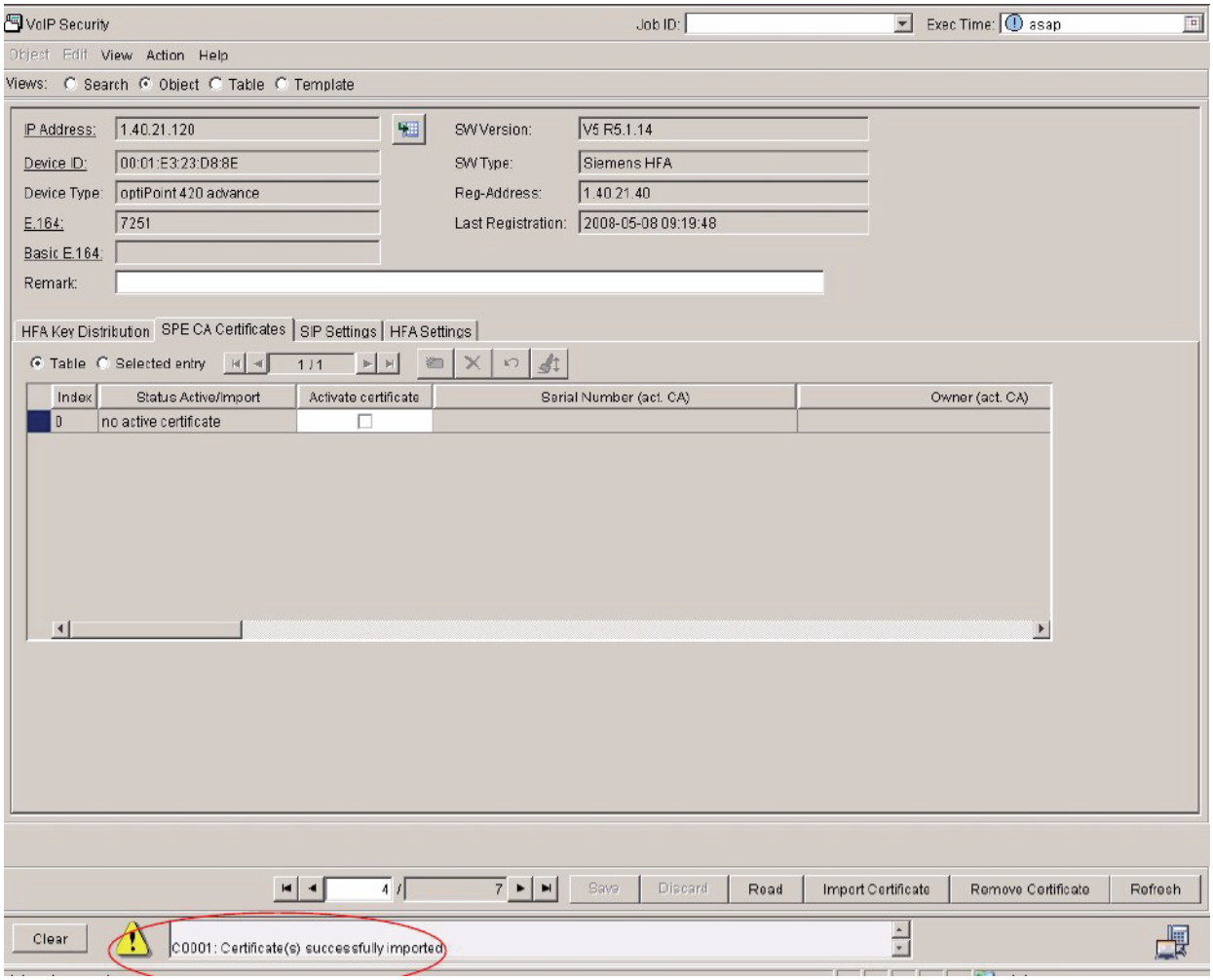
IP Devices > IP Phone Configuration > VoIP Security > tab **SPE CA Certificate**



