T-TeleSec LineCryptConfig

User's Guide

Deutsche
Telekom

Contents

Notes....5

The LineCrypt security concept....7
- Authentication....7
- Access control....7
- Encryption....8
- IKE....8
- System requirements....9
- Installation and program start....9
- User Interface....9
- Start up....11

Configuration....13
- Mode for LineCrypt SOHO....14
- Mode for LineCrypt I, IT and I+....15
- PPP-callback....17
- Call numbers....18

Network configuration....20
- Ethernet....20
- TCP/IP-Konfiguration....21
- Local network configuration....21
- Remote network configuration....24
- PPP configuration....26
- Configuration Security Policies....30

Rights configuration....34
- CA-List....35
- Rights check procedure....36

Password....39

Log data....40

Softwareupdate....41

Access data....42

Configuration examples....45
- Configuration of a virtual private network....45
- Configuration with directory service (1 head office, 2 branch offices)....51
- LineCrypt I+ in point to multipoint mode : Example....70

Factory setting........72
LineCrypt GSM........72
LineCrypt I, IT........72
LineCrypt I+........73
LineCrypt L........74
LineCrypt L100........75
LineCrypt DSL........76
LineCrypt SOHO........77

Notes

You can perform all the settings on your LineCrypt simply and conveniently with the LineCryptConfig software.

We strongly recommend that you read this user manual before using the LineCryptConfig. Deutsche Telekom cannot be held liable for any possible damage caused to the device or other facilities arising from the failure to follow the instructions in this manual. This manual is valid for LineCryptConfig Version 2.4.x.

Overview of pictorial symbols

⚠ Safety notes for averting risks to people and objects are marked with a warning triangle.

✋ Important notes for data security are marked with the hand pictogram.

💡 Important notes for LineCrypt operation are marked with the light bulb pictogram.

I, IT, SOHO If the information contained within a section is only applicable to particular LineCrypt types, the relevant types are specified.

LineCrypt types

LineCryptConfig may be used to perform the settings for the LineCrypt types I, IT, I+, L, L100, DSL, SOHO, and GSM. This manual describes the options and settings for all these LineCrypt types.

💡 Not all options and settings are available in all versions of the various LineCrypt devices. When configuring your device, you may therefore find that what you see on your screen differs from the diagrams shown.

Data security

The LineCrypt family's security objective is to guarantee authentic and confidential communication between two LineCrypt. This security objective can only be achieved if the LineCrypt is configured to allow encrypted connections only.

For a LineCrypt to function correctly and securely, compliance with the following organizational measures is required:

ORG1: The LineCrypt integration in the communication system must be such that only authorized users are able to use LineCrypt security functions from the red zone.

ORG2: Measures must be taken to prevent the possibility of a LineCrypt being used or manipulated by unauthorized persons, or falling into unauthorized hands with the Netkey Card.

ORG3: No rights may be granted for certificates for which the appropriate secret key is compromised.

Explanation of terms:

red zone: the area of the terminals and the LineCrypt, in which voice, user, and management data that merits protection exists in unencrypted form.

black zone: the area in which voice, user, and management data that merits protection is transferred encrypted.

The NetKey Cards contain an operating error counter. This counter registers every insertion of the card being plugged into a LineCrypt that is not intended for this. After a certain number of operating errors, the NetKey Card switches off and must be replaced by a new one.

The LineCrypt security concept

Authentication

During connection setup, both LineCrypt identify and authenticate themselves using the certificates stored on the chip card.

A certificate is, in simplified terms, an electronic proof of identity. LineCrypt uses X.509 certificates. This kind of certificate always contains a unique certificate number and a public key, which can be used to check signatures. It may also contain information on the identity of a person such as name, organization, or address.

Every certificate is protected against tampering that go unnoticed through an electronic signature of the issuer (publisher). The publisher of a certificate is also called the Certificate Authority (CA). LineCrypt accepts only certificates published by Deutsche Telekom. The keys (CA keys) used by the publisher to sign the certificates are stored in a special list – the so-called CA list. This list is part of the LineCrypt configuration, and is itself signed like a certificate. Since the publisher changes the CA key for certificate authentication at regular intervals, it may be that your LineCrypt CA list does not contain a valid CA key. In this case, the LineCrypt cannot check a certificate signed with such a key, and therefore rejects the use of this certificate. In order to use this certificate, you require a current CA list, which you can transfer to the LineCrypt with the configuration software.

In the course of authentication, the communication partners exchange certificates and check that they are correct. The RSA encryption method (1024 bit) is used for authentication. In the course of authentication, the exchange of a 128-bit-wide session key also takes place (likewise secured through the RSA encryption). This key is chosen randomly and is generated by the chip card.

Access control

Access control is implemented using the rights file. Within authentication, the authentication partner’s certificate is compared with the entries defined in the rights file, and a decision is made on whether to set up or shut down the connection based on the strategy described on page 38.

Encryption

The 128-bit session key calculated during authentication is used to encrypt the transport data. Encryption is based on the IDEA algorithm.

IKE

An IKE-compliant key exchange is supported by LineCrypt L and SOHO. In this case, the symmetrical encryption algorithms DES and Triple-DES are also available for user data encryption. The IKE-compliant key exchange uses a preshared secret for authentication. This preshared secret is linked to a given IP address. Therefore IKE cannot be used with dynamic IP addresses. The certificates stored on the chip card are not used for IKE.

Installing the configuration software

System requirements

- PC with one of the following Windows operating systems: Windows 95, 98, ME, NT, 2000 or XP
- Free serial interface RS 232 (V.24) with a Sub-D connector
- CD-ROM drive
- LineCrypt I, IT, I+, L, L!00, DSL, SOHO or GSM

Installation and program start

Run the "setup_de.exe" file (for the German-language installation) or the "setup_en.exe" file (for the English-language installation) from the CD-ROM provided, and follow the instructions on your screen.

User Interface

Use the LineCryptConfig (LCC) configuration software just as you would use any other Windows software. That way, you can keep to your usual method of working and move in your familiar desktop environment.

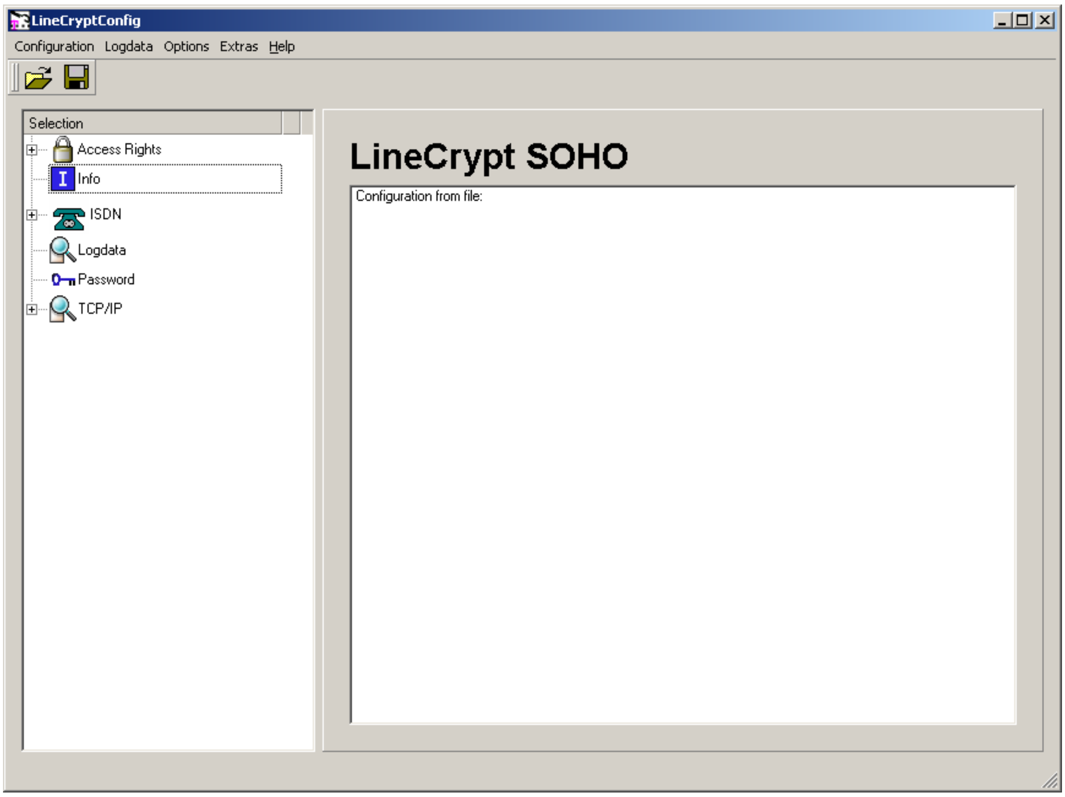
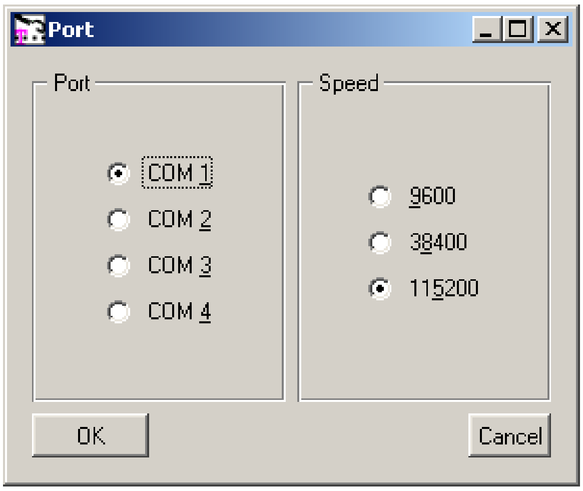


Figure 1: user interface

The user interface is divided into two parts. In the left part, you can select the various settings by clicking and expanding the icons. The dialogs assigned appear in the right part.

Start up

Start the LCC program using the Windows Start menu. Check that your LineCrypt is ready for operation. With the serial interface cable supplied, connect your LineCrypt to a free serial interface of your PC. On the ***Options*** menu, click ***Serial interface***, and then select the interface you have chosen. For fast operation, the speed of the interface should be set to 115200 Baud.



Port

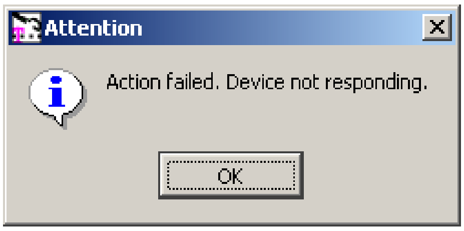
Port
● COM 1
○ COM 2
○ COM 3
○ COM 4

Speed
○ 9600
○ 38400
● 115200

Figure 2: Dialog interface

Now test the connection to the LineCrypt. To do this, select the Read info menu command on the Extras menu. The information displayed should now correspond to figure 2, the exact output depending on the type of LineCrypt, the software version, and the chip card.

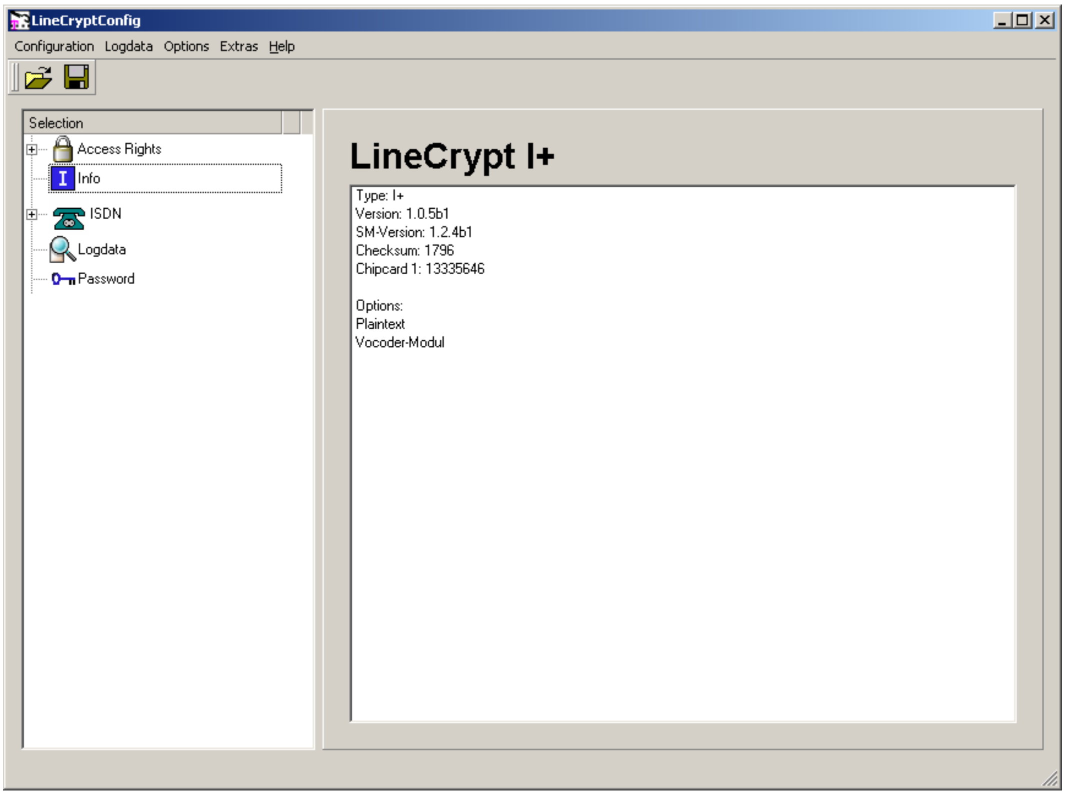
If the message “Device not responding” is displayed, check the connection to the LineCrypt as well as the settings you have performed.



Attention

Action failed. Device not responding.

Figure 3: Device not responding



Type: I+
Version: 1.0.5b1
SM-Version: 1.2.4b1
Checksum: 1796
Chipcard 1: 13335646

Options:
Plaintext
Vocoder-Modul

Figure 4: Info

In order that the changes to the options you have made may be reapplied when you next start the LCC, save the settings by selecting ***Save settings*** on the *Options* menu.

Configuration

The LineCrypt configuration software (LCC) distinguishes three operating modes:

1. Edit access data: Access data is used by the LineCrypt DSL, L, and SOHO. The access data contains the PPP connection data (password, user name, and telephone number) and can be stored separately from the remaining configuration on the LineCrypt chip card.

2. Edit configuration: In this operating mode, the LineCrypt configuration can be changed. The configuration is stored in the LineCrypt FLASH memory. Whether the access data stored on the chip card or the access data that is part of the configuration is used for the PPP connection setup is also defined within the configuration.

3. Expert mode: This operating mode enables you to perform advanced settings for the LCC. You should only use this mode if you have in-depth knowledge of the configuration.

To configure the LineCrypt, you carry out three steps. On the *Options* menu, select whether you want to change the access data or the configuration. You can now read out the existing configuration from the LineCrypt. To do this, select the *Read from device* menu command on the *Configuration* menu. If the configuration is password-protected, you will be prompted to make an entry.

Different passwords are used for the access data and the configuration.

Now alter the configuration as required. To write the changed configuration to the LineCrypt, select the *Write to device* menu command on the *Configuration* menu. The new configuration takes effect immediately. Active ISDN connections are not canceled. TCP/IP connections are interrupted and immediately restarted according to the new rules.

I, IT, I+, SOHO

Configuring the ISDN interface

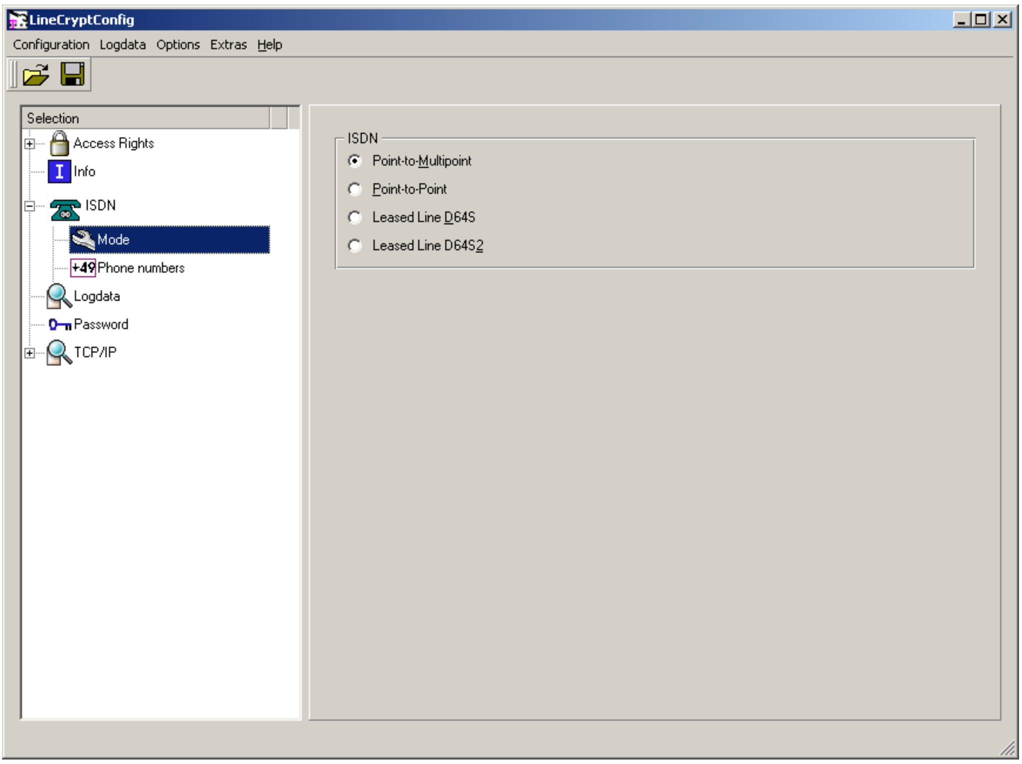
You can define the parameters of the ISDN interface under the ISDN icon. You perform the settings using three dialogs. The first dialog *Mode* contains general settings. In the second dialog, you perform the settings for the PPP callback for the LineCrypt SOHO. And in the last dialog, you define the call numbers.

SOHO

Mode for LineCrypt SOHO

Connection type

First define whether your LineCrypt is to be operated before a private branch exchange (PABX line, *Point-to-Point*), at the multi-terminal connection*(Point-to-Multipoint)*, or at the ISDN fixed connection. LineCrypt SOHO supports the digital *Leased Line D64S* (64 Kb/s) and the *Leased Line D64S2* (128 Kb/s).



ISDN

● Point-to-Multipoint

○ Point-to-Point

○ Leased Line D64S

○ Leased Line D64S2

Figure 5: Mode (SOHO)

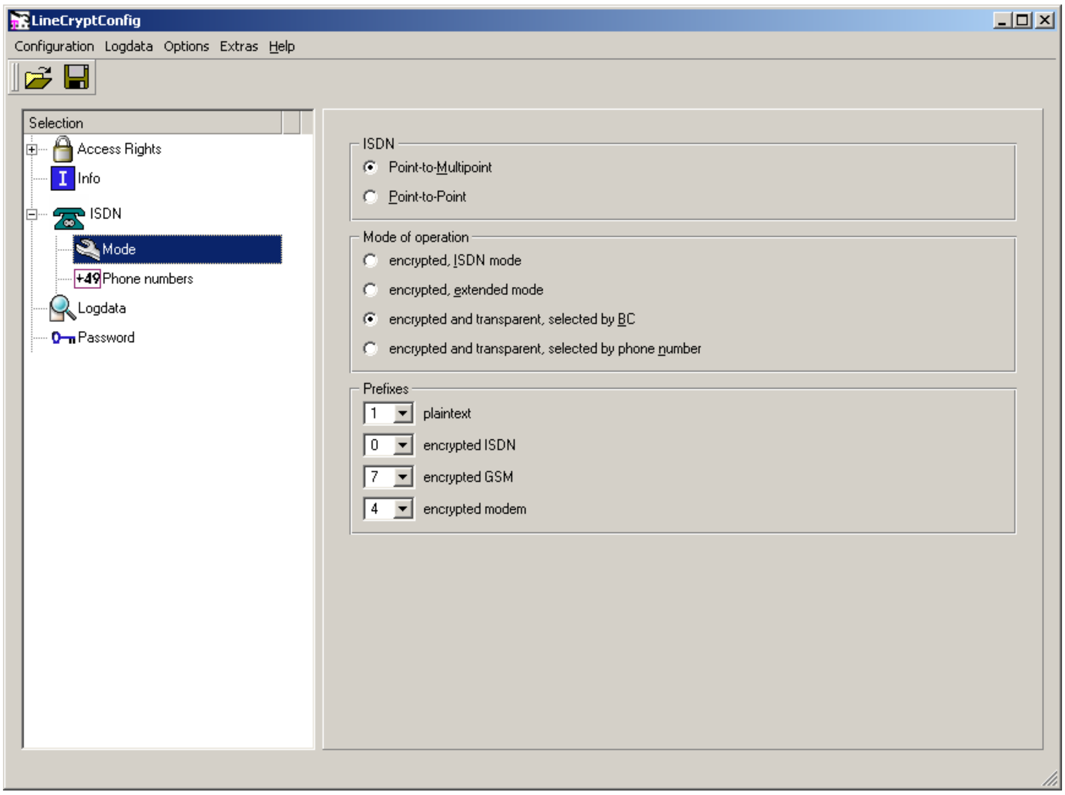
I, IT, I+

Mode for LineCrypt I, IT and I+

Connection type

First define whether your LineCrypt is to be operated before a private branch exchange (PABX line*, Point-to-Point*) or at the multi-terminal connection *(Point-to-Multipoint)*.

LineCrypt I and IT can only set up encrypted connections amongst themselves. Therefore, you do not need to perform any further settings for these types.



ISDN
● Point-to-Multipoint
○ Point-to-Point

Mode of operation
○ encrypted, ISDN mode
○ encrypted, extended mode
● encrypted and transparent, selected by BC
○ encrypted and transparent, selected by phone number

Prefixes

1	plaintext
0	encrypted ISDN
7	encrypted GSM
4	encrypted modem

Figure 6: Mode (I+)

I+

operating mode

For a LineCrypt I+, you should now define the operating mode.

Please note that the compressed transfer of the voice data via the transport protocols V.110 and V.32 requires an optional Vocoder module in the LineCrypt I+. If your LineCrypt is not equipped with this module, you cannot use the specified transport protocols. In this case, operating mode 2 is not available.

LineCrypt I+ supports four operating modes:

- Operating mode 1: *encrypted ISDN mode*: In this operating mode, the LineCrypt supports only encrypted HDLC connections to other LineCrypt via the ISDN channel. In this operating mode, the LineCrypt I+ behaves like a LineCrypt I. You therefore do not have to use any prefix numbers for outgoing connections.

- Operating mode 2: *encrypted, extended mode*: Encrypted connections with all available transmission protocols are supported. For outgoing calls, the transmission protocol is selected via a prefix number. Unencrypted connections are not supported in this operating mode.

- Operating mode 3: *encrypted and transparent, selection via BC* (bearer capability): In this operating mode, encrypted and unencrypted connections with all supported transport protocols are supported. For outgoing calls, the transport protocol is selected via a prefix number. Incoming calls with the service identification voice are handled as unencrypted calls. Calls with a different service identification (data, video, fax G4, etc.) are handled as encrypted calls.

- Operating mode 4: *encrypted and transparent, selection by phone number*: This operating mode differs from the previous operating mode only in the behavior for incoming calls. The LineCrypt decides whether an incoming call is to be handled as an encrypted or unencrypted call from the call number called. For this, it is possible to select individual end numbers or MSN for the plaintext in the call number dialog described below.

Prefixes

In operating modes 2, 3, and 4, the LineCrypt uses prefix numbers to determine the type of the outgoing call. In operating mode 1, no prefix numbers are used.

plaintext: Prefix number for unencrypted connections in operating modes 3 and 4.

encrypted ISDN: Prefix number for encrypted HDLC connections to other LineCrypt.

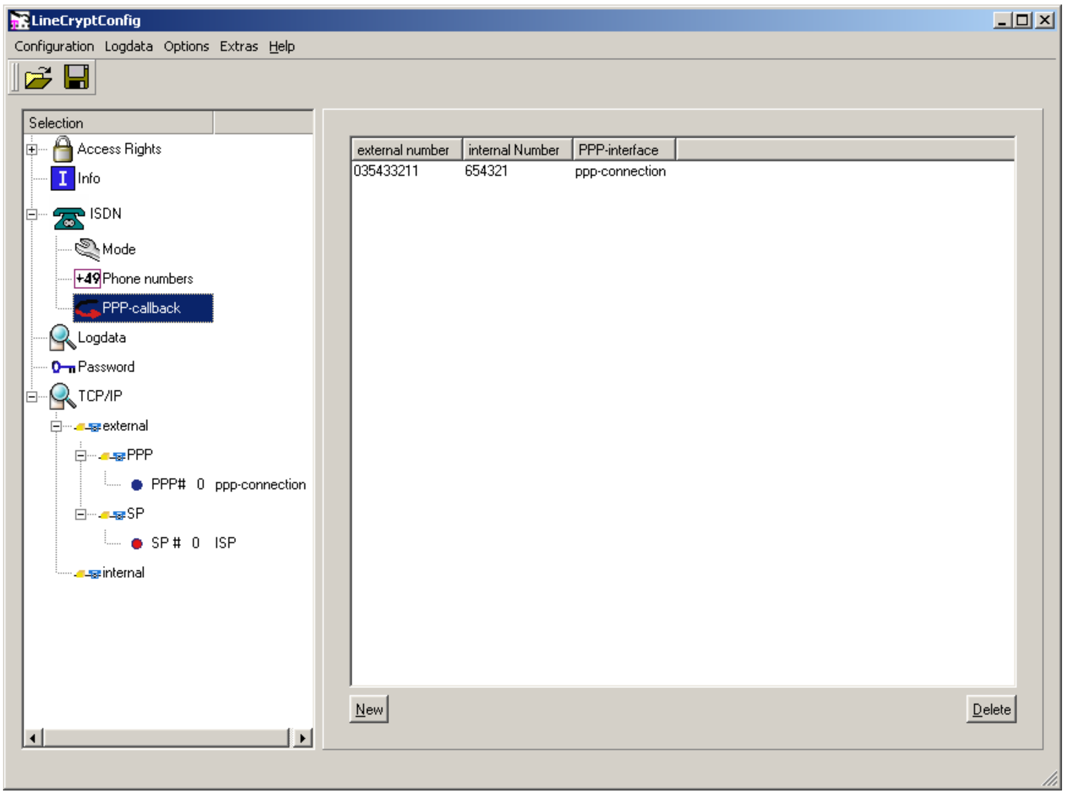
encrypted GSM: Prefix number for encrypted V.110 connections to the LineCrypt GSM. Connections to the LineCrypt GSM are only possible with the Vocoder module.

encrypted modem: Prefix number for encrypted V.32 connections. V.32 connections are only possible with the Vocoder module.