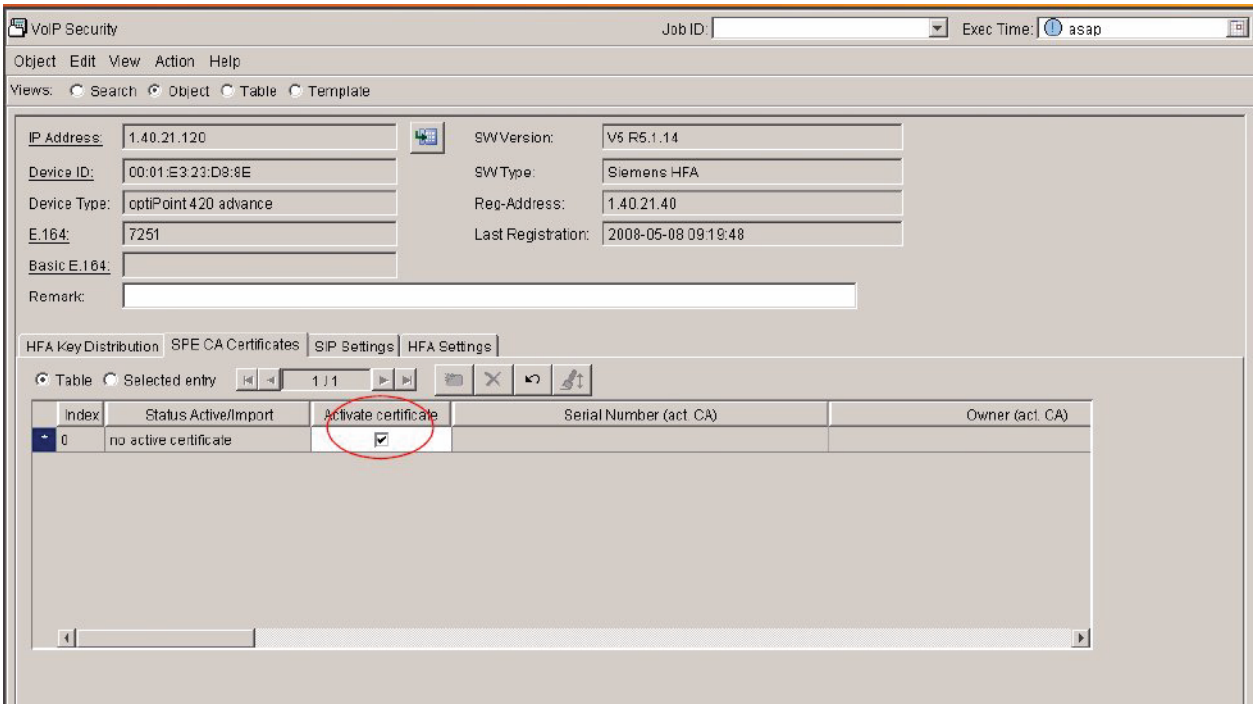
Select the CA certificate by using the button **Import Certificate** and **Browse**.