SOHO

PPP-callback

The PPP callback is only supported by the LineCrypt SOHO. An external call to the LineCrypt can trigger the setting up of a PPP connection. To create a new PPP callback entry, click the *New* button. Enter the calling number in the *external number* field. If you do not enter a number here, the setting up of the PPP connection is triggered by a call irrespective of the calling number. Now select the MSN or end number of the LineCrypt in the *internal number* field. Finally, select the *PPP interface* to be activated by the call.



external number	internal Number	PPP-interface
035433211	654321	ppp-connection

Figure 7: Callback

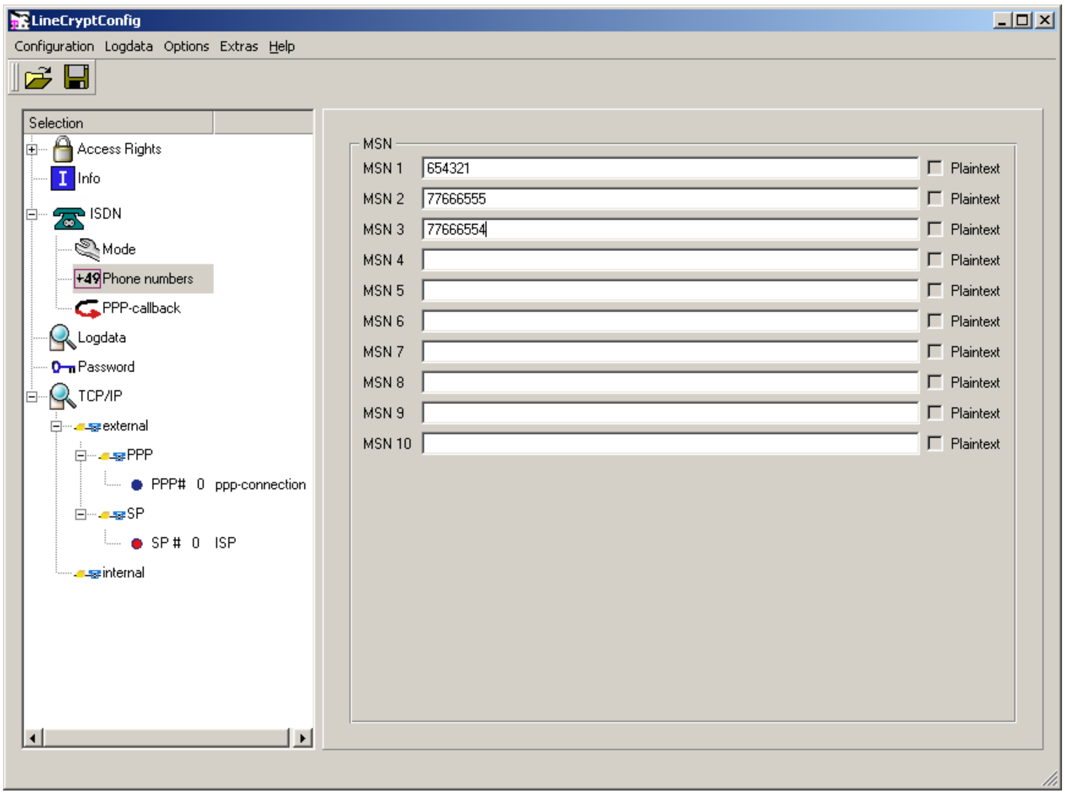
I, IT, I+, SOHO

Call numbers

MSN

If you selected Point-to-Multipoint in the dialog in figure 6, you can enter up to ten multiple subscriber numbers (*MSN*) here. If you clicked *Plaintext*, an incoming call is accepted as unencrypted when using operating mode 4 (see page 17); otherwise it is encrypted. Please note that LineCrypt I and IT do not support unencrypted calls.

.If no multiple subscriber numbers are specified, the LineCrypt accepts every incoming call. In operating mode 4, all incoming calls are handled as calls to be encrypted.



MSN

MSN 1 654321 □ Plaintext
MSN 2 77666555 □ Plaintext
MSN 3 77666554 □ Plaintext
MSN 4 □ Plaintext
MSN 5 □ Plaintext
MSN 6 □ Plaintext
MSN 7 □ Plaintext
MSN 8 □ Plaintext
MSN 9 □ Plaintext
MSN 10 □ Plaintext

Figure 8: Call numbers in Point-to-Multipoint mode

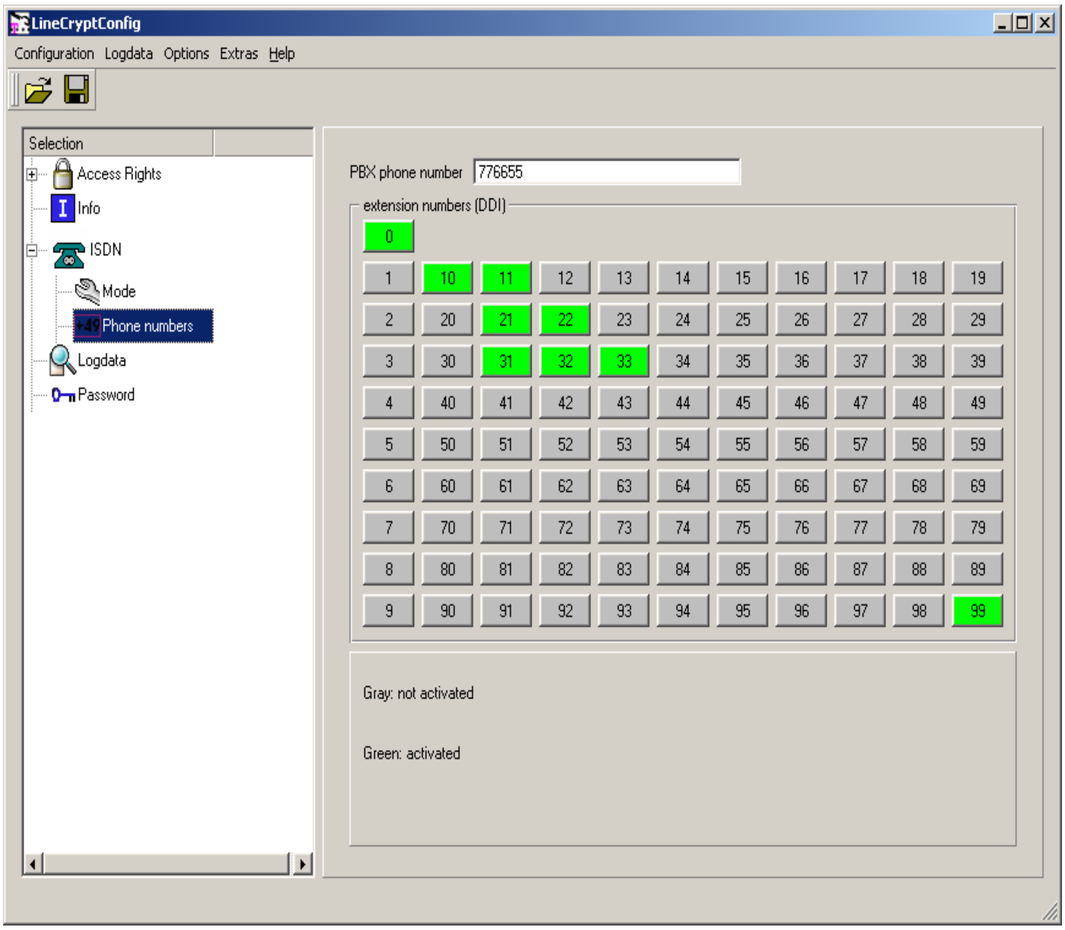
I, IT, I+

Numbering plan

If you selected Point-to-Point in the dialog in figure 6, you must first enter the *PBX phone number* (also used by your PABX) in the dialog in figure 9.

In the *extension number* plan, you can select one or two-digit numbers. Here you should refer to the numbering plan of your PABX. If you have selected a one-digit end number in a row, the two-digit end numbers are hidden in this row.

Calls to end numbers shown in gray are not accepted. Calls to end numbers shown in green are accepted, and are encrypted according to the chosen operating mode. Calls to end numbers show in red (operating mode 4 only) are put through unencrypted.



PBX phone number: 776655

extension numbers (DDI)

🟩 0										
1	🟩 10	🟩 11	12	13	14	15	16	17	18	19
2	20	🟩 21	🟩 22	23	24	25	26	27	28	29
3	30	🟩 31	🟩 32	🟩 33	34	35	36	37	38	39
4	40	41	42	43	44	45	46	47	48	49
5	50	51	52	53	54	55	56	57	58	59
6	60	61	62	63	64	65	66	67	68	69
7	70	71	72	73	74	75	76	77	78	79
8	80	81	82	83	84	85	86	87	88	89
9	90	91	92	93	94	95	96	97	98	🟩 99

Gray: not activated

Green: activated

Figure 9: Call numbers in Point-to-Point mode

If you do not select any numbers in the end number plan, the LineCrypt accepts every incoming call. In operating mode 4, all incoming calls are encrypted.

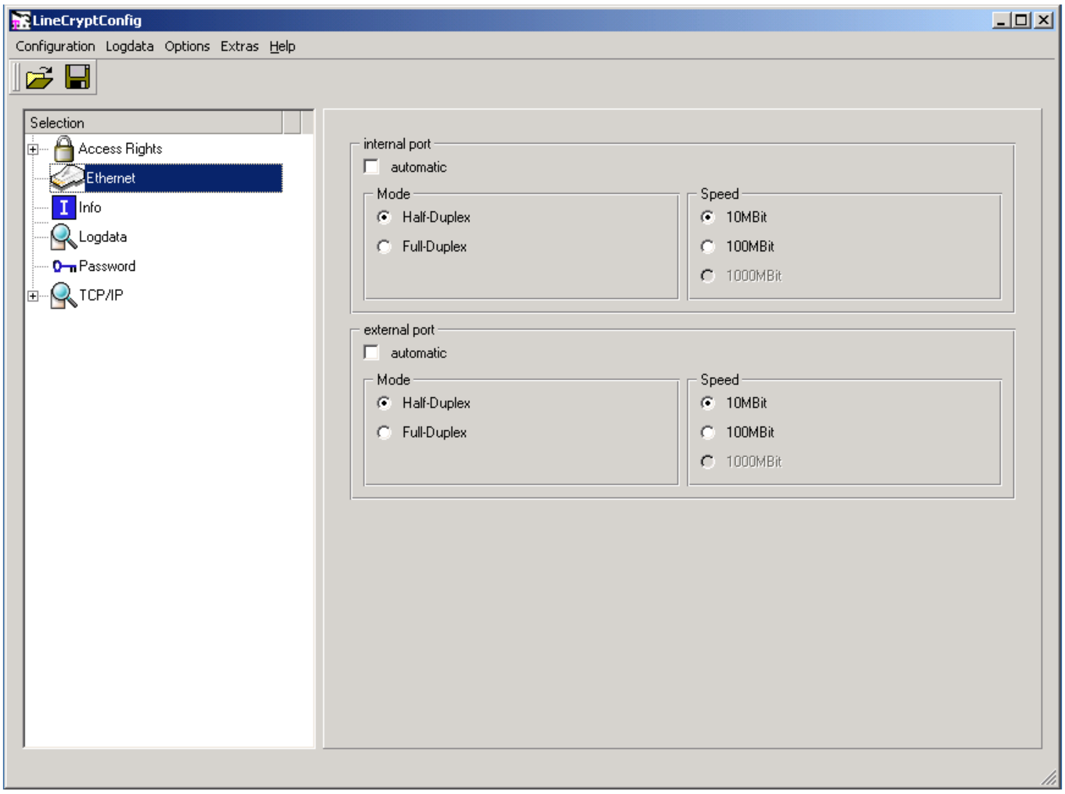
DSL, L, L100, SOHO

Network configuration

Before using your LineCrypt DSL, L, L100 or SOHO, various network settings are necessary, which you should adjust to your needs.

Ethernet

You can configure the parameters of the Ethernetports (speed, duplex) on the dialog figure 10 .



internal port

□ automatic

Mode

● Half-Duplex

○ Full-Duplex

Speed

● 10MBit

○ 100MBit

○ 1000MBit

external port

□ automatic

Mode

● Half-Duplex

○ Full-Duplex

Speed

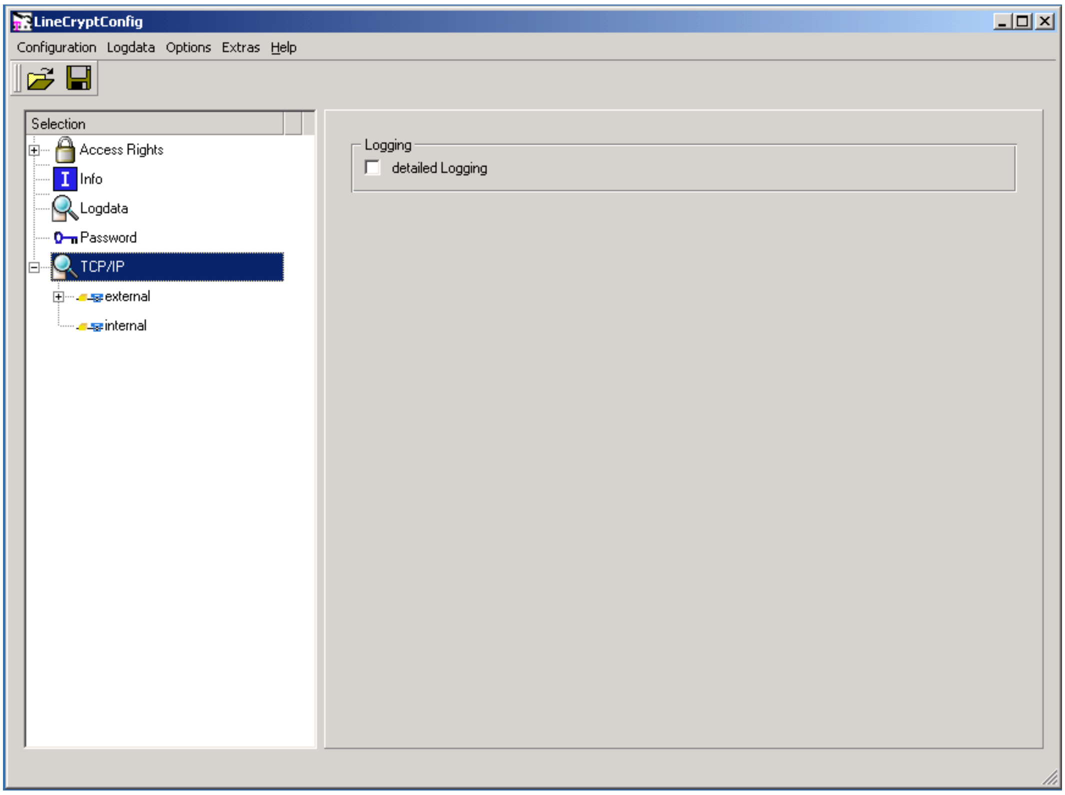
● 10MBit

○ 100MBit

○ 1000MBit

Figure 10: Ethernet

TCP/IP-Konfiguration



□ detailed Logging

Figure 11: TCP/IP-Configuration

The *detailed logging* option activates for the device the recording of events that are of relevance for startup and problem recovery.

DSL, L, SOHO

Here, you should note that for LineCrypt DSL, L and SOHO after the configuration has been written to the LineCrypt, detailed logging only remains active until the FLASH memory is half-full with the log file in the LineCrypt.

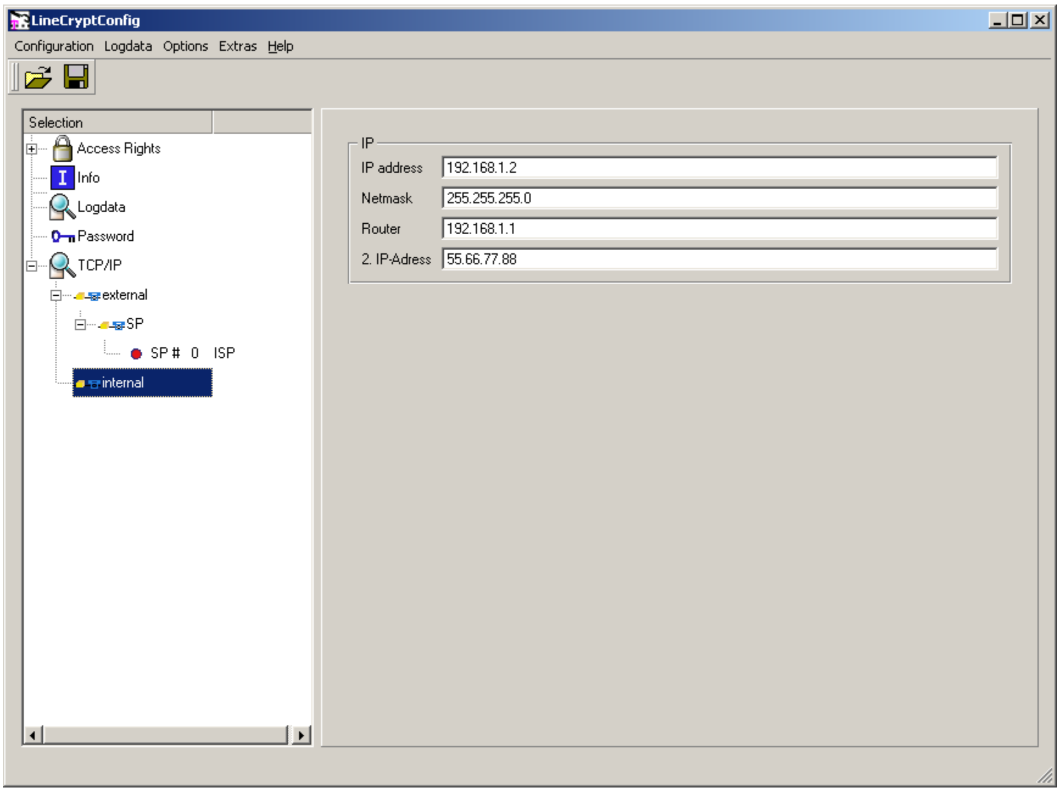
DSL, L, L100, SOHO

Local network configuration

You can configure the parameters of the internal Ethernet interface using the **TCP/IP-internal** dialog.

IP

Enter the *IP address* at which the LineCrypt is to be reached in your internal network. By specifying a *Netmask*, you define which bits of the IP address determine the network's IP address range. By specifying the *Router*, you define where IP packets that do not lie within the address range (resulting from the network mask and the IP address) are forwarded.



IP

IP address 192.168.1.2

Netmask 255.255.255.0

Router 192.168.1.1

2. IP-Adress 55.66.77.88

Figure 12: TCP/IP-Setting (Type L and L100)

The *2. IP address* entry is used to pass a second IP address to the LineCrypt for the red side. This is used by the LineCrypt for communication with the directory service. If no second IP address is set, the IP address entered in the first line is used for communication with the directory service. The use of a second IP address for the directory service can be useful and necessary if it allows the balancing of the IP address space or the elimination of IP address conflicts on the red side in conjunction with directory service communication.

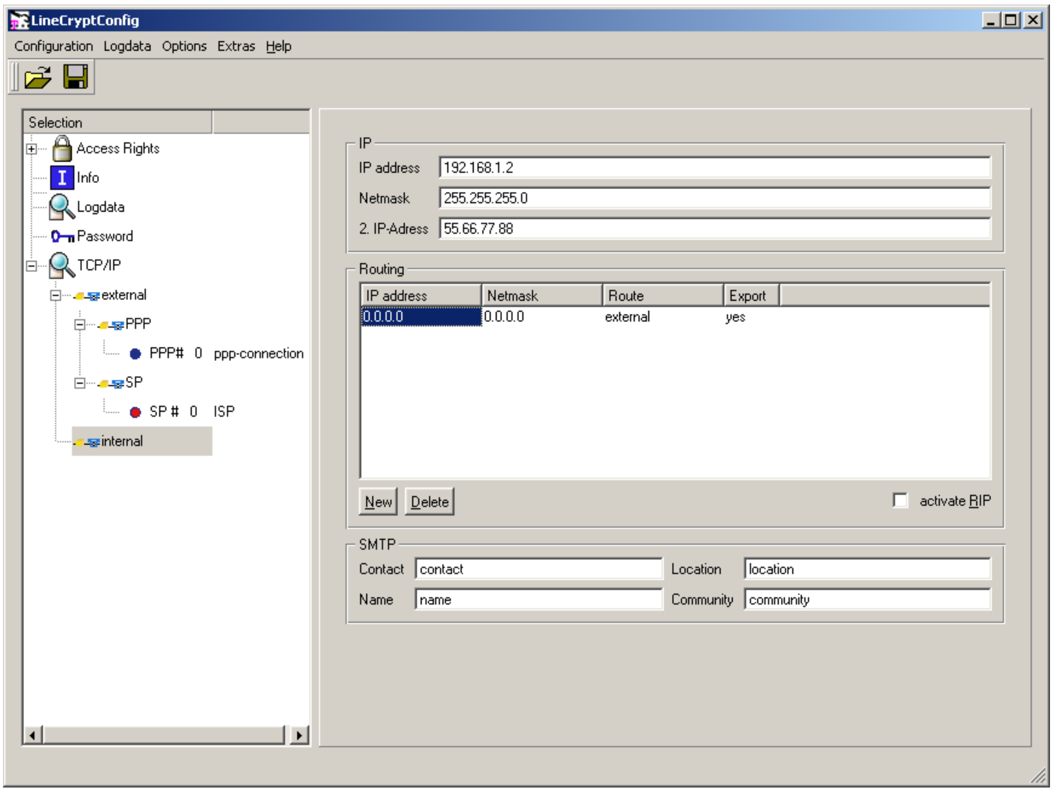
SOHO, L, L100, DSL

Routing

Here you define the routing table for the internal network side. A routing table entry defines a network area that is either:

- Routed via a router in the internal network or

- Routed to the external (black) side. To create such a routing entry, enter "*external*" or "0.0.0.0".



IP

IP address: 192.168.1.2

Netmask: 255.255.255.0

2. IP-Adress: 55.66.77.88

Routing

IP address	Netmask	Route	Export
0.0.0.0	0.0.0.0	external	yes

□ activate RIP

SMTP

Contact: contact

Location: location

Name: name

Community: community

Figure 13: TCP/IP-Setting (SoHo)

Routing entries with a smaller network area limit those with a larger network area. They are evaluated first by the LineCrypt firmware.

With the *Export* option, you define whether the LineCrypt exports the route to other routers in the network using the RIP protocol.

To enable encrypted communication, you must specify at least one route that has the entry 0.0.0.0 or *external* in the Route column.

SOHO, L, DSL With the *activate RIP* option, you activate/deactivate RIP for all routing entries for which the *Export* option is set to Yes. Only RIP 2 via Multicast is supported.

SOHO, L, DSL

SNMP

LineCrypt SOHO, DSL and L support SNMP (Simple Network Management Protocol). This enables other devices in the network to query the LineCrypt device information.

The following SNMP parameters can be set:

Name: The device name (usually the host name assigned to the LineCrypt internal IP address).

Contact: The device contact (for example, telephone number or an e-mail address of the appropriate group of people).

Location: The device location (for example, the room number where the device is installed).

Community: The SNMP community used to query the device.

If no entry is made here, the name,"contact,"location and community standard values are used.

DSL, L, L100, SOHO

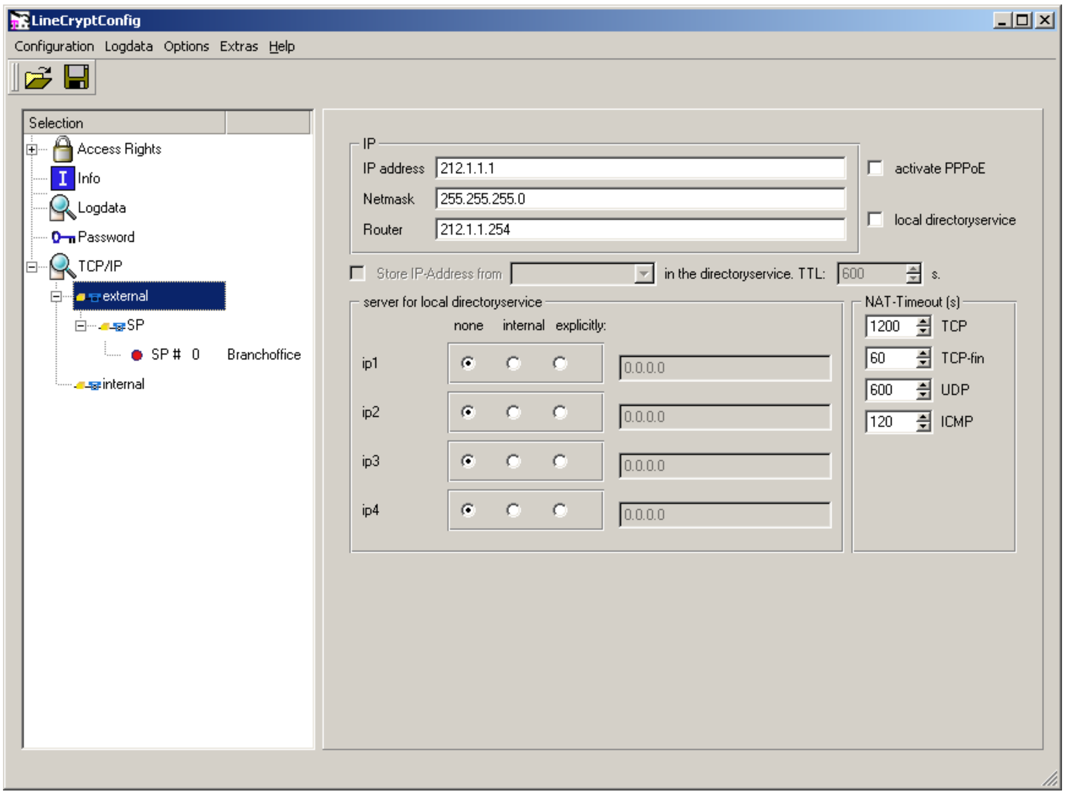
Remote network configuration

You can configure the parameters of the external interface (Ethernet or PPP) using the TCP/IP-external dialog.

L, L100, SOHO

IP

Enter the *IP address* at which the LineCrypt can be reached from outside. By specifying a *Netmask*, you define which bits of the IP address determine the network's IP address range. By specifying the *Router*, you define where IP packets that do not lie within the address range (resulting from the network mask and the IP address) are forwarded.



IP

IP address 212.1.1.1

Netmask 255.255.255.0

Router 212.1.1.254

□ activate PPPoE

□ local directoryservice

□ Store IP-Address from ▾ in the directoryservice. TTL: 600 s.

server for local directoryservice

	none	internal	explicitly:	
ip1	●	○	○	0.0.0.0
ip2	●	○	○	0.0.0.0
ip3	●	○	○	0.0.0.0
ip4	●	○	○	0.0.0.0

NAT-Timeout (s)

1200	TCP
60	TCP-fin
600	UDP
120	ICMP

Figure 14: External network

L

Activate PPPoE

The *activate PPPoE* switch activates DSL operation. If PPPoE is active, a PPP connection (see page 26) must be entered for operation.

L, SOHO

Activate local directory service

The switch *local directoryservice* activates the directory service server functionality integrated in the LineCrypt L. Please note that the local directory service is only consulted if a PPP → server for local directoryservice is set to *internal* or is explicitly set to its own internal address.

Store IP address from ppp 0 ▾ in the directory service

If you activate this function, then for every successful PPP connection setup, the LineCrypt will store the allocated IP address at all specified directory service servers. Here, you can choose the life time of the directory service entry (*TTL*). The LineCrypt will repeat the storage of the IP address after three-quarters of the specified time.

Please note that a setting that has not been coordinated with PPP → Connection → inactivity timeout can result in continuous connections.

server for local directoryservice

This is where you specify the IP addresses of the directory service servers. The options are no directory service server, the internal one, or one that you specify explicitly. If no directory service is to be consulted, set all four servers to *none*. If the activated local directory service is to be used, set one of the four directory server entries to *internal*. To use a particular directory service server, enable the *explicit* button and enter the IP address in the field provided.
It is worth noting that the LineCrypt will inquire at all directory services; however, in the search for a certificate number, the search is completed with the first successful answer.

NAT Timeout

TCP, *UDP*, and *ICMP* determine the time period (in seconds) in which the NAT context is retained for the respective connection after the last packet transferred.

TCP-fin, like the TCP timer, determines the time period in which the NAT context is retained for the respective TCP connection. This timer takes effect when the TCP connection is canceled by a connection partner, but has not yet been acknowledged by the other side. This makes it possible to release NAT contexts within a short time period even when the connection has not been correctly closed by both sides.

SOHO, DSL, L

PPP configuration

You can configure the PPP connections using the dialog under TCP/IP → *e*xternal → PPP. If PPPoE is activated for LineCrypt L (IP → activate PPPoE) or if your LineCrypt is type DSL, you only need to configure the settings for:

- PPP → Connection → Name
- PPP → Connection → inactivity timeout
- PPP → PPP partner → User and
- PPP → PPP partner → Password

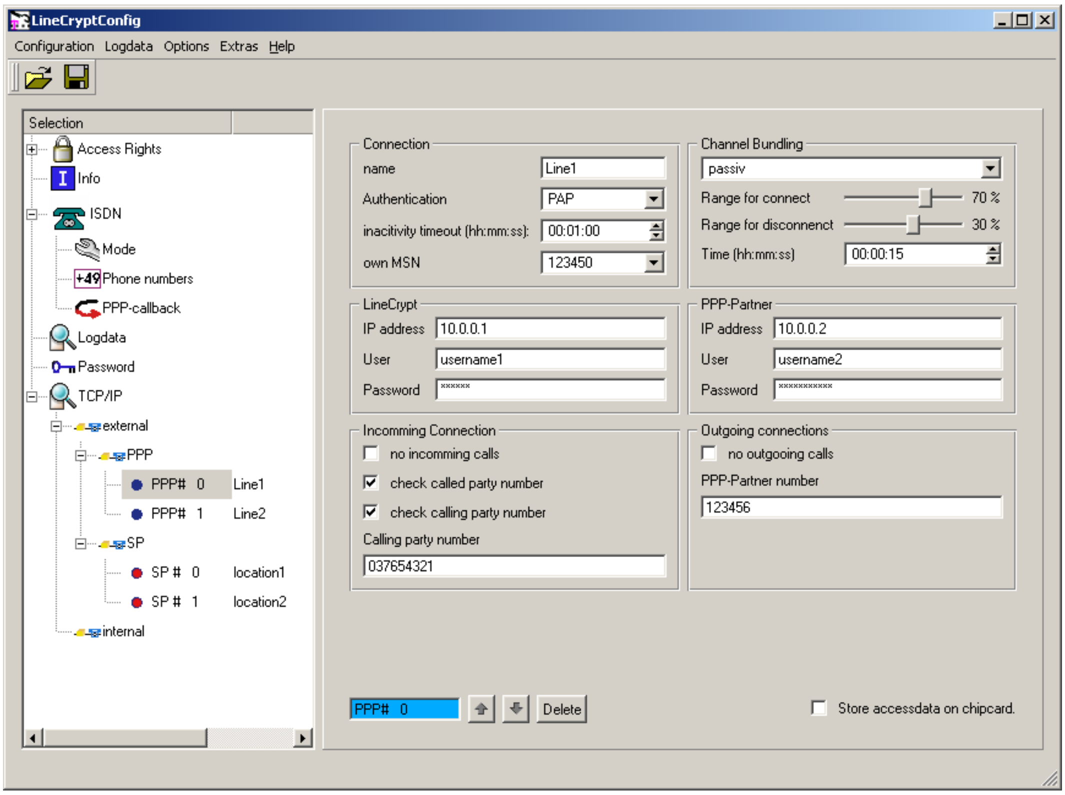
LineCrypt DSL and LineCrypt L with activate PPPoE support only one PPP entry.

To configure a PPP connection, the following details are generally necessary:

Connection

First enter a unique, descriptive *name* of your choice for the PPP connection. Select the Authentication type to be used for incoming connections. You have the following selection options:

none	No authentication
PAP	Transfer user name and password in plaintext (for example, for T-Online)
CHAP	The password is transferred encrypted. Authentication is repeated every 60 seconds.
CHAP (one)	Authentication is executed once only during connection setup.



Connection
name: Line1
Authentication: PAP
inactivity timeout (hh:mm:ss): 00:01:00
own MSN: 123450

Channel Bundling: passiv
Range for connect: 70 %
Range for disconnect: 30 %
Time (hh:mm:ss): 00:00:15

LineCrypt
IP address: 10.0.0.1
User: username1
Password: ******

PPP-Partner
IP address: 10.0.0.2
User: username2
Password: ***********

Incomming Connection
□ no incomming calls
☑ check called party number
☑ check calling party number
Calling party number: 037654321

Outgoing connections
□ no outgooing calls
PPP-Partner number: 123456

PPP# 0

□ Store accessdata on chipcard.

Figure 15: PPP-Settings

For every PPP connection, you can set the time period after which the connection is to be shut down if no data is transferred. Enter this time period in the *inactivity timeout* field.

When using the directory service functionality, please ensure that the time specified here is coordinated with the life time (TTL) of directory service storage. Otherwise continuous connections can occur.

If you configure the ISDN access as Point-to-Multipoint (see page 15), you can select from the *own MSN* list box one of the MSN entered in the dialog under ISDN → Phone numbers. If configuring as an ISDN PABX line, you can select the *local number* here. In this way, you define the end number, which is used in connection with the basic call number entered.

Outgoing ISDN connections are made under the selected MSN or end number.

If the button described later PPP → Incoming connections → calling party number number is not enabled, the first PPP connection is used for an incoming connection. If this button is enabled, the first PPP connection whose own MSN corresponds to the called number is used. Therefore, if you configure several PPP connections with the same MSN, you should take into account the sequence.

Channel Bundling

Here you select whether you want to use ISDN channel bundling. If you use channel bundling, the second ISDN B channel is also used for data transmission when a defined bandwidth is exceeded. You have the following selection options:

no channel bundling – channel bundling is not supported

passive channel bundling – channel bundling is supported if requested by the opposite side

active channel bundling – channel bundling is supported and initiated if required

Range for connect

Here you can define the bandwidth that triggers the setting up of the second B channel when it is exceeded.

Range for disconnect

Here you can define the bandwidth that triggers the shutdown of the second B channel when it is fallen below.

Time

The bandwidth necessary to trigger the setting up or shutdown of a connection must be exceed or fallen below for a specific period of time. You can define this time here.

LineCrypt

In the IP address field, enter the local IP address of the LineCrypt for the selected PPP connection. If you requested authentication under PPP → Connection → Authentication, the LineCrypt requires the remote side to enter the *User* name and *Password*. Enter this data in the fields provided.

If the connection is not established on account of incorrect user data, you will find entries in the following form in the log data:

```
PPP[0]: outgoing PAP authentication failed for: 001234123123123545454545#0001@t-online.de
PPP[0]: outgoing CHAP authentication failed for: 0001234123123123545454545#0001@t-online.de
```

PPP-Partner

Enter the *IP address* of the PPP partner. If you want the IP address to be allocated, enter 0.0.0.0 here. For the authentication types PAP and CHAP, a *User* name and *Password* are required for the logon on the opposite side. You can enter them here. The LineCrypt uses the user name and password if the remote side requests authentication.

Incoming connection

If you do not want to allow any incoming calls, enable the *no incoming calls* button. In this case, you do not need to perform any further settings.

If you enable the *check called party number* button, only calls to the LineCrypt own MSN or local number are accepted.

Using the *check calling party number* button, define whether the transferred call number is to be checked with the number configured in the *calling party number* field for incoming calls.

Outgoing connections

If you enable the *no outgoing calls* switch, no outgoing calls are allowed. The *PPP partner number* is used if the PPP connection is initiated by the local side.

Store access data on chip card

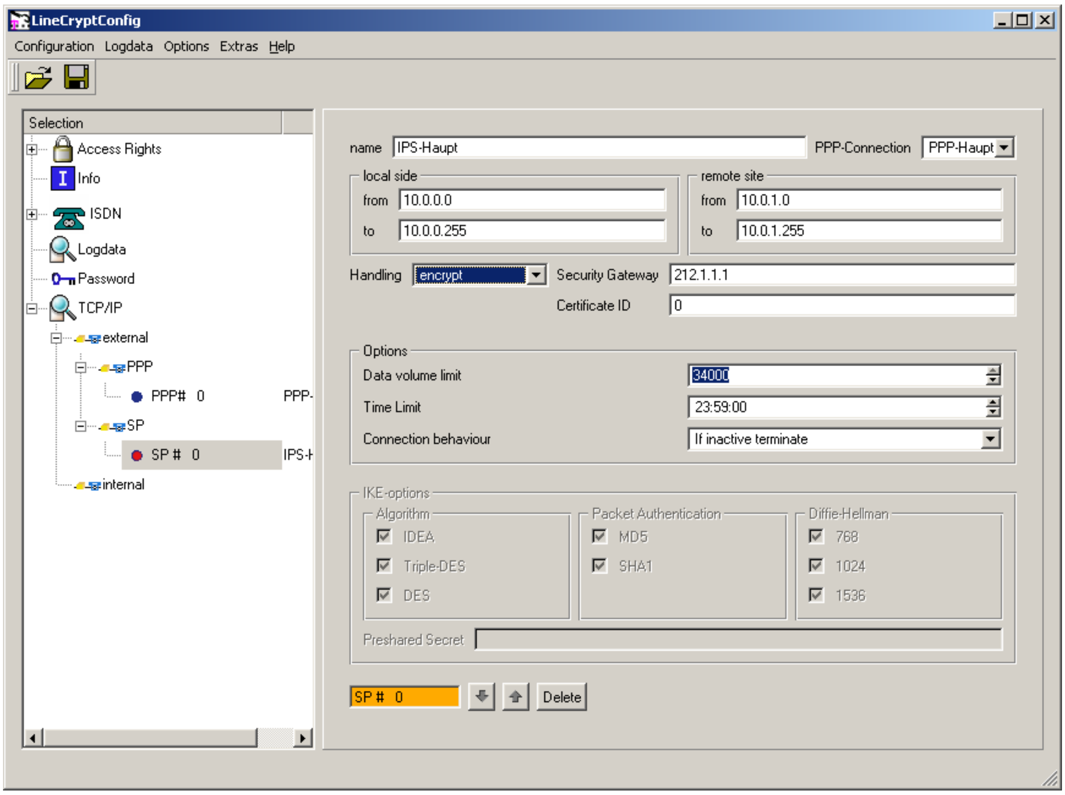
If this switch is enabled, the access data stored on the chip card is used instead of the entries defined in the configuration. The configuration of the access data is described on page 42.

DSL, L, L100, SOHO

Configuration Security Policies

You can configure the Security Policy rules using the dialog under **TCP/IP** → **External** → **SP**.

A Security Policy defines a range of IP addresses for the local and remote side, and how IP packets that fulfill these IP addresses are to be handled by the LineCrypt (forward encrypted or unencrypted, or discard).



name: IPS-Haupt
PPP-Connection: PPP-Haupt

local side
from: 10.0.0.0
to: 10.0.0.255

remote site
from: 10.0.1.0
to: 10.0.1.255

Handling: encrypt
Security Gateway: 212.1.1.1
Certificate ID: 0

Options
Data volume limit: 34000
Time Limit: 23:59:00
Connection behaviour: If inactive terminate

IKE-options
Algorithm: ☑ IDEA ☑ Triple-DES ☑ DES
Packet Authentication: ☑ MD5 ☑ SHA1
Diffie-Hellman: ☑ 768 ☑ 1024 ☑ 1536
Preshared Secret:

SP # 0

Figure 16: Security Policy Configuration

You should take into account the sequence of the Security Policies in the dialog box, since the LineCrypt always applies the first suitable rule. You can change the sequence using the arrow buttons in the lower part of the dialog.

You should give every Security Policy a unique *name*.

For a LineCrypt SOHO, you must specify the *PPP-connection* over which data applicable to the Security Policy is to be sent. LineCrypt L and DSL support PPP over Ethernet (PPPoE) only, and allow only one PPP connection.

Any attempt to set up IP connections that do not fall into the IP address ranges defined by the Security Policies for the local side and remote side is rejected by the LineCrypt. If the remote connection partner is a LineCrypt, a suitable Security Policy that authorizes the local LineCrypt for communication must be configured in the remote partner device.

Whilst only the relevant IP address ranges of the local and remote side need to be specified for an unencrypted connection, additional details are necessary for an encrypted connection. The local tunnel end point is given through the local IP address of the local LineCrypt PPP connection used.

The specification of a *Security Gateway* defines the second tunnel end point. Therefore enter the external IP address of the remote LineCrypt here. In this case, an additionally entered certificate number is not used by the LineCrypt.

If you do not know the security gateway's IP address and an inquiry first has to be made to the directory service, set the security gateway's IP address to 0.0.0.0. This is generally the case if you want to communicate with a LineCrypt DSL or another LineCrypt with no permanent IP address. In this case, enter the certificate number of the partner device in the *Certificate ID* field.

If you set the security gateway's IP address to 0.0.0.0 and the partner device's certificate number to 0, only incoming connections are possible.

In the *Handling* list box, you define what is to happen with the selected data packets. Here you have the following options:

encrypt

Communication between the local and remote network side takes place over an encrypted IPSec tunnel. For this, the specification of the security gateway and the PPP entry to be used is necessary. This mode is recommended if you want to establish encrypted connections with other LineCrypt.

encrypt with IKE

As for encrypt, with the difference that the IKE key exchange protocol is used.

DES and Triple-DES encryption are optionally available for the user data encryption.

not encrypt

The data packets are forwarded unchanged. Unencrypted communication is therefore possible.

reject

The data packets are discarded, that is, they are neither forwarded nor processed in any way. No communication is established. The data packet's sender receives an ICMP message "Destination unreachable".

not encrypt, NAT

The IP addresses of the data packets are translated using NAT. No encryption takes place.

Local and remote side

Under local side and remote side, you can set the IP addresses for which the rule is to apply. From the range of IP addresses, enter the first and last address for which the rule is to apply.

If you want a rule to apply for all IP addresses, set *from* to 0.0.0.0 and *to* to 255.255.255.255. If you want to select an individual address, enter this address in the *from* and *to* fields.

Options

- Data volume limit -Enter the maximum data quantity transported with a key (in MB). The largest data quantity that can be set is 34000 MB.

- *Time limit* – You can define a key's validity period in this field. The maximum validity period is 23 hours and 59 minutes (that is, 1439 minutes) and can be set to the minute.

If the time given by the time restriction or the data quantity given by the volume restriction is reached, the session key used becomes invalid. A new authentication is performed just beforehand, and a new session key is generated.

You can specify a *Connection behavior* for the IPSec tunnel.

- If inactive terminate – If no IP packets are transferred for 16 minutes, the IPSec tunnel is terminated.

- Keep inactive connection – The IPSec tunnel is not shut down within the key's life if the connection is inactive.

- Set up connection always – An IPSec tunnel is set up spontaneously and is continually retained even if there are no IP packets to transport.

L, SOHO

IKE-Options

You can perform the following settings for the IKE key exchange protocol. These settings are only available if you selected the *encrypt with IKE* action:

- *Algorithm*: Supported encryption algorithms (IDEA, Triple-DES, and DES)

- Supported Hash algorithms for the *Packet authentication* (MD5 and SHA-1)

- Supported key lengths of the *Diffie-Hellman* key generation (768, 1024, and 1536 bit)

- *Preshared secret*: The preshared secret is used for the authentication of the partner devices. Both devices must use the same value. Enter a 32-digit hexadecimal number here.

Rights configuration

When setting up an encrypted connection, LineCrypt I, IT, and I+ use the certificates stored on the chip card.

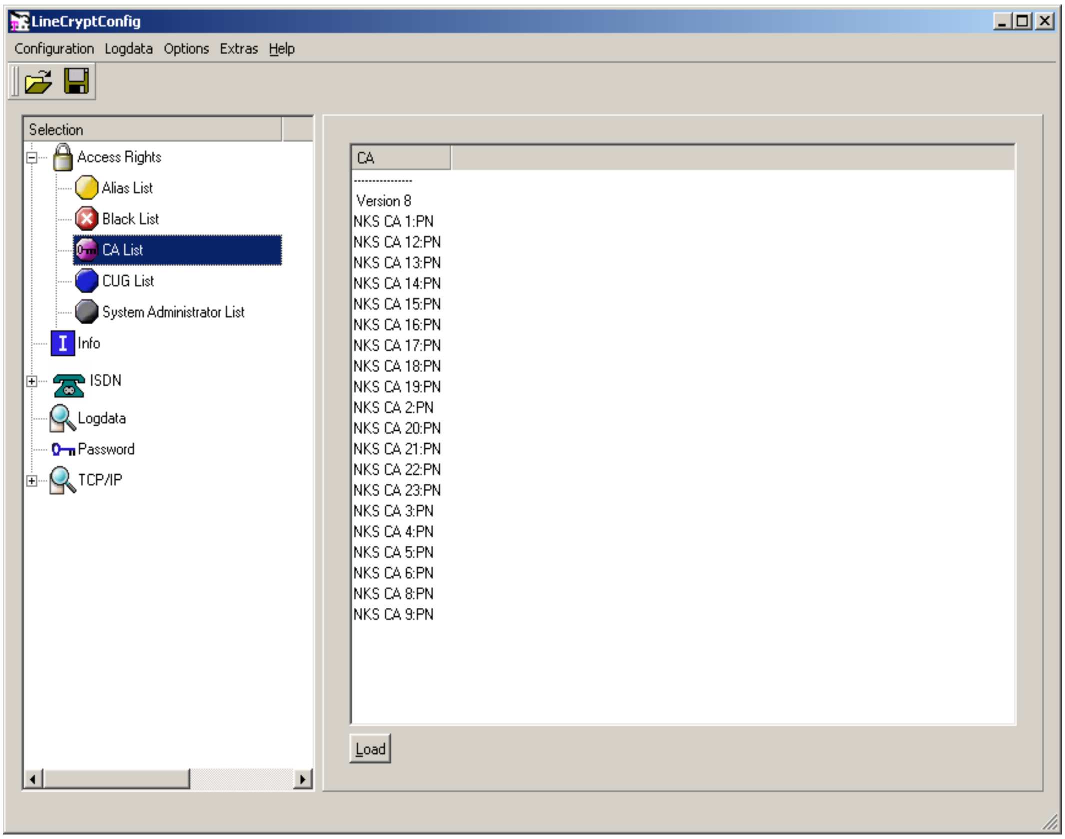
These certificates are used for the LineCrypt types DSL, L, and SOHO if you selected the ”encrypt” option in the Handling list box for the relevant Security Policy (in the dialog under TCP/IP → External → SP on page 31). If you selected a different option (”not encrypt”, ”encrypt with IKE”, ”not encrypt, NAT” or ”reject”), the certificates are not used and the mechanisms described in this section are not deployed!

If an encrypted connection is to be set up between two LineCrypt, the LineCrypt establishes an encrypted connection between authorized communication partners only. For the partner’s identification, the certificate number stored on the chip card (see also page 7) is used.

CA-List

The CA list contains the keys used to check the partner certificates. Partner certificates that were signed with keys not on the CA list are not accepted. In the case, you require an updated CA list. After receiving a new CA list, you can transfer it to the configuration with the ”Load” button.

The connection between two terminals is only established if both LineCrypt accept one another as authorized partners. If there are problems, you should view the log file.

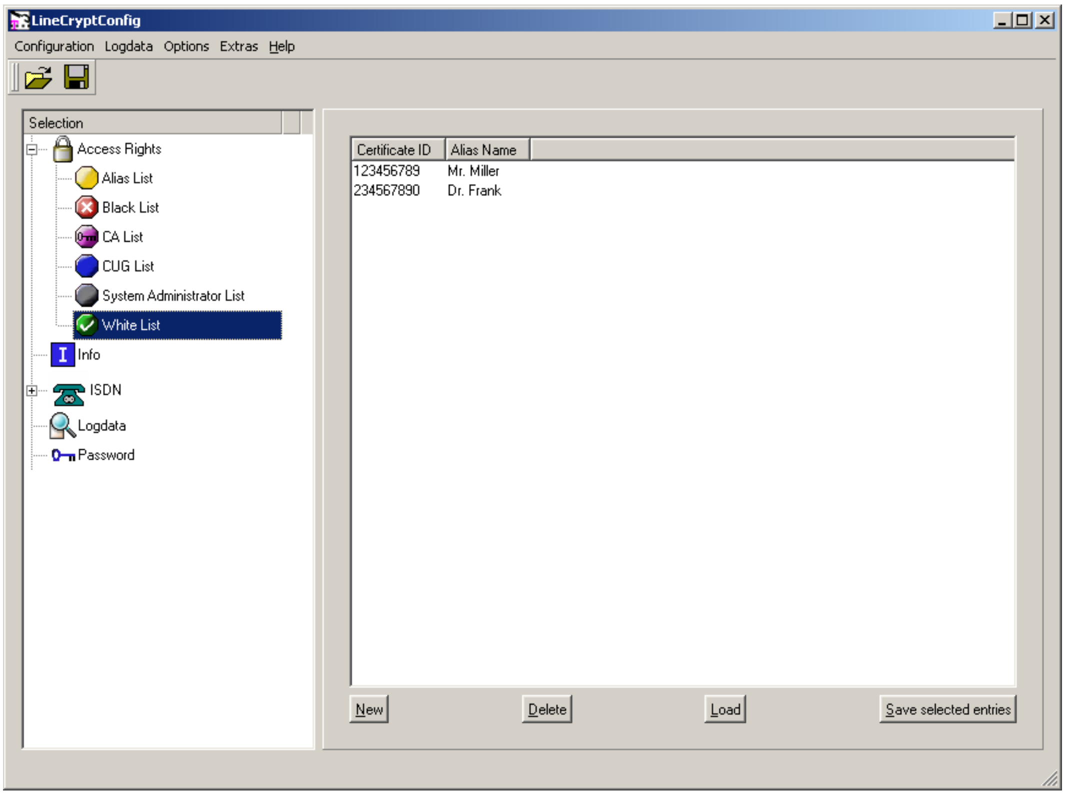


```
---------------
Version 8
NKS CA 1:PN
NKS CA 12:PN
NKS CA 13:PN
NKS CA 14:PN
NKS CA 15:PN
NKS CA 16:PN
NKS CA 17:PN
NKS CA 18:PN
NKS CA 19:PN
NKS CA 2:PN
NKS CA 20:PN
NKS CA 21:PN
NKS CA 22:PN
NKS CA 23:PN
NKS CA 3:PN
NKS CA 4:PN
NKS CA 5:PN
NKS CA 6:PN
NKS CA 8:PN
NKS CA 9:PN
```

Figure 17: CA-List

Rights check procedure

The certificate numbers of authorized partners are entered in the white list, non-authorized partners in the black list. The black list takes precedence over all other lists. If a certificate number can be found both in the white list and in the black list, no connection is set up.