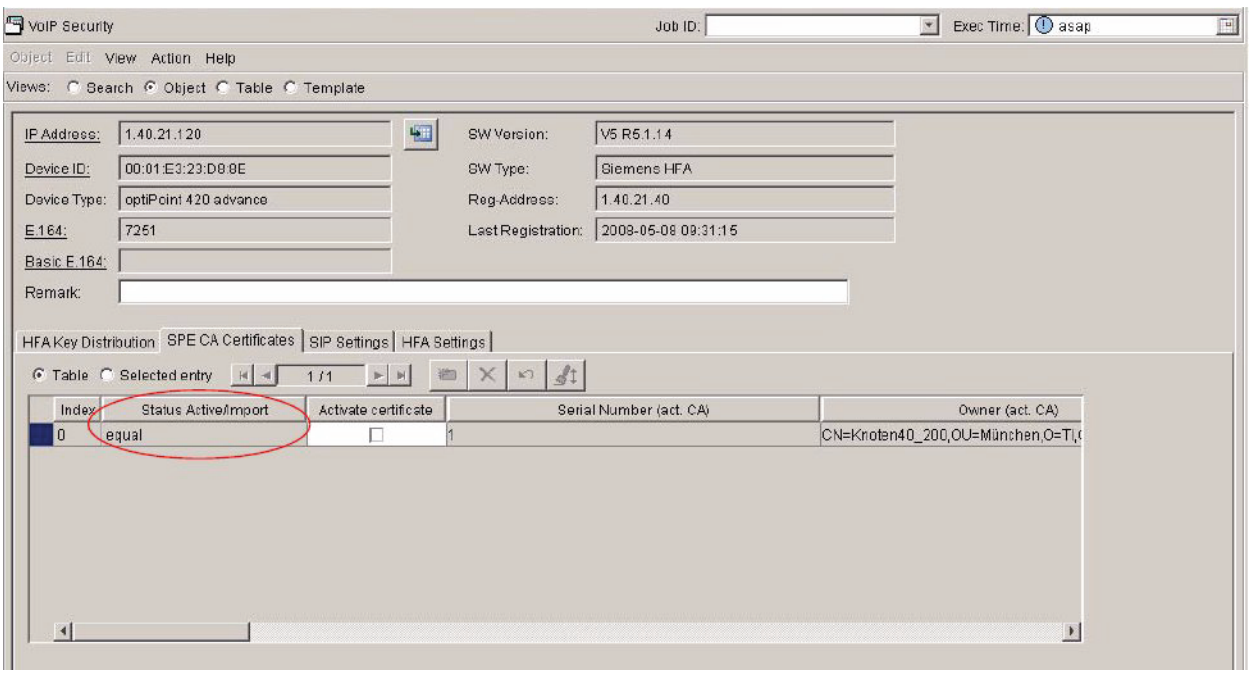
If the import of the certificate was successful a message is displayed.



Activation of the certificate.



If the activation was successful the status (**Status Active/Import**) will change from **no active certificate** to **equal**.

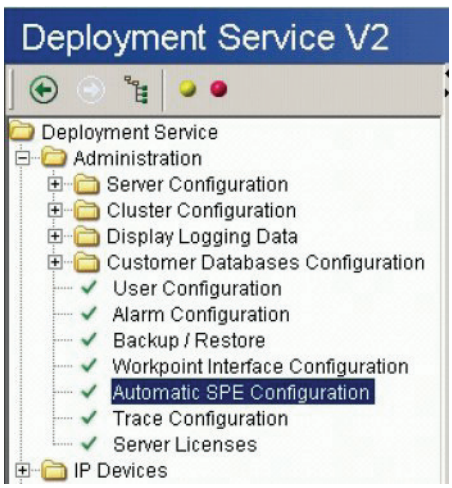


8 Automatic SPE Configuration

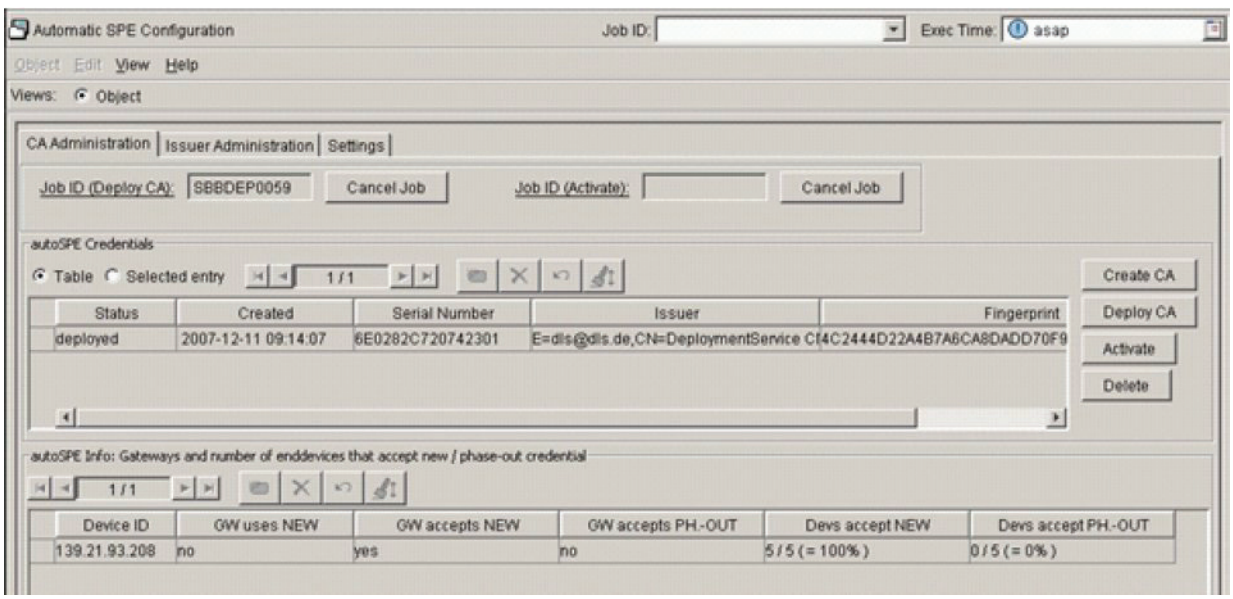
This chapter is only intended as a brief overview of the necessary steps in DLS. For a detailed description, refer to the DLS V2 Administrator Manual: (http://apps.g-dms.com:8081/techdoc/de/P31003S2320M1000100A9/index.htm).