Certificate ID	Alias Name
123456789	Mr. Miller
234567890	Dr. Frank

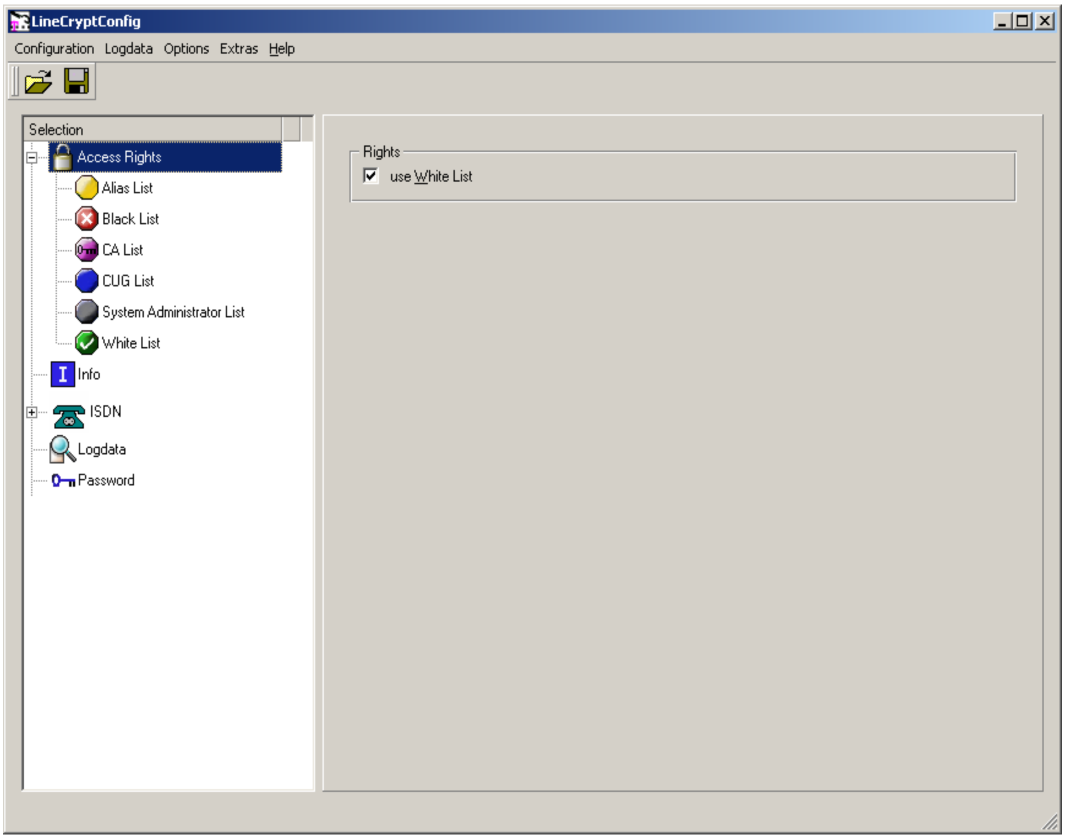
Figure 18: White List

If you do not use a Company Card, the CUG list is empty and the activated white list has no entries, no encrypted connections can be set up. If you want all partners except for those on the black list to be accepted, you should deactivate the white list.

Partners entered in the system administrator list are authorized to configure the LineCrypt over the ISDN line (types I, IT, and I+) or over the network (types L,L100,SOHO, and DSL). If you leave this list empty, the LineCrypt can only be configured via the serial interface.

Special chip cards (Company Card) contain a user group characteristic. This enables the implementation of closed user groups. The characteristic can be entered in the user group list, and allows all cards that have this characteristic and are not on the black list to set up an encrypted connection.

Every entry in the white, black, and system administrator list can contain an alias name. This alias name is used for log file analysis (to make the entries more readable). Alias names for certificates that are not used in any of the three lists specified can be stored in the alias list.



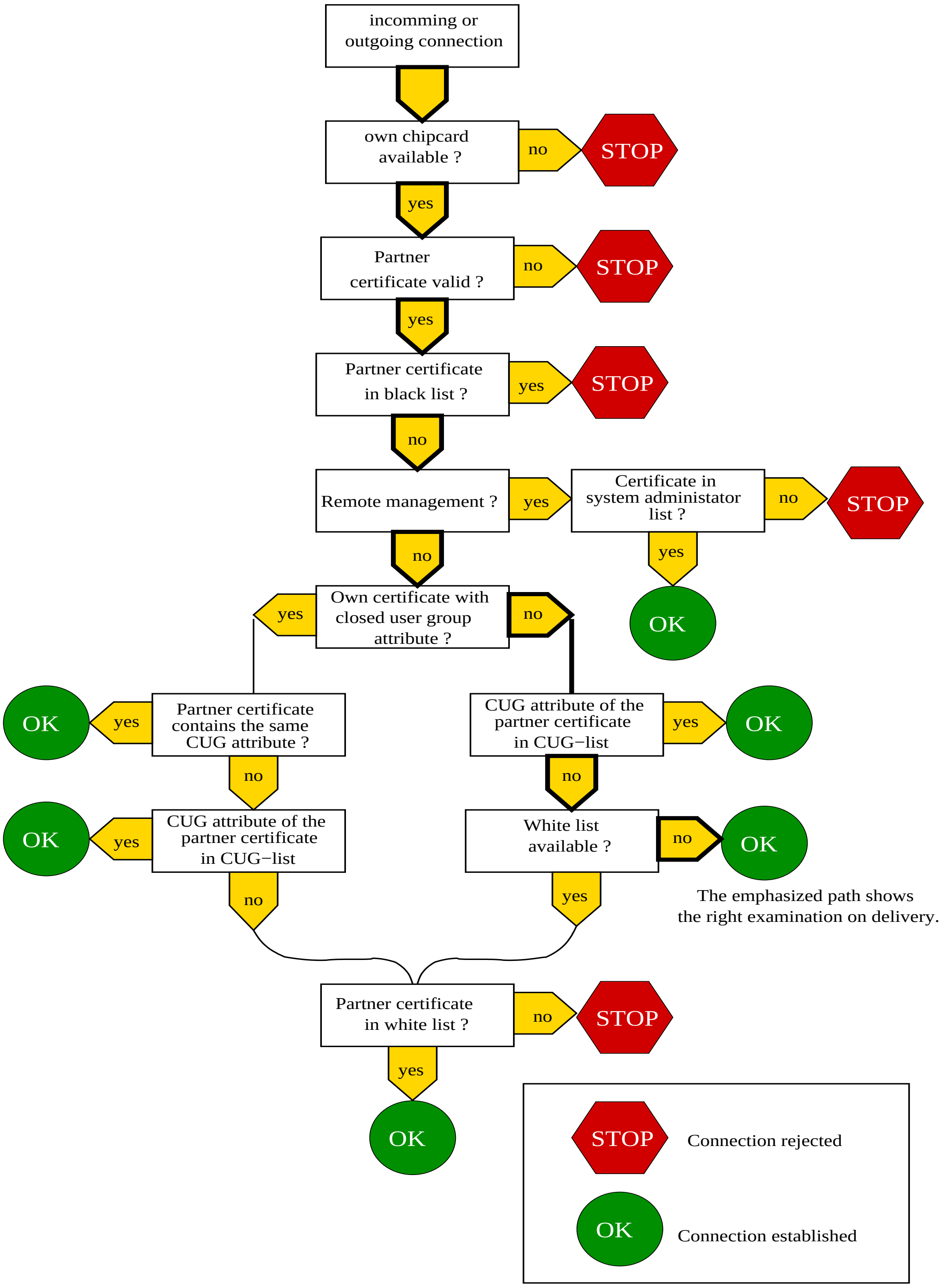
Rights
☑ use White List

Figure 19: use White List

If you want encrypted communication with just a few partners, activate the white list (see figure 19) and enter all the partners in the white list.

If you want encrypted communication with many partners of a group, use a Company Card or enter the user group characteristic in the user group list.

If you basically want encrypted communication with anyone who has a valid chip card, deactivate the white list and enter just the cards you want to exclude in the black list.



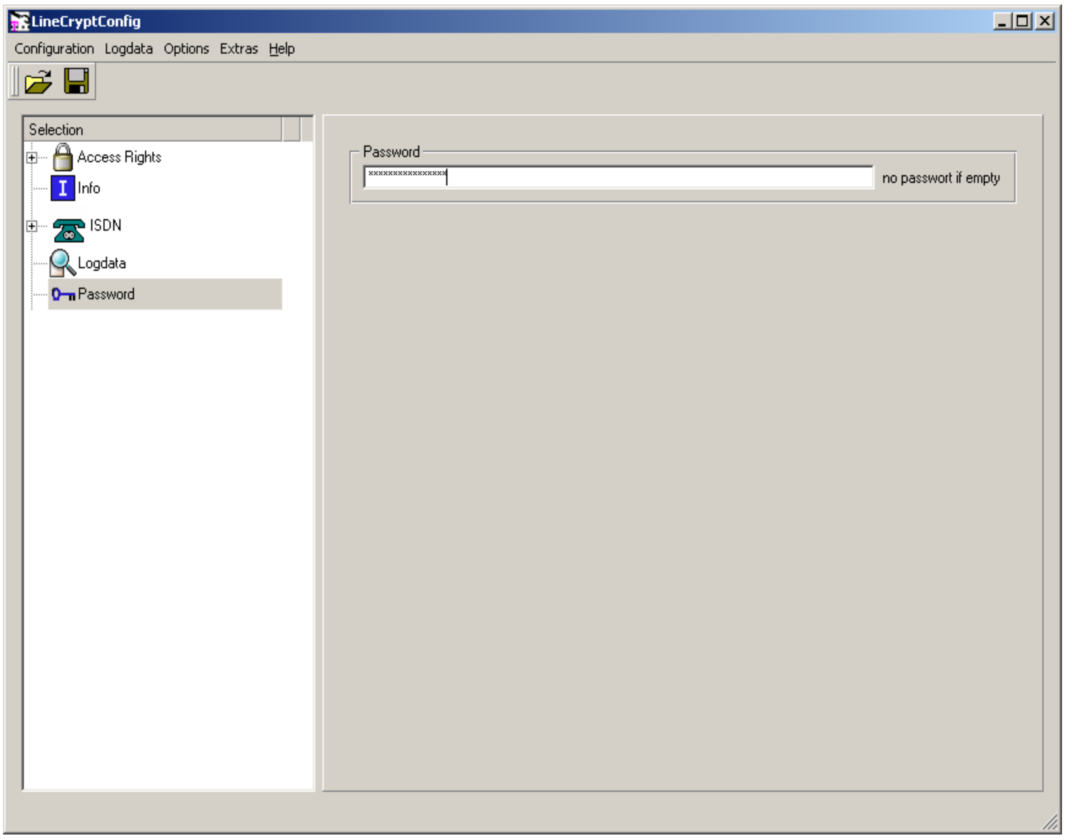
incomming or outgoing connection
own chipcard available ?
no
STOP
yes
Partner certificate valid ?
no
STOP
yes
Partner certificate in black list ?
yes
STOP
no
Remote management ?
yes
Certificate in system administator list ?
no
STOP
yes
OK
no
Own certificate with closed user group attribute ?
yes
no
Partner certificate contains the same CUG attribute ?
yes
OK
no
CUG attribute of the partner certificate in CUG−list
yes
OK
no
CUG attribute of the partner certificate in CUG−list
yes
OK
no
White list available ?
no
OK
yes
The emphasized path shows the right examination on delivery.
Partner certificate in white list ?
no
STOP
yes
OK
STOP
Connection rejected
OK
Connection established

Figure 20: Procedure for checking rights

Figure 20 shows the procedure for checking rights in detail.

Password

Changes to the LineCrypt configuration can be password-protected. If you leave the field empty, there is no password protection. This password is not identical to the chip card PIN and is stored in the LineCrypt.



Password: ****************

no passwort if empty

Figure 21: Password

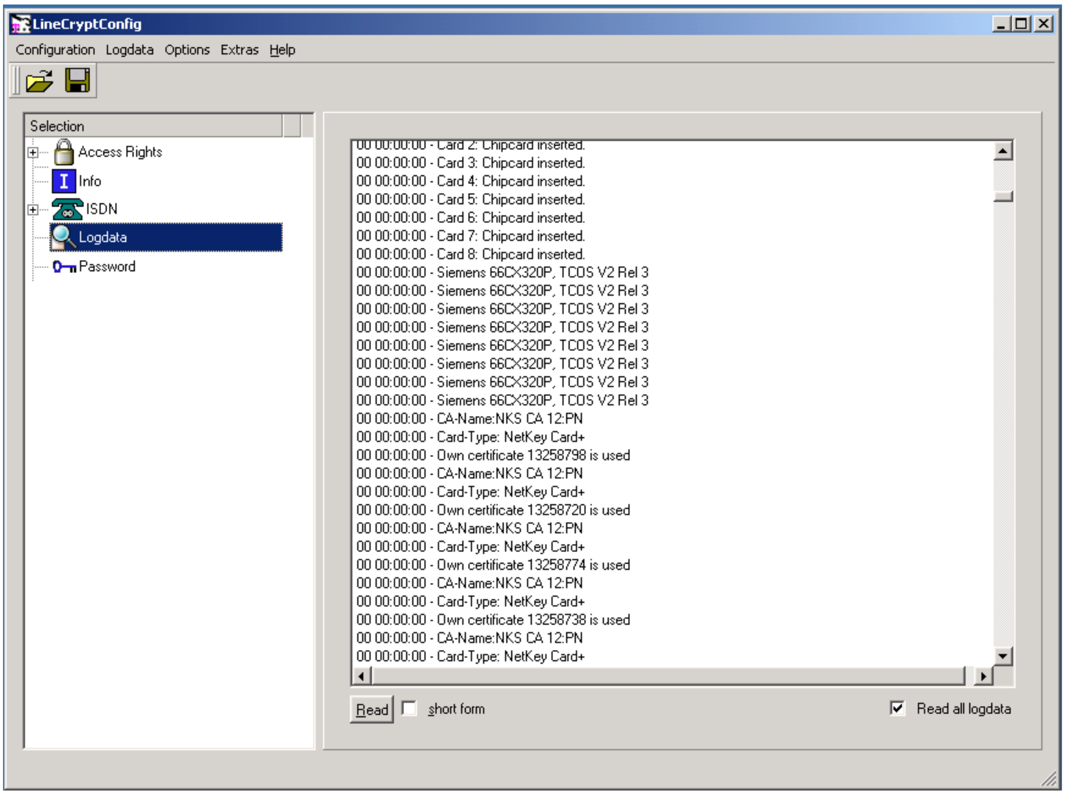
Pay attention to spaces when making your entry. Spaces are valid characters in the password. Even passwords that consist entirely of spaces are valid, although they should not be used!

If you want to use a LineCrypt password, make a note of it and keep it in a safe place. If you set up a LineCrypt password and lose it, you will only be able to use your LineCrypt management functions again after a chargeable service intervention.

Log data

You can view information about the connections using the log data dialog.

The log file is deleted when a new configuration is written to the LineCrypt. To delete the log file explicitly, select the *Delete Logdata* menu command on the *Logdata* menu.



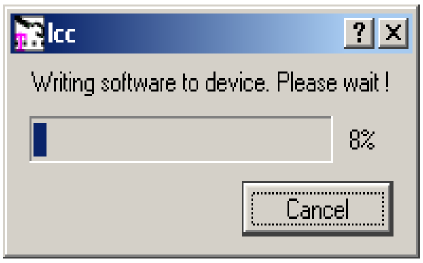
```
00 00:00:00 - Card 2: Chipcard inserted.
00 00:00:00 - Card 3: Chipcard inserted.
00 00:00:00 - Card 4: Chipcard inserted.
00 00:00:00 - Card 5: Chipcard inserted.
00 00:00:00 - Card 6: Chipcard inserted.
00 00:00:00 - Card 7: Chipcard inserted.
00 00:00:00 - Card 8: Chipcard inserted.
00 00:00:00 - Siemens 66CX320P, TCOS V2 Rel 3
00 00:00:00 - Siemens 66CX320P, TCOS V2 Rel 3
00 00:00:00 - Siemens 66CX320P, TCOS V2 Rel 3
00 00:00:00 - Siemens 66CX320P, TCOS V2 Rel 3
00 00:00:00 - Siemens 66CX320P, TCOS V2 Rel 3
00 00:00:00 - Siemens 66CX320P, TCOS V2 Rel 3
00 00:00:00 - Siemens 66CX320P, TCOS V2 Rel 3
00 00:00:00 - Siemens 66CX320P, TCOS V2 Rel 3
00 00:00:00 - CA-Name:NKS CA 12:PN
00 00:00:00 - Card-Type: NetKey Card+
00 00:00:00 - Own certificate 13258798 is used
00 00:00:00 - CA-Name:NKS CA 12:PN
00 00:00:00 - Card-Type: NetKey Card+
00 00:00:00 - Own certificate 13258720 is used
00 00:00:00 - CA-Name:NKS CA 12:PN
00 00:00:00 - Card-Type: NetKey Card+
00 00:00:00 - Own certificate 13258774 is used
00 00:00:00 - CA-Name:NKS CA 12:PN
00 00:00:00 - Card-Type: NetKey Card+
00 00:00:00 - Own certificate 13258738 is used
00 00:00:00 - CA-Name:NKS CA 12:PN
00 00:00:00 - Card-Type: NetKey Card+
```

Figure 22: Logdata

L100 If the which “Read all logdata” is activated, the whole logfile will be read. If the switch is deactivated, only previously unread logdata will be read.

Softwareupdate

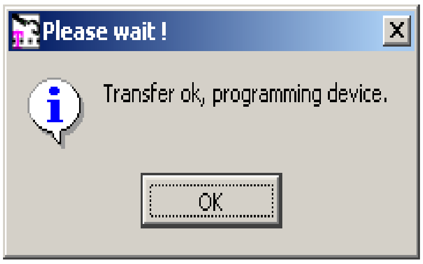
If there is new software, you can transfer it to the LineCrypt by selecting the *Software-update* menu command on the *Extras* menu. The new software only takes effect after a reset. To trigger the reset, select the *Reset* menu command on the *Extras* menu. With a software update, the log data is deleted.



Writing software to device. Please wait !

Figure 23: Software update

Only software whose version number is greater than or equal to the version number of the software in the LineCrypt can be imported.



Transfer ok, programming device.

Figure 24: LineCrypt is programmed

During the programming of the LineCrypt, the line voltage must not be interrupted or otherwise the new software will be inoperable and a chargeable service intervention will be necessary.

SOHO, DSL, L

Access data

To configure the access data, you use the configuration software's *Edit access data* mode. You can select this mode under the A*ccess data* menu command on the *Options* menu (see page 30). The access data is used if you enabled the Store access data on chip card switch in the dialog under TCP/IP → external → PPP.

Read the access data from the connected LineCrypt by selecting the **Read from device** menu command on the **Configuration** menu.

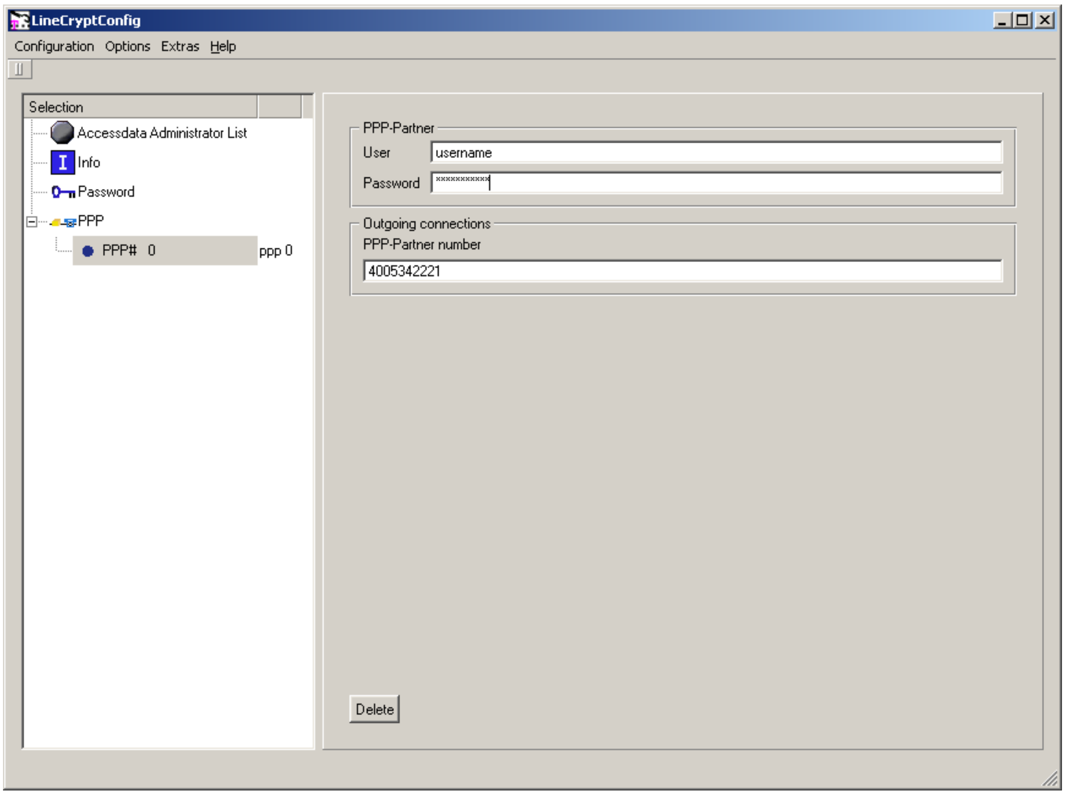
Enter the following access data for the active connections:

- Access name at the PPP partner (for example, 000123412312312354545454545#0001@t-online.de)

- password

- Telephone number to be called (only relevant for LineCrypt SOHO)

- List of certificate numbers of the system administrators who may view and change the access data via remote management.


LineCryptConfig
Configuration Options Extras Help
Selection
Accessdata Administrator List
Info
Password
PPP
PPP# 0
ppp 0
Delete

PPP-Partner

User username

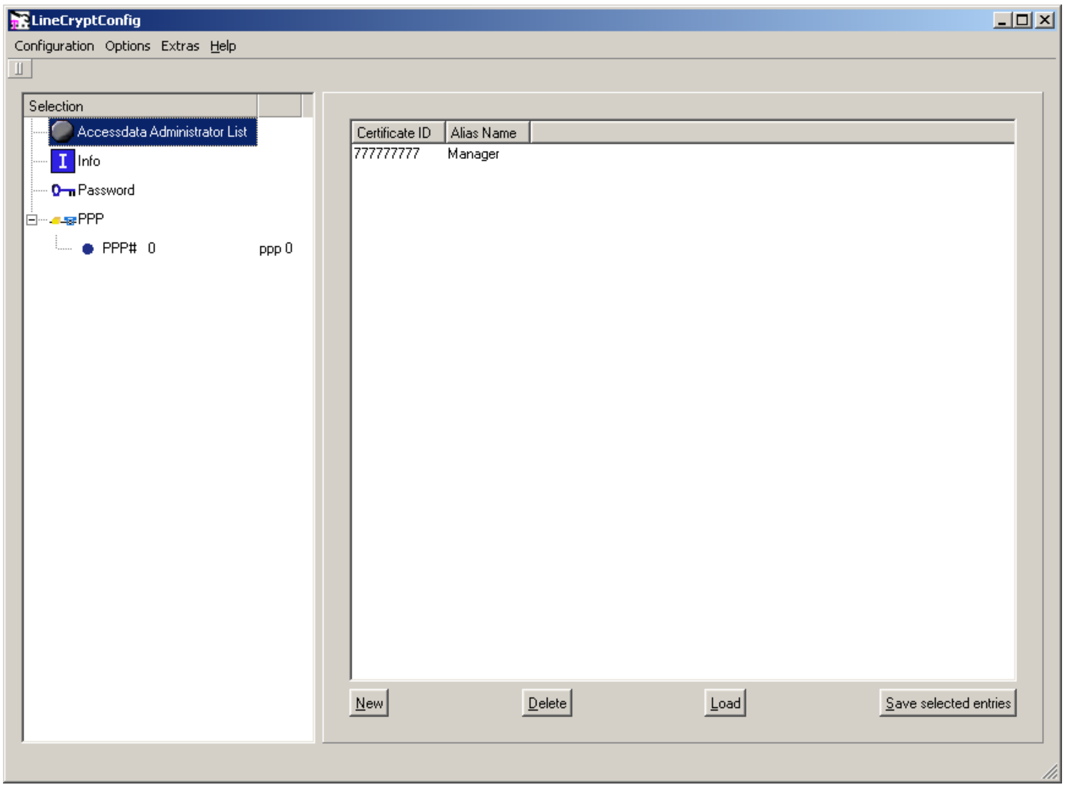
Password ***********

Outgoing connections

PPP-Partner number 4005342221

Figure 25: Access data configuration

If you want a system administrator to be able to view and change the access data over the network, enter the relevant certificate numbers in the dialog in figure 25. If this list remains empty, the access data can only be viewed and changed via the serial interface.



Certificate ID	Alias Name
777777777	Manager

Figure 26: Access data Administrator list

The access data can be protected via a separate password. This password is independent of the configuration password in the Password dialog on page 39.

Transfer the access data back to the LineCrypt by selecting the *Write to device* menu command on the *Configuration* menu.

Configuration examples

SOHO

Configuration of a virtual private network

The network shown in the picture below serves as an example of the configuration of a VPN with permanent IP addresses.

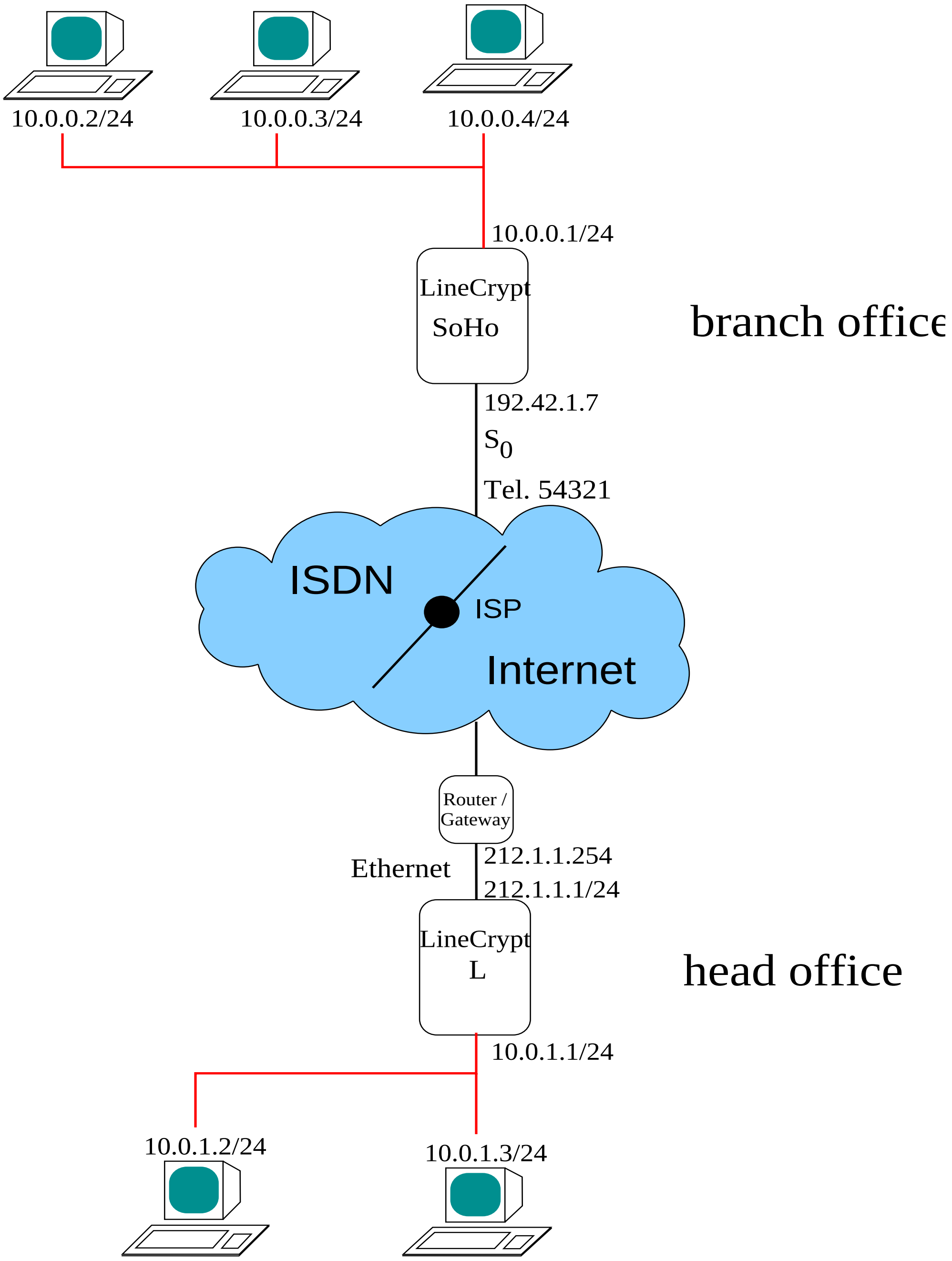
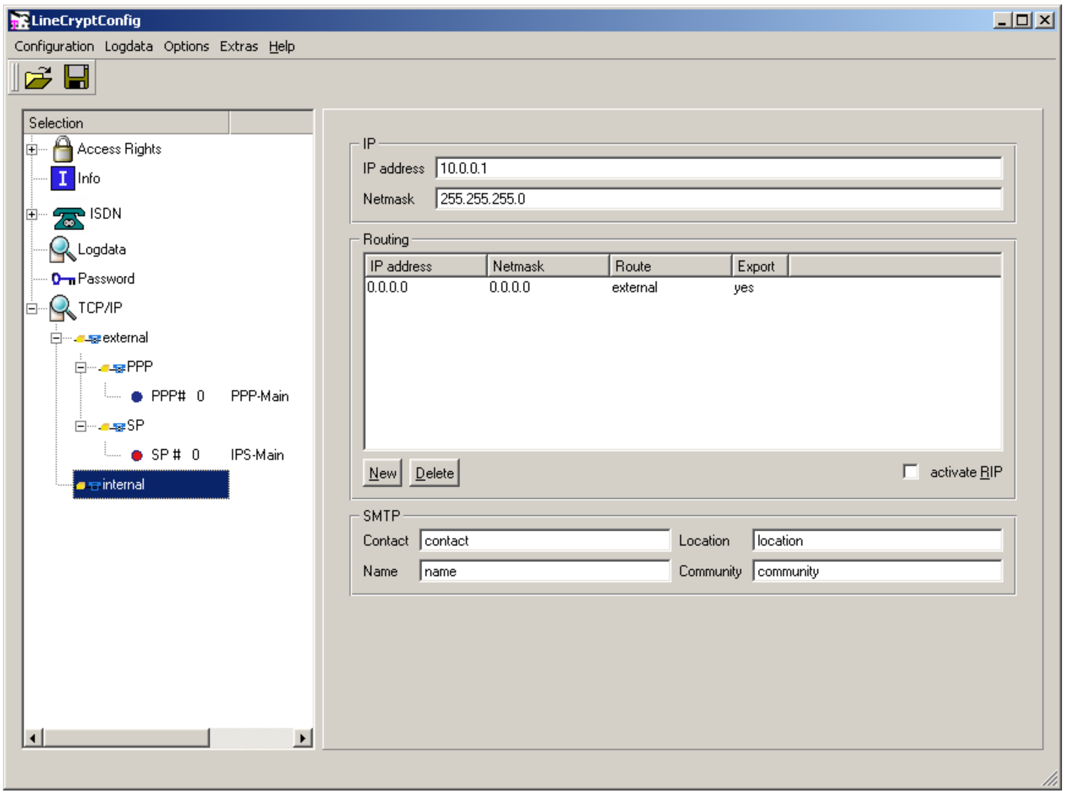


Figure 27: Example VPN

The example shows a branch office, which is connected via an ISDN line with an Internet Service Provider (ISP) that allocates permanent IP addresses. A secure connection is to be established from the branch office to the principal establishment. For this, a PPP connection to the ISP is established. Using this PPP connection, a secure IPSec connection is established for the setting up of a VPN.

TCP/IP configuration of the branch office’s LineCrypt



IP address 10.0.0.1

Netmask 255.255.255.0

IP address	Netmask	Route	Export
0.0.0.0	0.0.0.0	external	yes

□ activate RIP

Contact contact

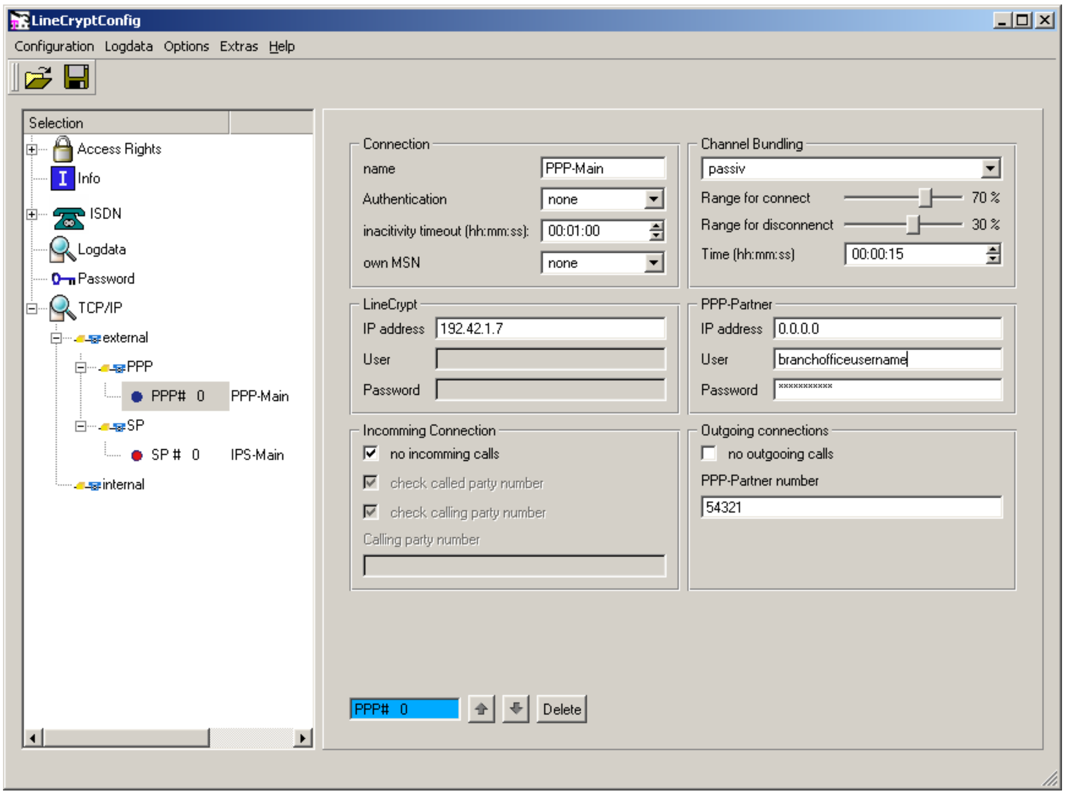
Location location

Name name

Community community

Figure 28: Branch office: TCP/IP - internal

In the dialog in figure 28, you need to enter the IP address and the network mask of the local LineCrypt. To enable encrypted communication, you must specify at least one route that has the entry ”external” in the Route column.



PPP# 0 PPP-Main

SP # 0 IPS-Main

Connection

name: PPP-Main

Authentication: none

inactivity timeout (hh:mm:ss): 00:01:00

own MSN: none

Channel Bundling: passiv

Range for connect: 70 %

Range for disconnect: 30 %

Time (hh:mm:ss): 00:00:15

LineCrypt

IP address: 192.42.1.7

User:

Password:

PPP-Partner

IP address: 0.0.0.0

User: branchofficeusername

Password: ***********

Incomming Connection

☑ no incomming calls

☑ check called party number

☑ check calling party number

Calling party number:

Outgoing connections

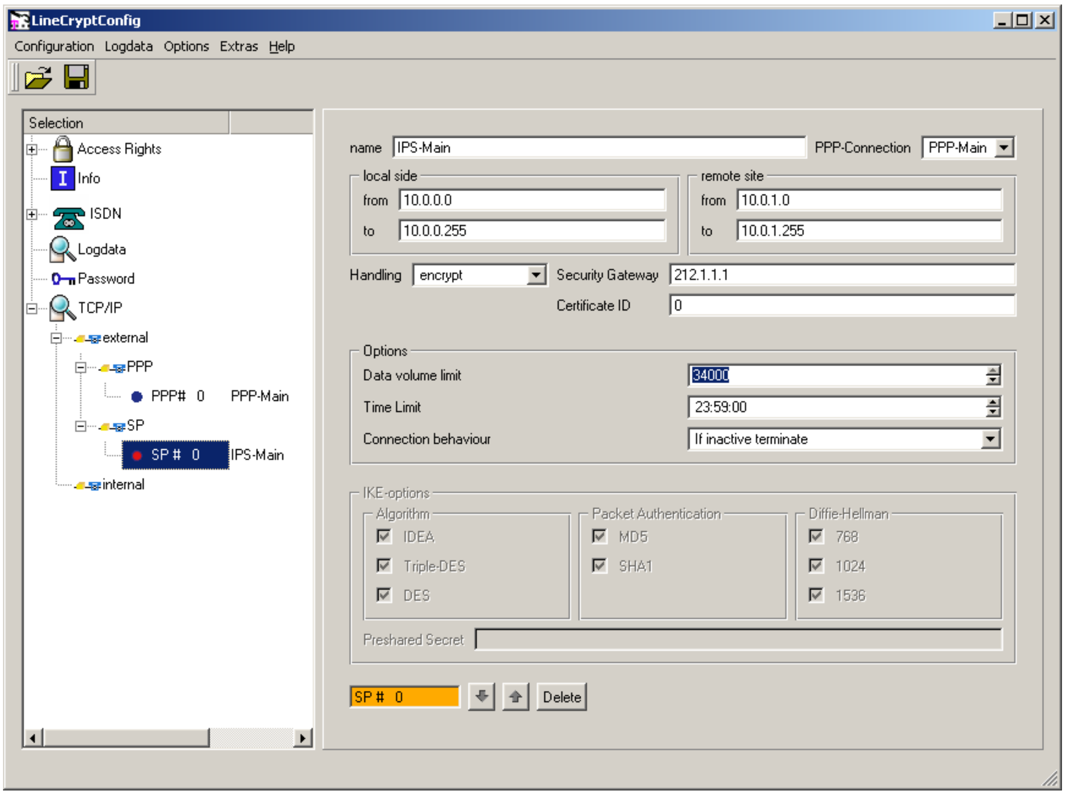
□ no outgooing calls

PPP-Partner number: 54321

PPP# 0

Figure 29: Branch office: PPP

The IP addresses and call numbers of the remote partner devices are configured in accordance with the network scheme shown. The LineCrypt sets up the connection to the ISP independently. No connections are set up from the ISP to the LineCrypt. To prevent any other dial-in, incoming calls are prohibited.



name: IPS-Main
PPP-Connection: PPP-Main

local side
from: 10.0.0.0
to: 10.0.0.255

remote site
from: 10.0.1.0
to: 10.0.1.255

Handling: encrypt
Security Gateway: 212.1.1.1
Certificate ID: 0

Options
Data volume limit: 34000
Time Limit: 23:59:00
Connection behaviour: If inactive terminate

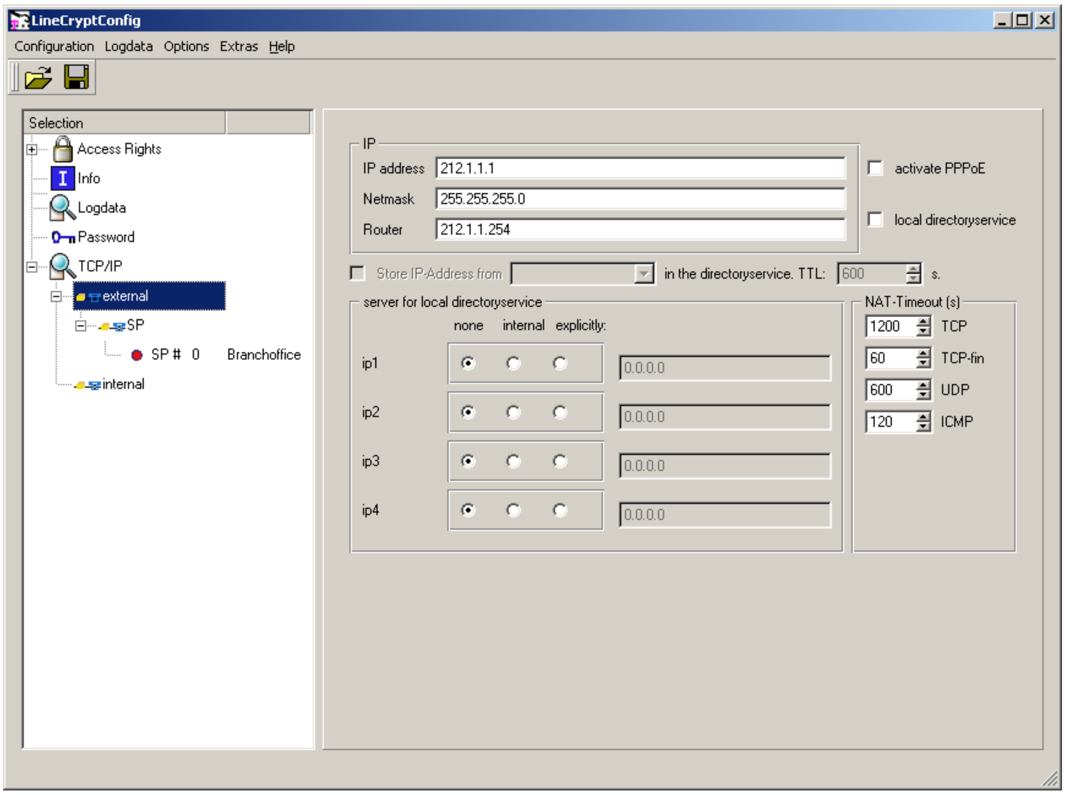
IKE-options
Algorithm: ☑ IDEA ☑ Triple-DES ☑ DES
Packet Authentication: ☑ MD5 ☑ SHA1
Diffie-Hellman: ☑ 768 ☑ 1024 ☑ 1536
Preshared Secret:

Figure 30: Branch office: Security Policy

If the remote connection partner is a LineCrypt (compulsory for encrypted connections (without IKE)), a suitable Security Policy that authorizes the local LineCrypt SOHO for communication must be configured in the remote partner device.

Configuration of the head office's LineCrypt

Figure 30 shows the configuration of the external Ethernet interface of the LineCrypt located at the head office.



- Access Rights
- Info
- Logdata
- Password
- TCP/IP
  - external
    - SP
      - ● SP # 0 Branchoffice
  - internal

IP
IP address 212.1.1.1
Netmask 255.255.255.0
Router 212.1.1.254

□ activate PPPoE
□ local directoryservice

□ Store IP-Address from [ ] in the directoryservice. TTL: 600 s.

server for local directoryservice

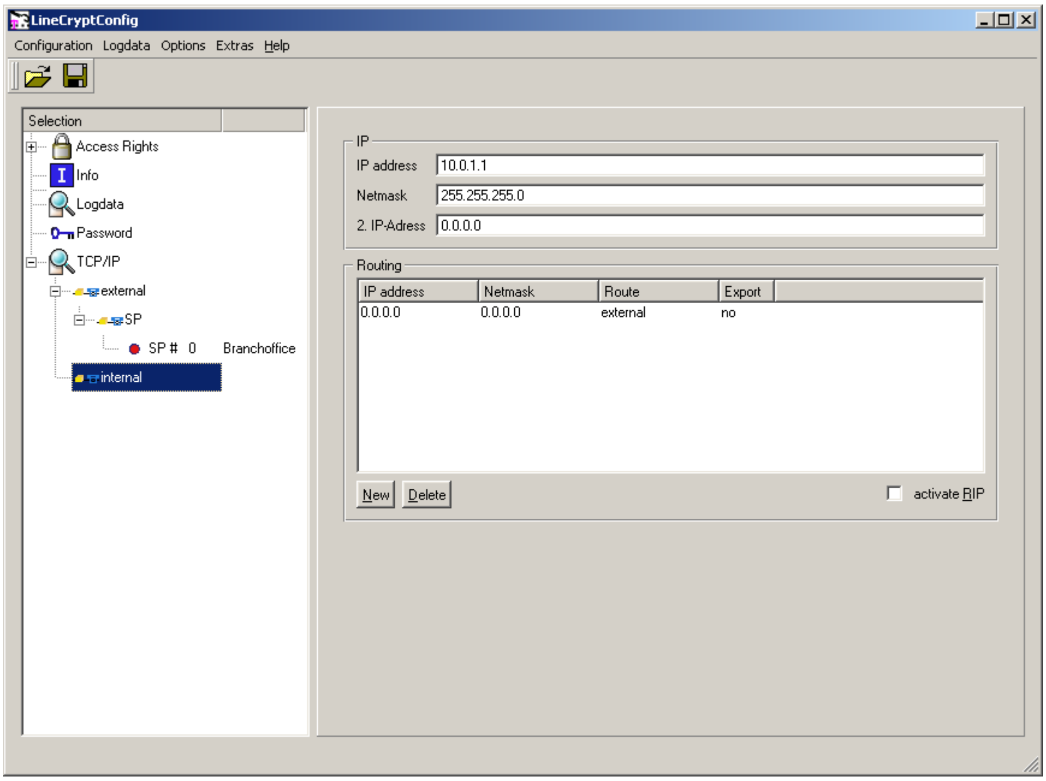
	none	internal	explicitly:	
ip1	●	○	○	0.0.0.0
ip2	●	○	○	0.0.0.0
ip3	●	○	○	0.0.0.0
ip4	●	○	○	0.0.0.0

NAT-Timeout (s)

1200	TCP
60	TCP-fin
600	UDP
120	ICMP

Figure 31: Head office: TCP/IP external

The configuration of the internal interface is shown in figure 31. For the branch office's LineCrypt to be able to communicate with the head office, at least one Security Policy entry is necessary. This type of entry is shown in figure 32.



IP

IP address 10.0.1.1

Netmask 255.255.255.0

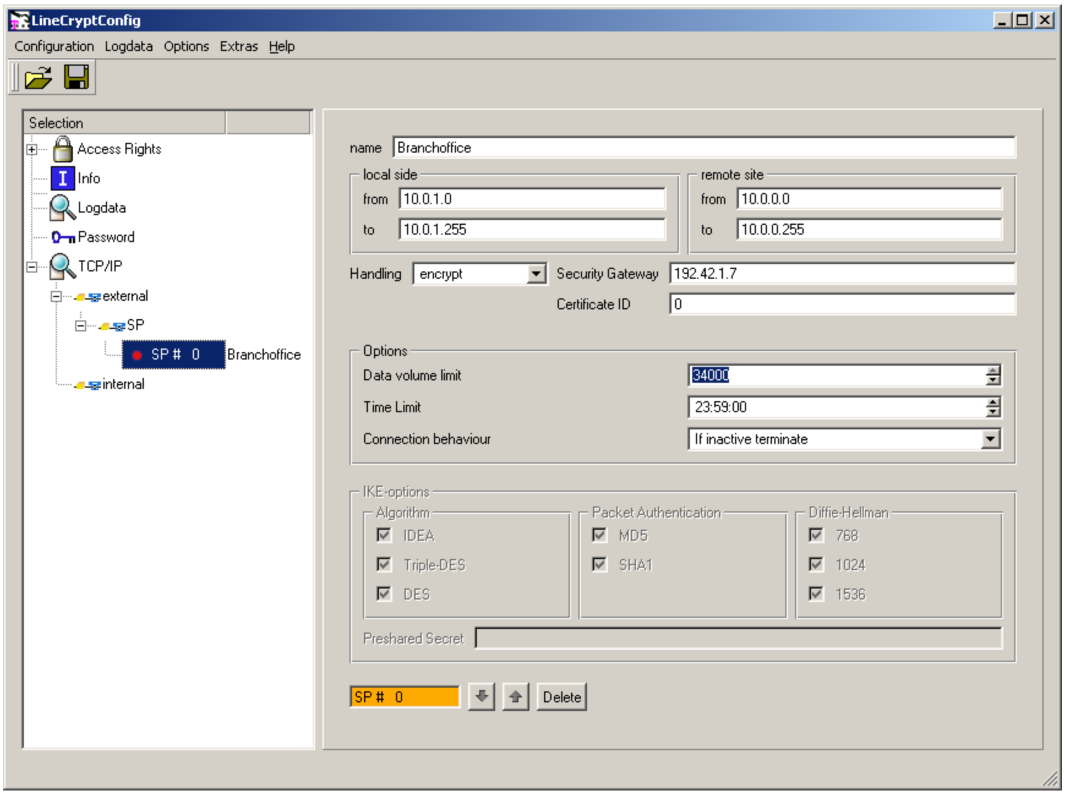
2. IP-Adress 0.0.0.0

Routing

IP address	Netmask	Route	Export
0.0.0.0	0.0.0.0	external	no

□ activate RIP

Figure 32: Head office: TCP/IP internal



name Branchoffice

local side: from 10.0.1.0 to 10.0.1.255

remote site: from 10.0.0.0 to 10.0.0.255

Handling encrypt

Security Gateway 192.42.1.7

Certificate ID 0

Options

Data volume limit 34000

Time Limit 23:59:00

Connection behaviour If inactive terminate

IKE-options

Algorithm: ☑ IDEA ☑ Triple-DES ☑ DES

Packet Authentication: ☑ MD5 ☑ SHA1

Diffie-Hellman: ☑ 768 ☑ 1024 ☑ 1536

Preshared Secret

Figure 33: Head office: Security Policy

DSL, L SOHO

Configuration with directory service (1 head office, 2 branch offices)

The example shows a company that operates a LineCrypt L at its head office. A branch office with a LineCrypt DSL and a branch office with a LineCrypt SOHO are connected via this LineCrypt. Both branch offices use Internet access with dynamic IP address allocation. A VPN is established between all locations via a PPP connection.