With DLS V2 R2 you can create, distribute and activate certificates with the function **Automatic SPE Configuration**.

Deployment Service > Customer Database Configuration > Automatic SPE Configuration

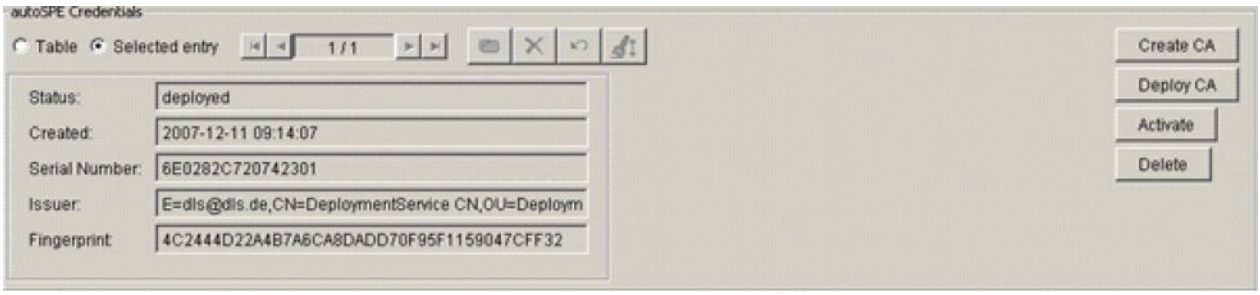


In the **Automatic SPE Configuration** window you have the possibility to create, distribute and activate CA and SPE certificates.



CA Administration tab:

The **CA Administration** tab gives an overview about the currently used credentials for SPE and whether they are known to the DLS administrated SPE capable gateways as well as the devices connected to these gateways.



Create CA button: Generation of a CA certificate.

Distribute CA button: Distribution and activation of a CA certificate.

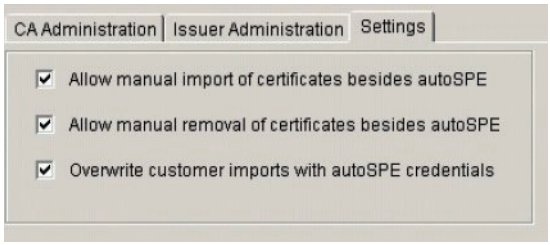
Activate button: Generation and distribution of a CA signed SPE certificate.

Delete button: Delete a certificate.

Issuer Configuration tab:

The **Issuer Configuration** tab offers the possibility to modify the issuer information of the credential to be created or use DLS internal default values instead.

Setings tab:


CA Administration
Issuer Administration
Settings
Allow manual import of certificates besides autoSPE
Allow manual removal of certificates besides autoSPE
Overwrite customer imports with autoSPE credentials

Index