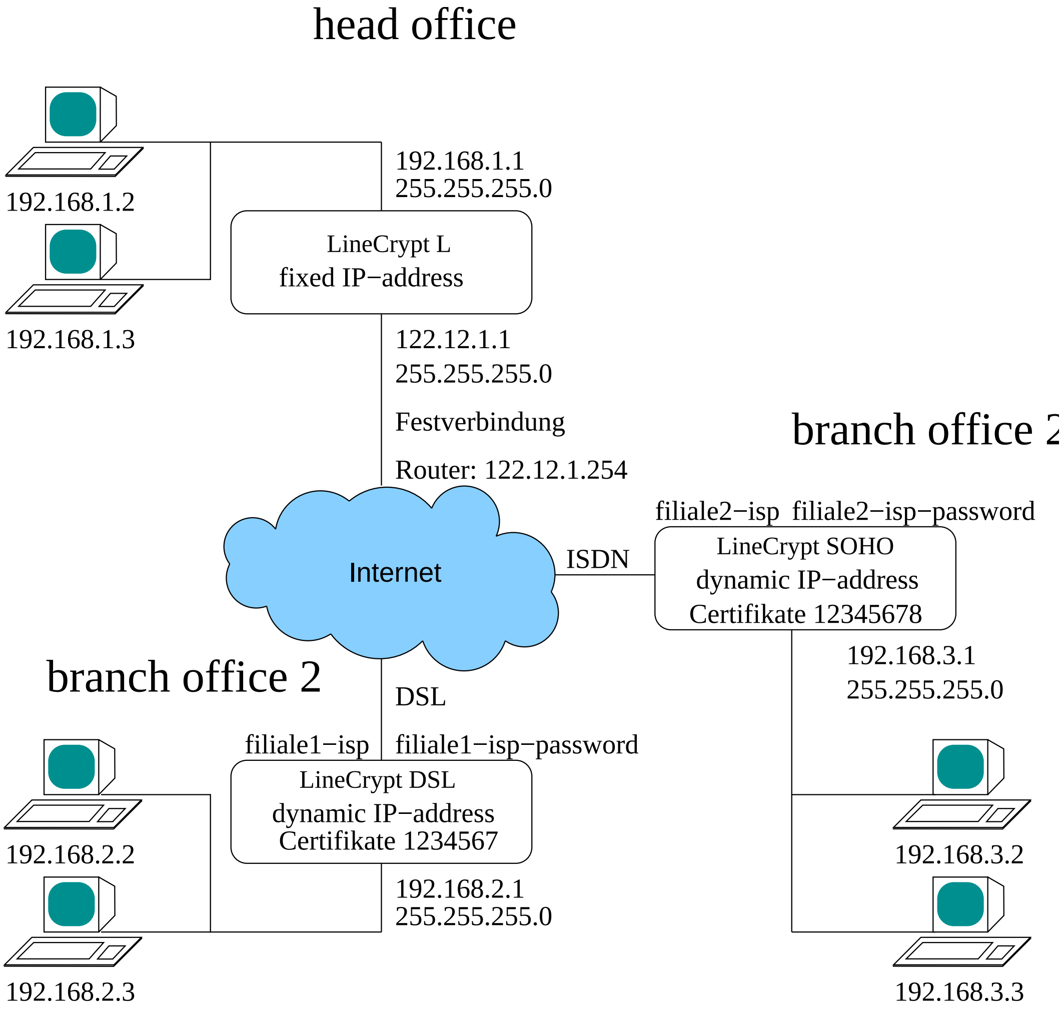
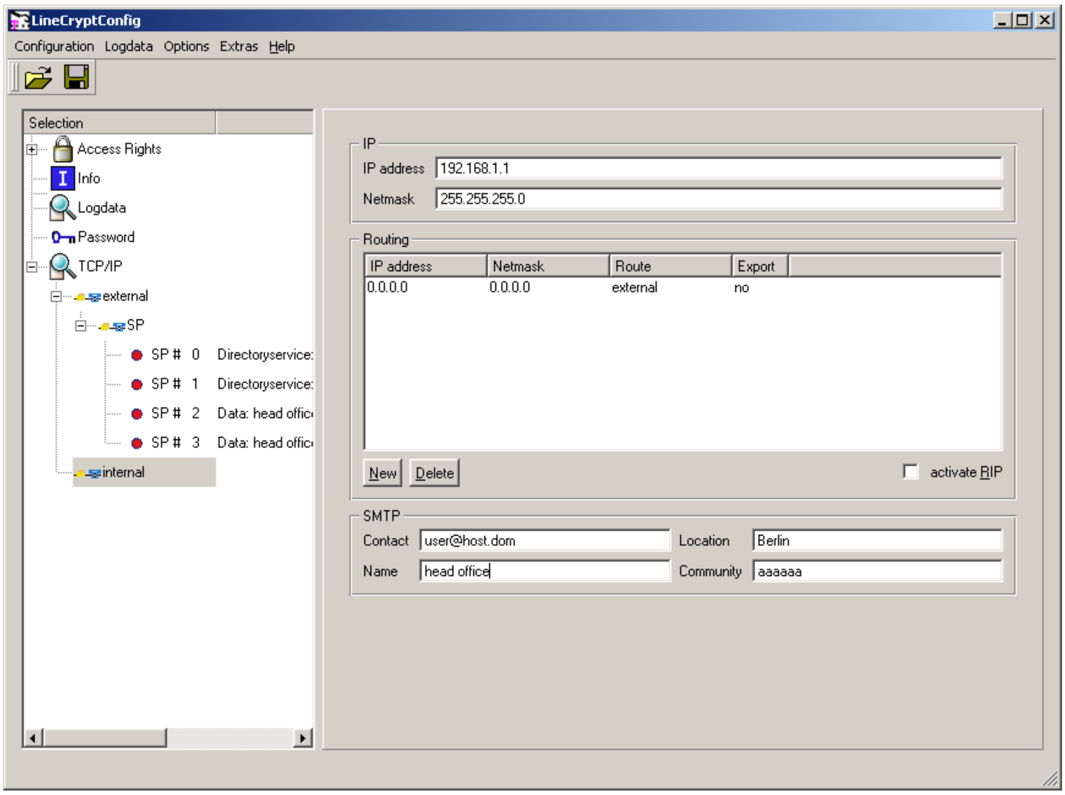


Figure 34: Network diagram

The head office's LineCrypt operates a directory service where the other LineCrypt store their IP address as soon as they have connected with the Internet. The LineCrypt that want to communicate with another dynamically connected LineCrypt will consult this directory service about the IP address with the required certificate number.

Configuration of the LineCrypt at the head office

The configuration of the LineCrypt at the head office is shown first. Both communication between the locations and the directory service function are only successful if the other LineCrypt are configured appropriately.



IP

IP address 192.168.1.1

Netmask 255.255.255.0

Routing

IP address	Netmask	Route	Export
0.0.0.0	0.0.0.0	external	no

□ activate RIP

SMTP

Contact user@host.dom

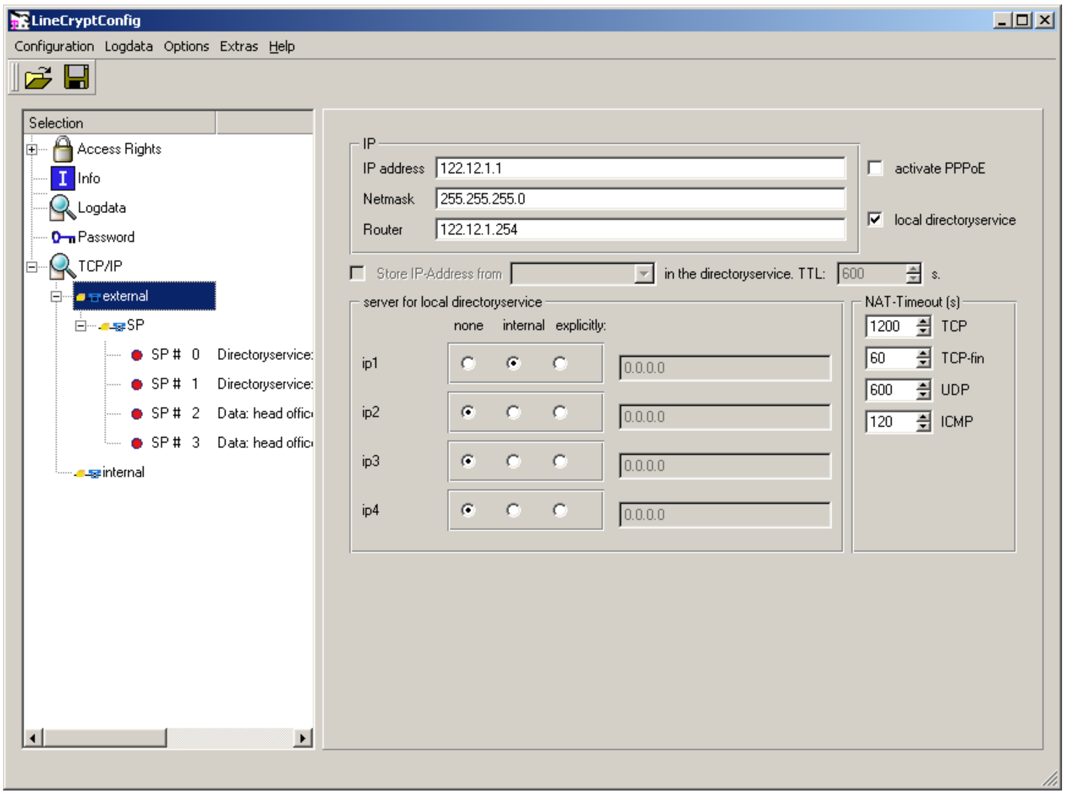
Location Berlin

Name head office

Community aaaaaa

Figure 35: Head office: TCP - internal

In the dialog in figure 35, you need to enter the IP address and the network mask of the local side. To enable communication with other devices, the entry shown must be made in the routing table.



SP # 0 Directoryservice:
SP # 1 Directoryservice:
SP # 2 Data: head offic
SP # 3 Data: head offic

IP
IP address 122.12.1.1
Netmask 255.255.255.0
Router 122.12.1.254

□ activate PPPoE
☑ local directoryservice

□ Store IP-Address from in the directoryservice. TTL: 600 s.

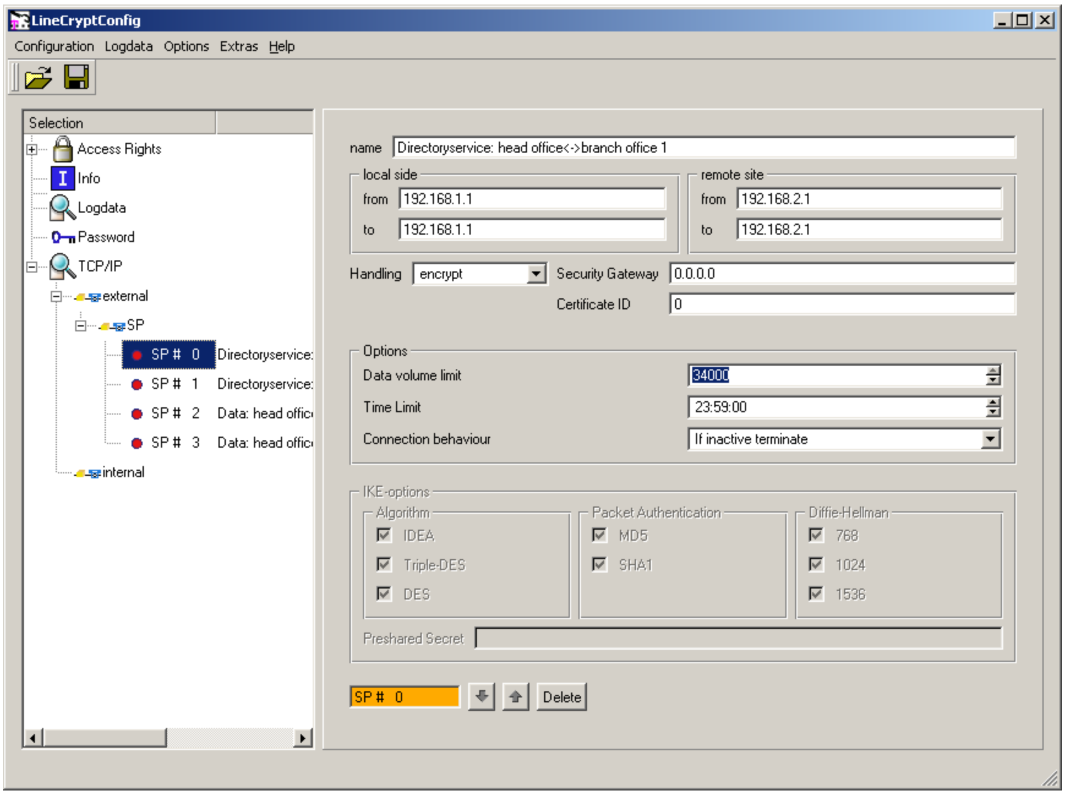
server for local directoryservice

	none	internal	explicitly:	
ip1	○	●	○	0.0.0.0
ip2	●	○	○	0.0.0.0
ip3	●	○	○	0.0.0.0
ip4	●	○	○	0.0.0.0

NAT-Timeout (s)
1200 TCP
60 TCP-fin
600 UDP
120 ICMP

Figure 36: Head office: TCP - external

In the dialog in figure 36, the external side is set according to the network scheme. The directory service is activated and the LineCrypt uses the internal directory service first. The head office consults its own directory service to determine the IP numbers of the branch offices.



name: Directoryservice: head office<->branch office 1

local side: from 192.168.1.1, to 192.168.1.1

remote site: from 192.168.2.1, to 192.168.2.1

Handling: encrypt

Security Gateway: 0.0.0.0

Certificate ID: 0

Options

Data volume limit: 34000

Time Limit: 23:59:00

Connection behaviour: If inactive terminate

IKE-options

Algorithm: ☑ IDEA ☑ Triple-DES ☑ DES

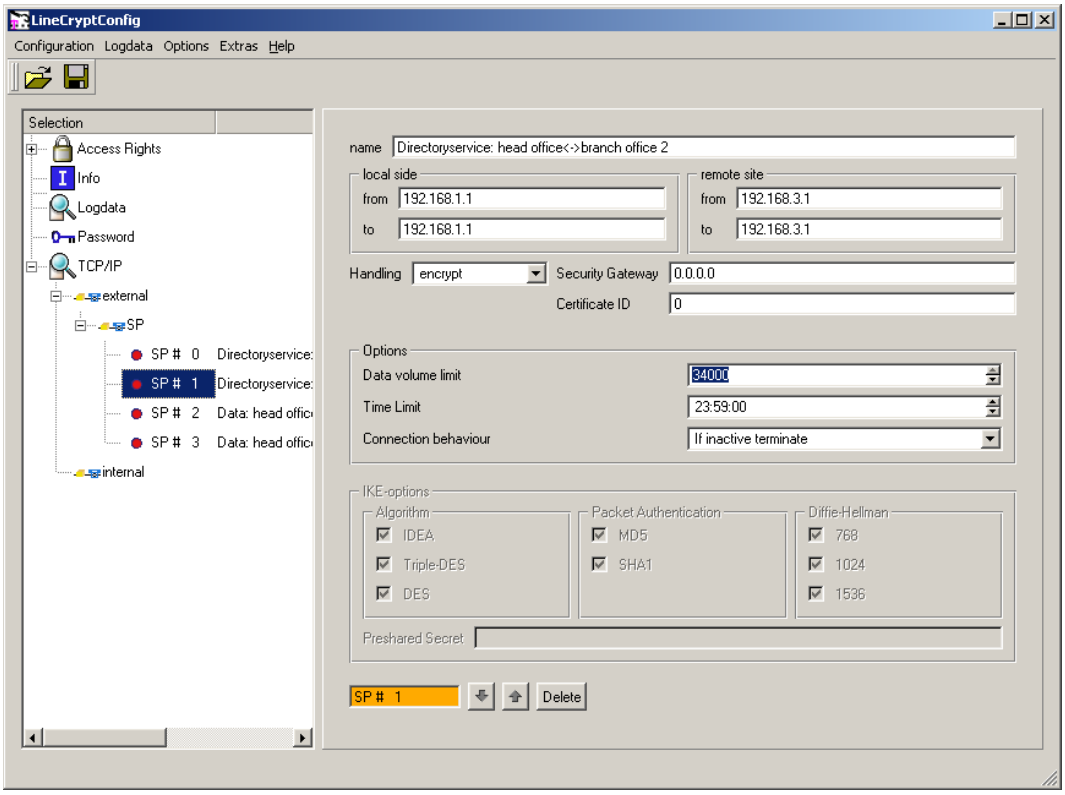
Packet Authentication: ☑ MD5 ☑ SHA1

Diffie-Hellman: ☑ 768 ☑ 1024 ☑ 1536

Preshared Secret:

Figure 37: Head office: Security Policy directory service: branch office 1

The Policy entry in figure 37 allows the LineCrypt at branch office 1 to communicate with the directory service. Since the security gateway's IP address is set to 0.0.0.0 and the certificate number is set to 0, only incoming connections are possible.



name: Directoryservice: head office<->branch office 2

local side
from: 192.168.1.1
to: 192.168.1.1

remote site
from: 192.168.3.1
to: 192.168.3.1

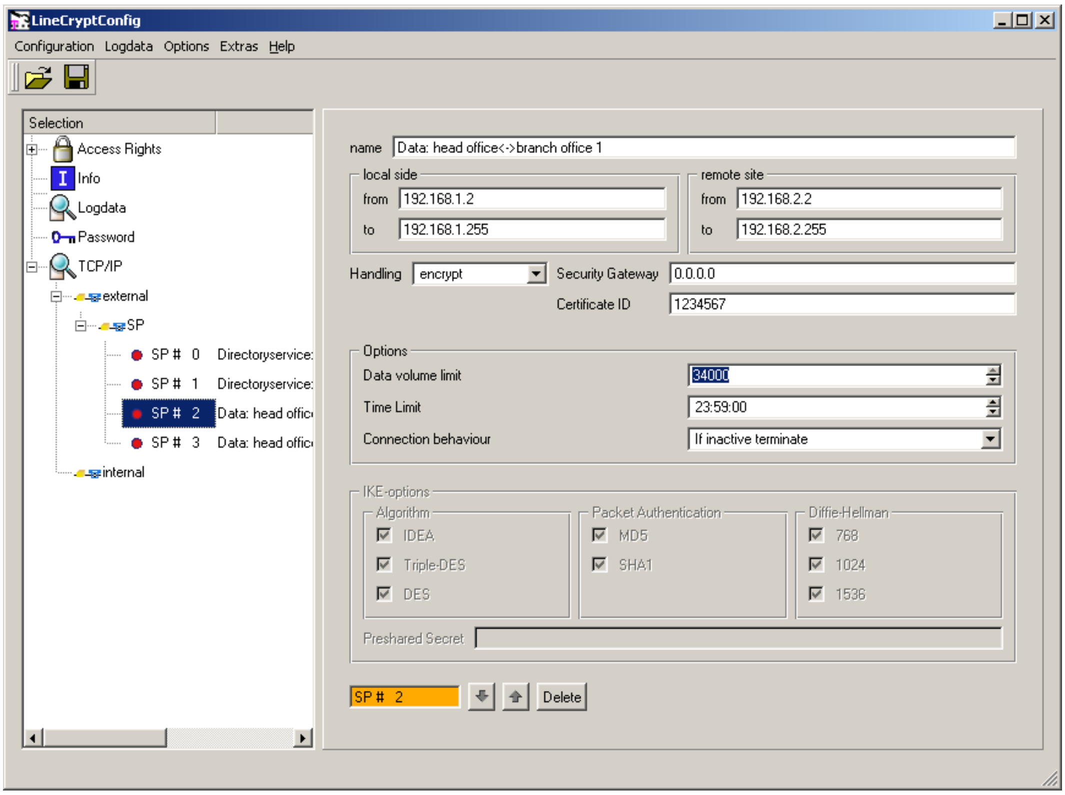
Handling: encrypt
Security Gateway: 0.0.0.0
Certificate ID: 0

Options
Data volume limit: 34000
Time Limit: 23:59:00
Connection behaviour: If inactive terminate

IKE-options
Algorithm: ☑ IDEA ☑ Triple-DES ☑ DES
Packet Authentication: ☑ MD5 ☑ SHA1
Diffie-Hellman: ☑ 768 ☑ 1024 ☑ 1536
Preshared Secret:

Figure 38: Head office: Security Policy: directory service branch office 2

This Policy entry (figure 38) allows the LineCrypt at branch office 2 to communicate with the directory service.



SP # 0 Directoryservice:
SP # 1 Directoryservice:
SP # 2 Data: head offic
SP # 3 Data: head offic

name: Data: head office<->branch office 1

local side
from: 192.168.1.2
to: 192.168.1.255

remote site
from: 192.168.2.2
to: 192.168.2.255

Handling: encrypt
Security Gateway: 0.0.0.0
Certificate ID: 1234567

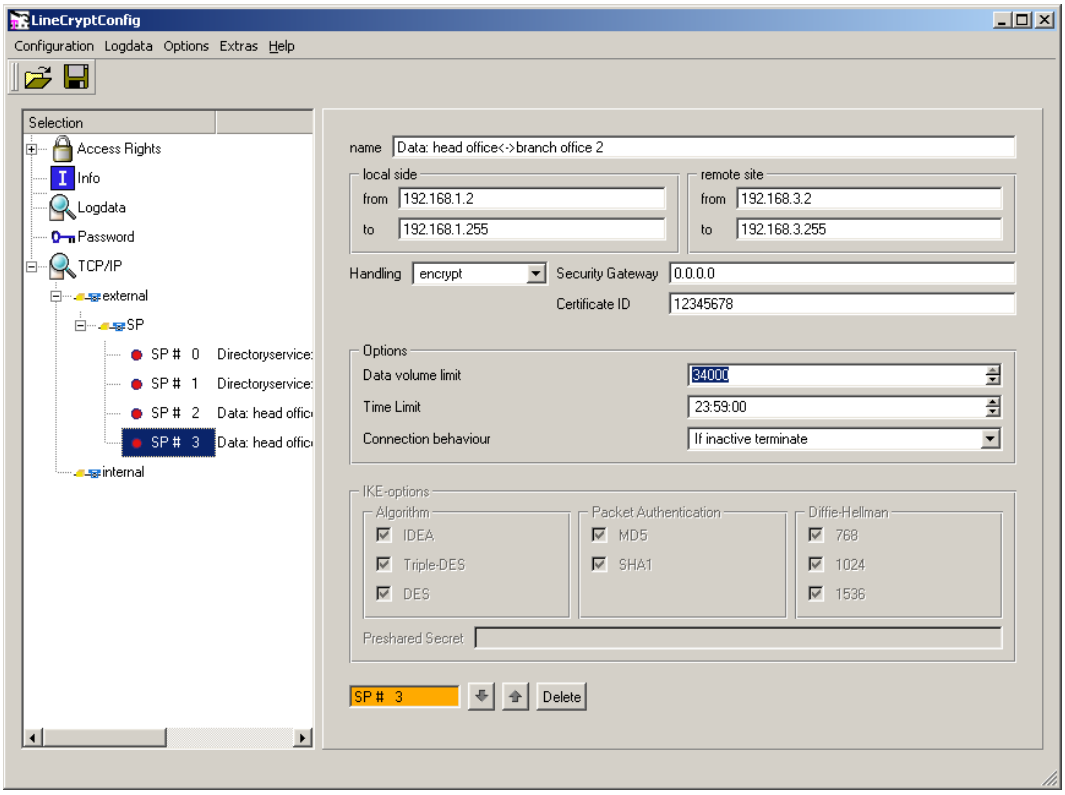
Options
Data volume limit: 34000
Time Limit: 23:59:00
Connection behaviour: If inactive terminate

IKE-options
Algorithm: ☑ IDEA ☑ Triple-DES ☑ DES
Packet Authentication: ☑ MD5 ☑ SHA1
Diffie-Hellman: ☑ 768 ☑ 1024 ☑ 1536
Preshared Secret:

SP # 2

Figure 39: Head office: Security Policy: branch office 1

Figure 39 shows a Policy entry that allows the LineCrypt at branch office 1 to communicate with the head office. In order that the head office may also reach branch office 1 at the respective IP address, you need to specify the certificate number of the chip card in the LineCrypt at branch office 1.



name: Data: head office<->branch office 2

local side
from: 192.168.1.2
to: 192.168.1.255

remote site
from: 192.168.3.2
to: 192.168.3.255

Handling: encrypt
Security Gateway: 0.0.0.0
Certificate ID: 12345678

Options
Data volume limit: 34000
Time Limit: 23:59:00
Connection behaviour: If inactive terminate

IKE-options

Algorithm
☑ IDEA
☑ Triple-DES
☑ DES

Packet Authentication
☑ MD5
☑ SHA1

Diffie-Hellman
☑ 768
☑ 1024
☑ 1536

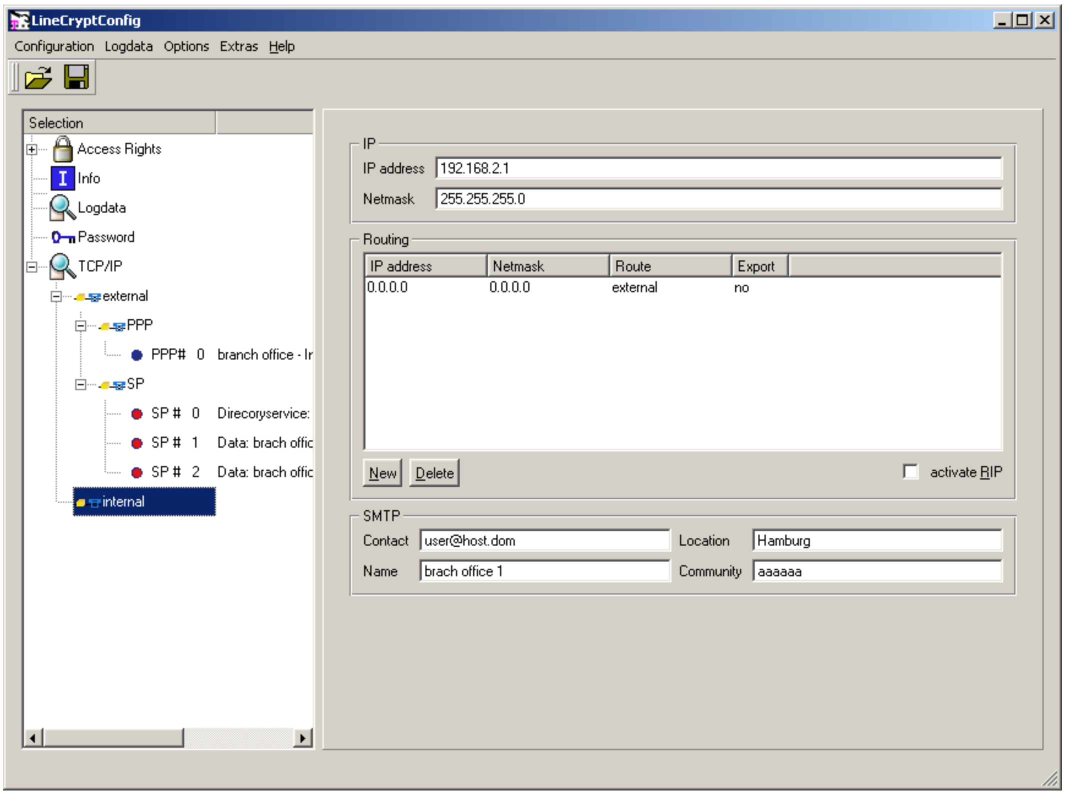
Preshared Secret:

SP # 3

Figure 40: Head office: Security Policy: branch office 2

The Policy entry in figure 40 allows the LineCrypt at branch office 2 to communicate with the head office. In order that the head office may also reach branch office 2 at the respective IP address, you need to specify the certificate number of the chip card in the LineCrypt at branch office 2.

Configuration of the LineCrypt at branch office 1



IP

IP address 192.168.2.1

Netmask 255.255.255.0

Routing

IP address	Netmask	Route	Export
0.0.0.0	0.0.0.0	external	no

□ activate RIP

SMTP

Contact user@host.dom

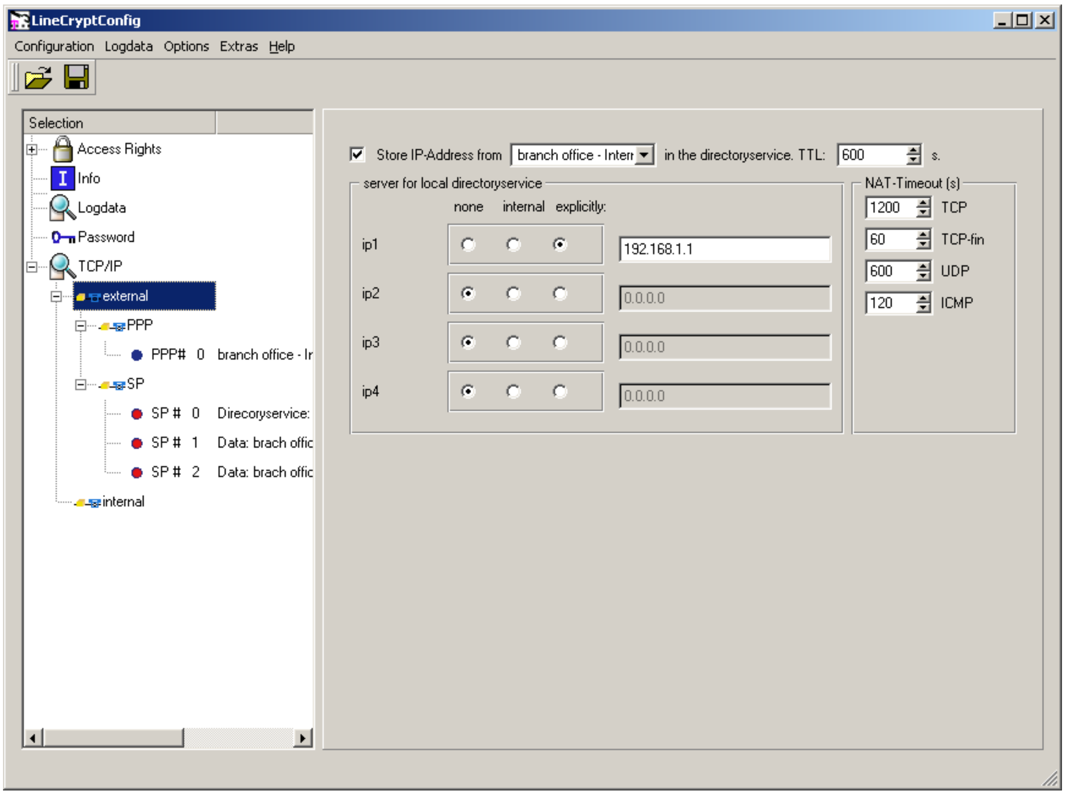
Location Hamburg

Name brach office 1

Community aaaaaa

Figure 41: Branch office 1: TCP/IP -internal

In the dialog in figure 41, you need to enter the IP address and the network mask of the local side. To enable communication with other devices, the entry shown in the routing table must be made.



- Access Rights
- Info
- Logdata
- Password
- TCP/IP
  - external
    - PPP
      - PPP# 0 branch office - Ir
    - SP
      - SP # 0 Direcoryservice:
      - SP # 1 Data: brach offic
      - SP # 2 Data: brach offic
  - internal

☑ Store IP-Address from branch office - Intern in the directoryservice. TTL: 600 s.

server for local directoryservice

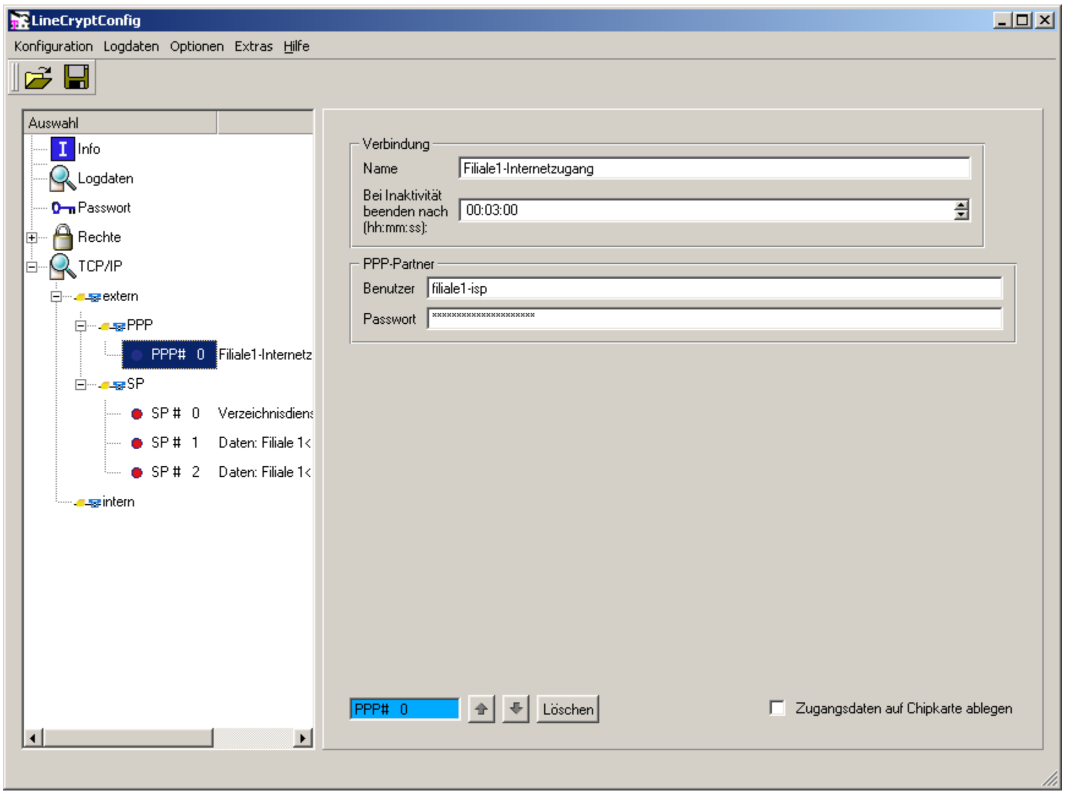
	none	internal	explicitly:	
ip1	○	○	●	192.168.1.1
ip2	●	○	○	0.0.0.0
ip3	●	○	○	0.0.0.0
ip4	●	○	○	0.0.0.0

NAT-Timeout (s)

1200	TCP
60	TCP-fin
600	UDP
120	ICMP

Figure 42: branch office 1: TCP/IP -external

In this dialog (figure 42), the external side is set as a PPP connection according to the network scheme. The LineCrypt uses the head office’s directory service. That is why the red IP address of the head office’s LineCrypt is used as the first directory service server.



Verbindung

Name: Filiale1-Internetzugang

Bei Inaktivität beenden nach (hh:mm:ss): 00:03:00

PPP-Partner

Benutzer: filiale1-isp

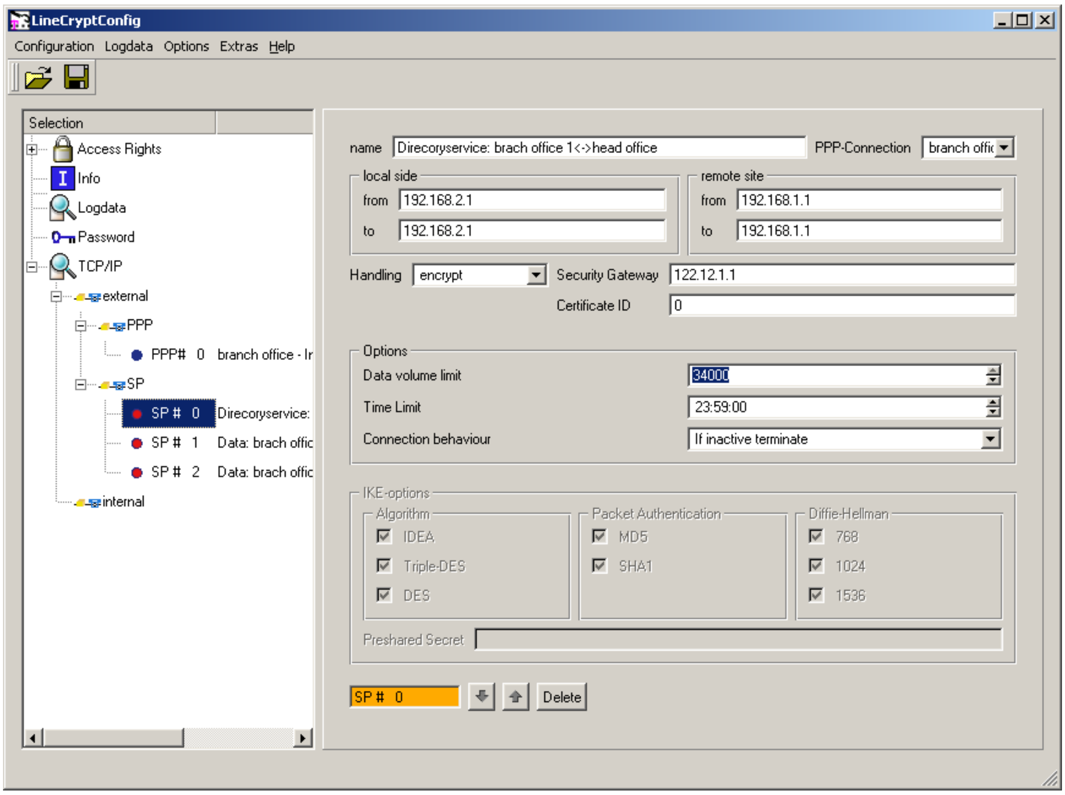
Passwort: ********************

□ Zugangsdaten auf Chipkarte ablegen

Figure 43: branch office 1: PPP

The dialog in figure 43 describes the Internet access of branch office 1.

The setting of the hold time to three minutes means that the LineCrypt can terminate the PPP connection before the repeated storage of the IP address as soon as no data is transported.



PPP# 0 branch office - Ir

SP # 0 Direcoryservice:

SP # 1 Data: brach offic

SP # 2 Data: brach offic

name: Direcoryservice: brach office 1<->head office

PPP-Connection: branch offic

local side
from: 192.168.2.1
to: 192.168.2.1

remote site
from: 192.168.1.1
to: 192.168.1.1

Handling: encrypt

Security Gateway: 122.12.1.1

Certificate ID: 0

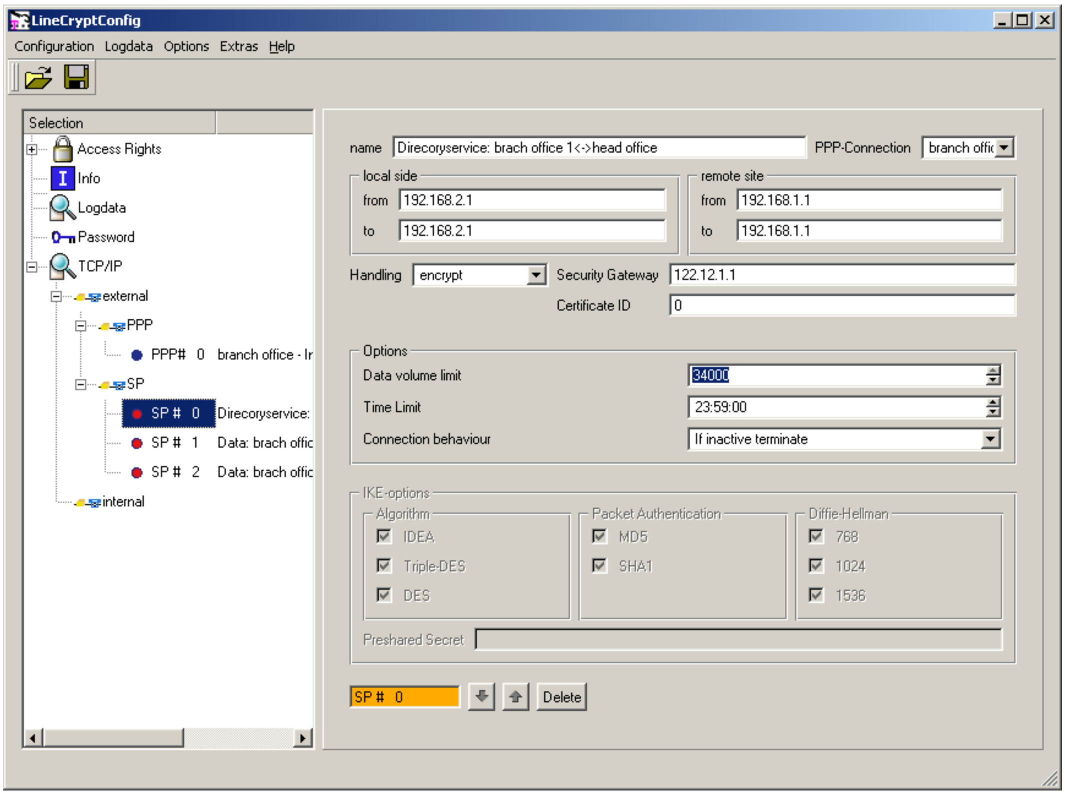
Options
Data volume limit: 34000
Time Limit: 23:59:00
Connection behaviour: If inactive terminate

IKE-options
Algorithm: ☑ IDEA ☑ Triple-DES ☑ DES
Packet Authentication: ☑ MD5 ☑ SHA1
Diffie-Hellman: ☑ 768 ☑ 1024 ☑ 1536
Preshared Secret:

SP # 0

Figure 44: branch office 1: Security Policy: directory service

The Policy entry in figure 44 allows the LineCrypt at branch office 1 to communicate with the directory service.



name: Direcoryservice: brach office 1<->head office
PPP-Connection: branch offic

local side
from: 192.168.2.1
to: 192.168.2.1

remote site
from: 192.168.1.1
to: 192.168.1.1

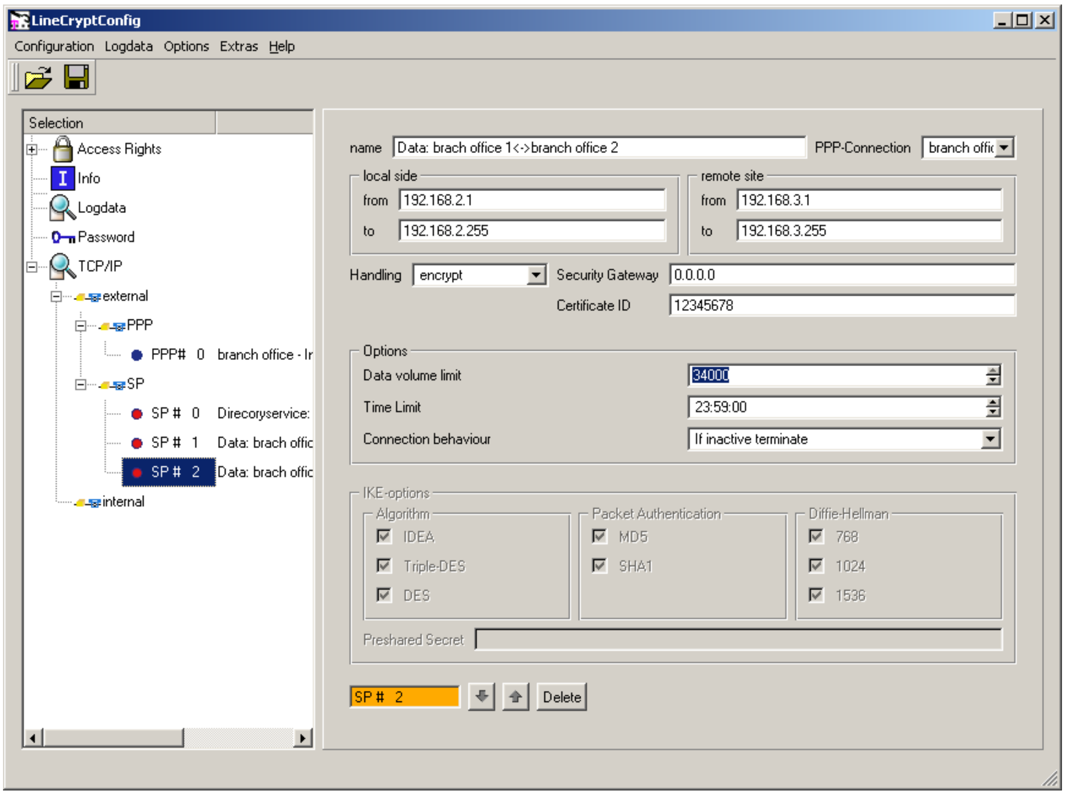
Handling: encrypt
Security Gateway: 122.12.1.1
Certificate ID: 0

Options
Data volume limit: 34000
Time Limit: 23:59:00
Connection behaviour: If inactive terminate

IKE-options
Algorithm: ☑ IDEA ☑ Triple-DES ☑ DES
Packet Authentication: ☑ MD5 ☑ SHA1
Diffie-Hellman: ☑ 768 ☑ 1024 ☑ 1536
Preshared Secret:

Figure 45: branch office 1: Security Policy: head office

The Policy entry in figure 45 allows the LineCrypt at branch office 1 to communicate with the head office. Since the central LineCrypt can be reached with a permanent IP address, no certificate number is necessary for communication.



name: Data: brach office 1<->branch office 2
PPP-Connection: branch offic

local side
from: 192.168.2.1
to: 192.168.2.255

remote site
from: 192.168.3.1
to: 192.168.3.255

Handling: encrypt
Security Gateway: 0.0.0.0
Certificate ID: 12345678

Options
Data volume limit: 34000
Time Limit: 23:59:00
Connection behaviour: If inactive terminate

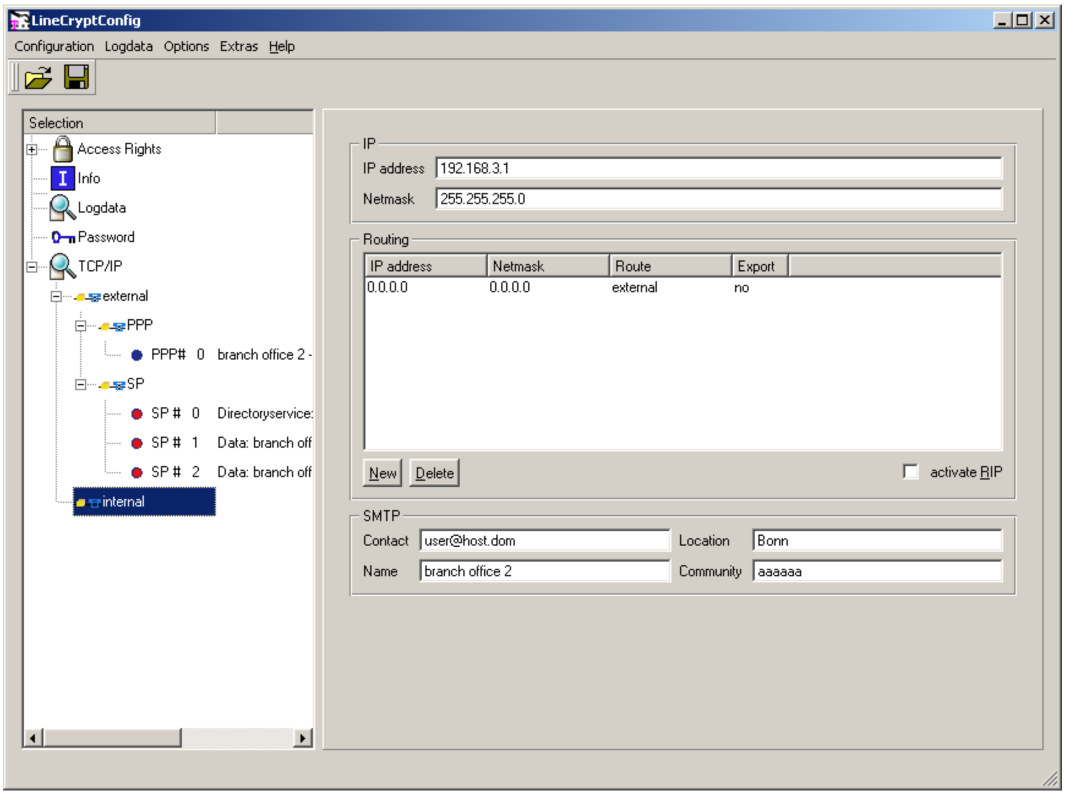
IKE-options
Algorithm: ☑ IDEA ☑ Triple-DES ☑ DES
Packet Authentication: ☑ MD5 ☑ SHA1
Diffie-Hellman: ☑ 768 ☑ 1024 ☑ 1536
Preshared Secret:

SP # 2

Figure 46: branch office 1: Security Policy:-branch office 2

This Policy entry allows the LineCrypt at branch office 1 to communicate with branch office 2. For this, the certificate number of branch office 2 is required.

Configuration of the LineCrypt at branch office 2



IP

IP address 192.168.3.1

Netmask 255.255.255.0

Routing

IP address	Netmask	Route	Export
0.0.0.0	0.0.0.0	external	no

□ activate RIP

SMTP

Contact user@host.dom

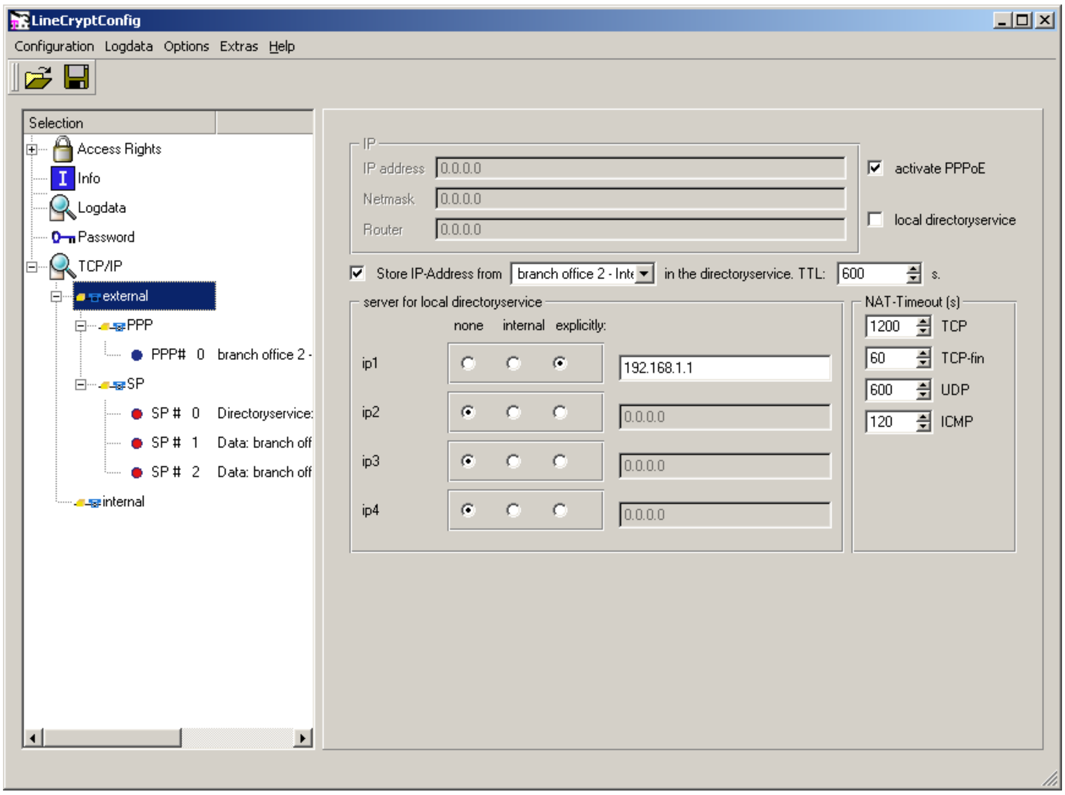
Location Bonn

Name branch office 2

Community aaaaaa

Figure 47: Branch office 2: TCP/IP - internal

In this dialog, you need to enter the IP address and the network mask of the local side. To enable communication with other devices, the entry shown in the routing table must be made.



IP
IP address 0.0.0.0
Netmask 0.0.0.0
Router 0.0.0.0

☑ activate PPPoE

□ local directoryservice

☑ Store IP-Address from branch office 2 - Inte in the directoryservice. TTL: 600 s.

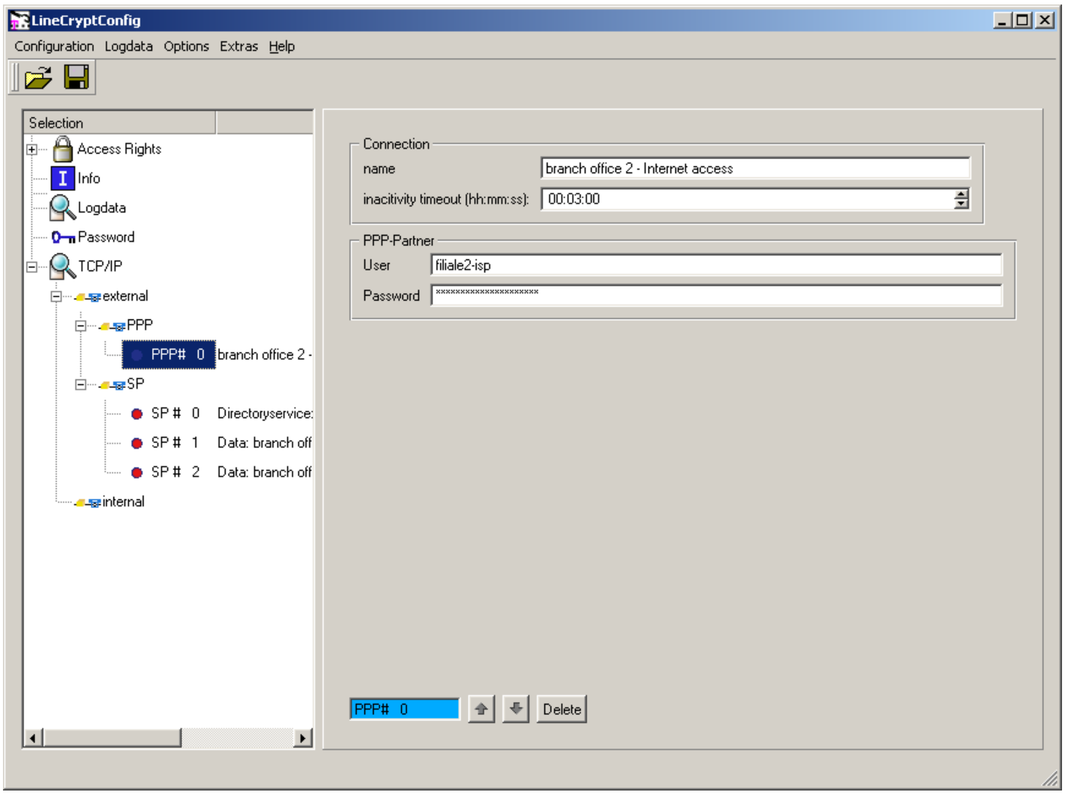
server for local directoryservice

	none	internal	explicitly:	
ip1	○	○	●	192.168.1.1
ip2	●	○	○	0.0.0.0
ip3	●	○	○	0.0.0.0
ip4	●	○	○	0.0.0.0

NAT-Timeout (s)
1200 TCP
60 TCP-fin
600 UDP
120 ICMP

Figure 48: Branch office 2: TCP/IP - external

In the dialog in figure 48, the external side is set as a PPP connection according to the network scheme. The directory service is not activated, and the LineCrypt uses the internal IP address of the LineCrypt at the head office as the first directory service server.



Connection

name: branch office 2 - Internet access

inacitivity timeout (hh:mm:ss): 00:03:00

PPP-Partner

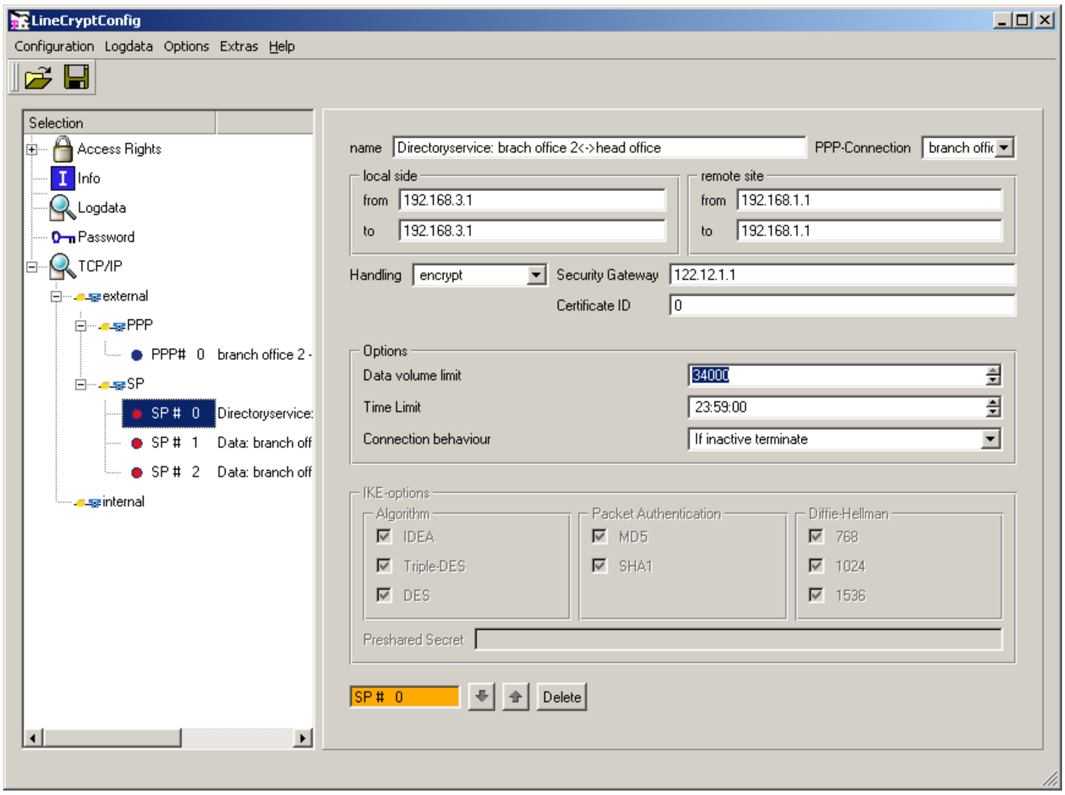
User: filiale2-isp

Password: ********************

Figure 49: Branch office 2: PPP

Figure 49 describes the Internet access of branch office 2.

The setting of the hold time to three minutes means that the LineCrypt can terminate the PPP connection before the repeated storage of the IP address as soon as no data is transported.



name: Directoryservice: brach office 2<->head office
PPP-Connection: branch offic

local side
from: 192.168.3.1
to: 192.168.3.1

remote site
from: 192.168.1.1
to: 192.168.1.1

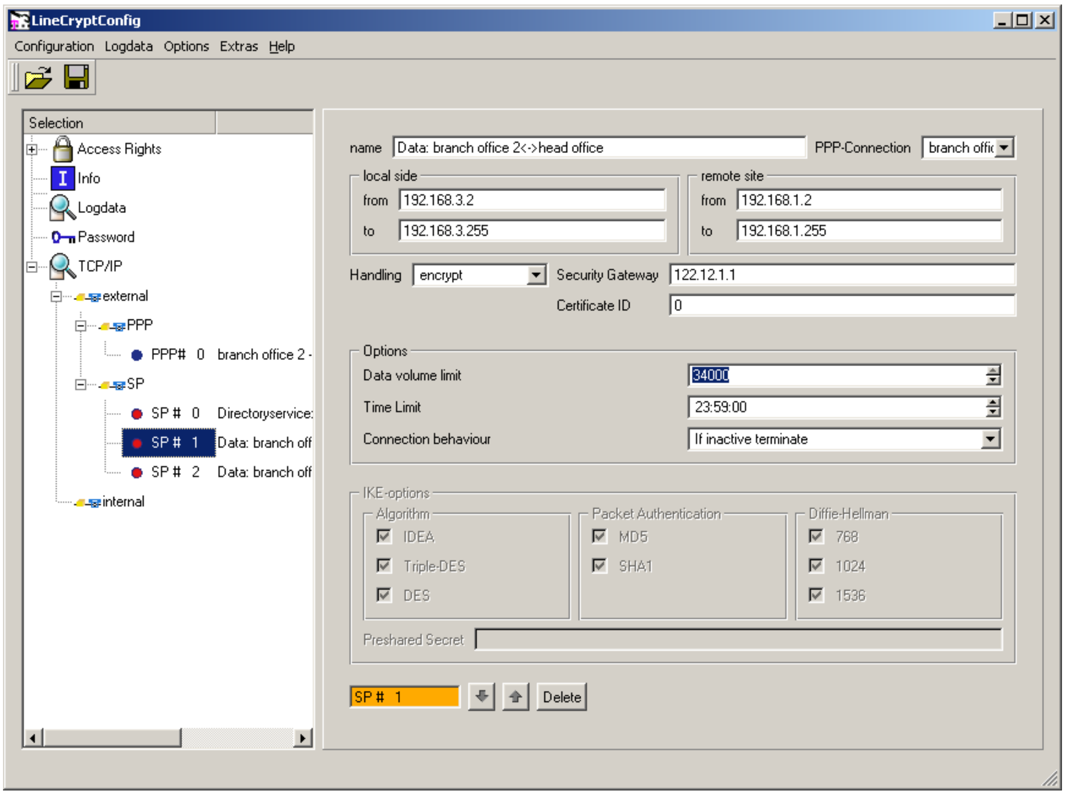
Handling: encrypt
Security Gateway: 122.12.1.1
Certificate ID: 0

Options
Data volume limit: 34000
Time Limit: 23:59:00
Connection behaviour: If inactive terminate

IKE-options
Algorithm: ☑ IDEA ☑ Triple-DES ☑ DES
Packet Authentication: ☑ MD5 ☑ SHA1
Diffie-Hellman: ☑ 768 ☑ 1024 ☑ 1536
Preshared Secret:

Figure 50: Branch office 2: security policy: directory service

The Policy entry in figure 50 allows the LineCrypt at branch office 2 to communicate with the directory service.



name: Data: branch office 2<->head office
PPP-Connection: branch offic

local side
from: 192.168.3.2
to: 192.168.3.255

remote site
from: 192.168.1.2
to: 192.168.1.255

Handling: encrypt
Security Gateway: 122.12.1.1
Certificate ID: 0

Options
Data volume limit: 34000
Time Limit: 23:59:00
Connection behaviour: If inactive terminate

IKE-options

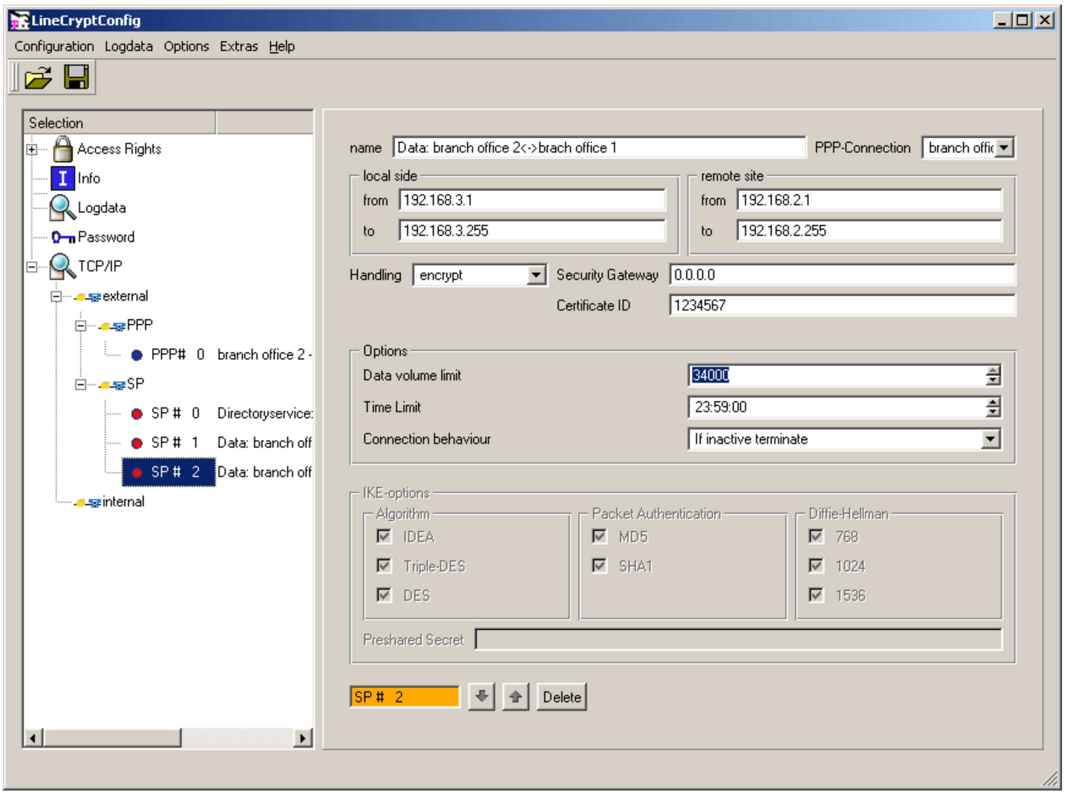
Algorithm	Packet Authentication	Diffie-Hellman
☑ IDEA	☑ MD5	☑ 768
☑ Triple-DES	☑ SHA1	☑ 1024
☑ DES		☑ 1536

Preshared Secret:

SP # 1

Figure 51: Branch office 2: Security Policy: head office

The Policy entry in figure 51 allows the LineCrypt at branch office 1 to communicate with the head office. The central LineCrypt can be reached with a permanent IP address, so no certificate number is necessary for communication.



name: Data: branch office 2<->brach office 1
PPP-Connection: branch offic

local side
from: 192.168.3.1
to: 192.168.3.255

remote site
from: 192.168.2.1
to: 192.168.2.255

Handling: encrypt
Security Gateway: 0.0.0.0
Certificate ID: 1234567

Options
Data volume limit: 34000
Time Limit: 23:59:00
Connection behaviour: If inactive terminate

IKE-options
Algorithm: ☑ IDEA ☑ Triple-DES ☑ DES
Packet Authentication: ☑ MD5 ☑ SHA1
Diffie-Hellman: ☑ 768 ☑ 1024 ☑ 1536
Preshared Secret:

SP # 2

Figure 52: Branch office 2: Security Policy: branch office 1

This Policy entry 52 allows the LineCrypt at branch office 2 to communicate directly with branch office 1. For this, the certificate number of branch office 1 is required.

I, IT, I+

LineCrypt I+ in point to multipoint mode : Example

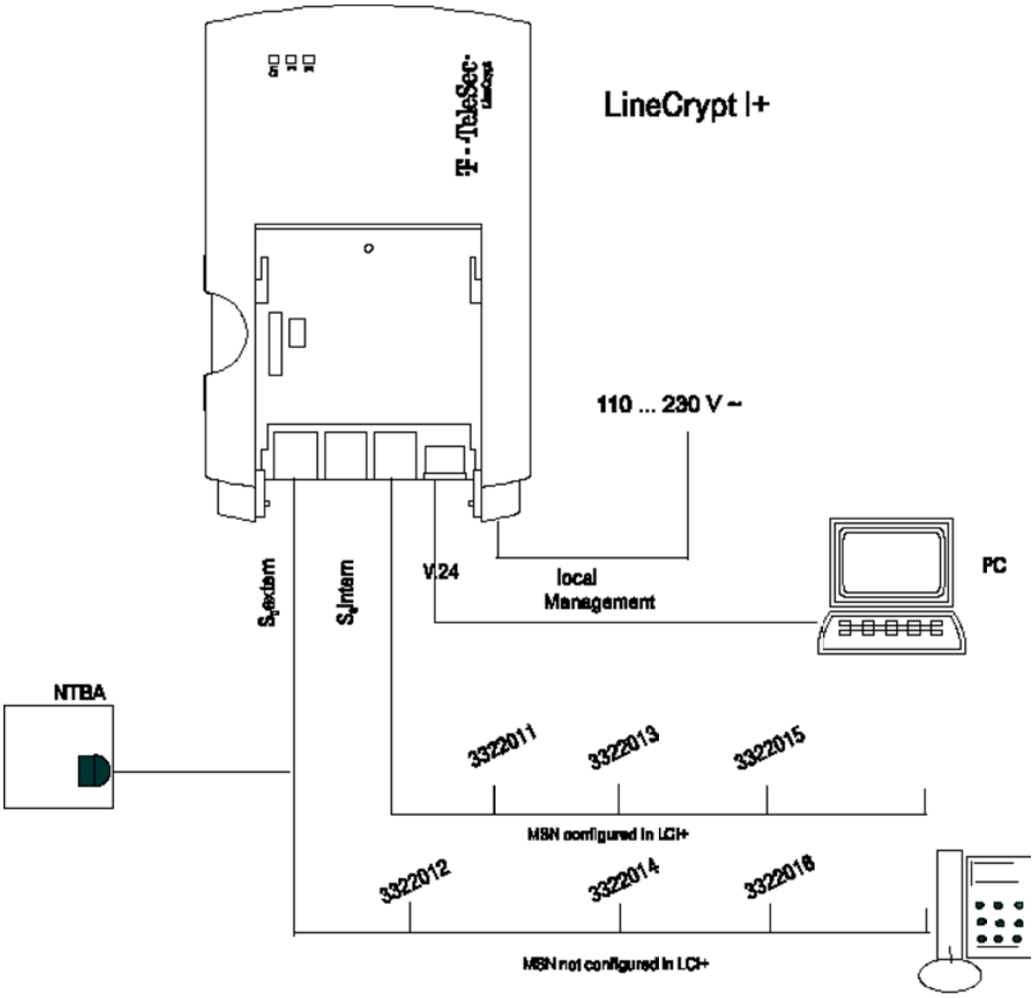
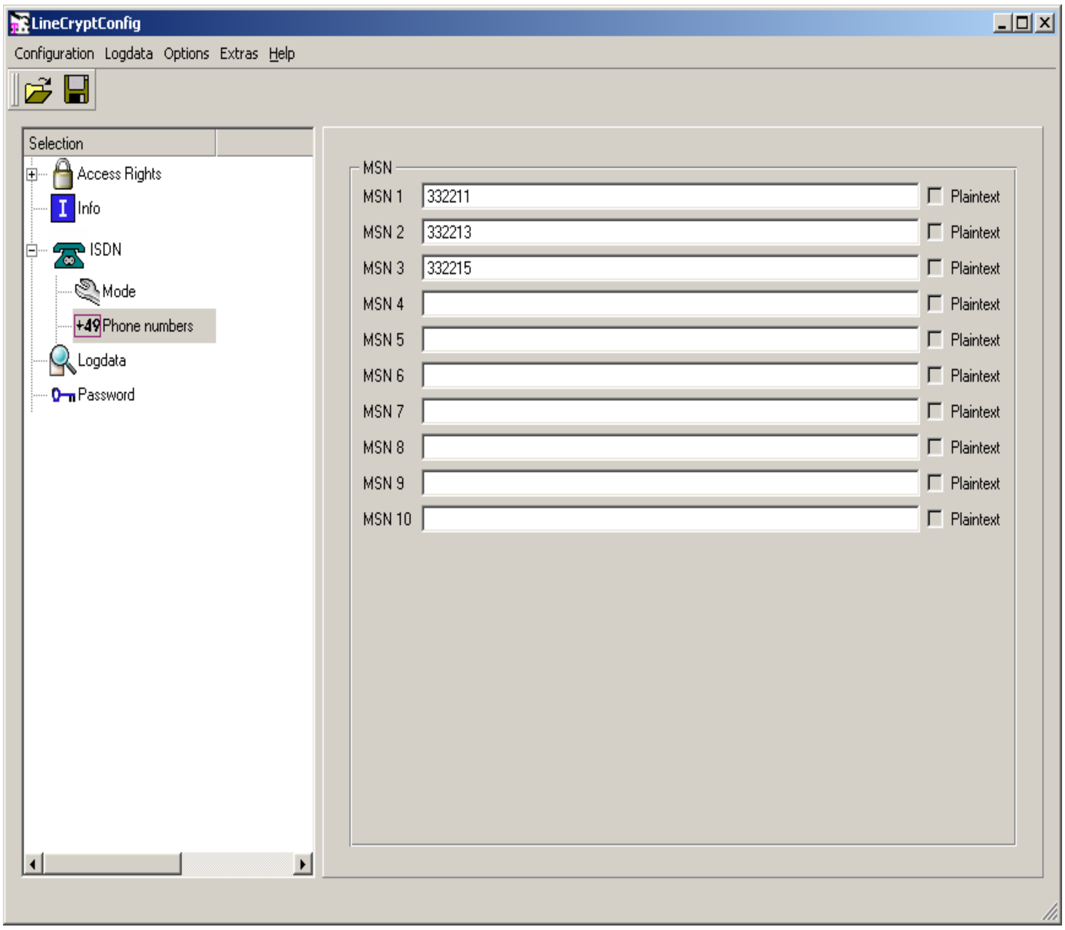


Figure 53: LineCrypt I+ in point to multipoint mode

In the configuration shown, incoming calls with the call numbers 3322011, 3322013, and 3322015, or calls initiated by devices on the S_0 internal bus of the LineCrypt I+ are protected by the LineCrypt I+. Incoming calls (except for those with the call numbers 3322011, 3322013, and 3322015) can be accepted by devices connected in parallel to the LineCrypt I+. These connections, like the outgoing connections of these devices, are then not secured by the LineCrypt I+.



MSN

MSN 1	332211	☐ Plaintext
MSN 2	332213	☐ Plaintext
MSN 3	332215	☐ Plaintext
MSN 4		☐ Plaintext
MSN 5		☐ Plaintext
MSN 6		☐ Plaintext
MSN 7		☐ Plaintext
MSN 8		☐ Plaintext
MSN 9		☐ Plaintext
MSN 10		☐ Plaintext

Figure 54: MSN-Configuration

Factory setting

Your LineCrypt comes with some settings that have already been prepared for you. To restore the LineCrypt to its configuration as when it left the factory, select the ***Factory Settings*** **menu command on the** ***Configuration*** menu. The current configuration is overwritten.

LineCrypt GSM

The following settings are pre-selected at the factory:

Authorizations	White list: deactivated Black list: empty CUG list: empty System administrator list: empty

LineCrypt I, IT

The following settings are pre-selected at the factory:

ISDN	IDSN access type: multi-terminal connection, no MSN
Authorizations	White list: deactivated Black list: empty CUG list: empty System administrator list: empty
Password	No password protection

LineCrypt I+

The following settings are pre-selected at the factory:

ISDN	IDSN access type: multi-terminal connection, no MSN Mode 3: encrypted and plaintext connections, incoming calls with the service attribute ”voice” are not encrypted, outgoing calls with prefix number: 0: ISDN encrypted 1: plaintext 4: modem encrypted 7: GSM encrypted
Authorizations	White list: deactivated Black list: empty CUG list: empty System administrator list: empty
Password	No password protection

Before you can establish connections to other devices with your LineCrypt L, you need to configure your device accordingly using the LineCryptConfig software. This includes:

- The TCP/IP settings of the network interface
- Directory service settings
- The configuration of authorized and unauthorized partner certificates

You should adjust these settings to your specific requirements. The following settings are pre-selected at the factory:

TCP/IP	IP address of the red side: 0.0.0.0 Network mask of the red side: 0.0.0.0 IP address of the black side: 0.0.0.0 Network mask of the black side: 0.0.0.0
SP	No Security Policies
Directory service	No servers; storage of the current IP address deactivated
Authorizations	White list: deactivated Black list: empty CUG list: empty System administrator list: empty
Password	No password protection

LineCrypt L100

Before you can establish connections to other devices with your LineCrypt L100, you need to configure your device accordingly using the LineCryptConfig software. This includes:

- The TCP/IP settings of the network interface
- The configuration of authorized and unauthorized partner certificates

You should adjust these settings to your specific requirements. The following settings are pre-selected at the factory:

TCP/IP	IP address of the red side: 0.0.0.0 Network mask of the red side: 0.0.0.0 IP address of the black side: 0.0.0.0 Network mask of the black side: 0.0.0.0
SP	No Security Policies
Authorizations	White list: deactivated Black list: empty CUG list: empty System administrator list: empty
Password	No password protection

LineCrypt DSL

Before you can establish connections to other devices with your LineCrypt DSL, you need to configure your device accordingly using the LineCryptConfig software. This includes:

- The TCP/IP settings of the network interface
- PPP settings
- Directory service settings
- The configuration of authorized and unauthorized partner certificates

You should adjust these settings to your specific requirements.

The following settings are pre-selected at the factory:

TCP/IP	IP address of the red side: 192.168.0.1 Network mask of the red side: 255.255.0.0
SP	No Security Policies
PPP	No PPP connection
Directory service	No servers; storage of the current IP address deactivated
Authorizations	White list: deactivated Black list: empty CUG list: empty System administrator list: empty
Password	No password protection

LineCrypt SOHO

Before you can establish connections to other devices with your LineCrypt SOHO, you need to configure your device accordingly using the LineCryptConfig software. This includes:

- The TCP/IP settings of the network interface
- PPP settings
- Directory service settings
- Security Policy settings for the authorized IP networks
- The configuration of authorized and unauthorized partner certificates

You should adjust these settings to your specific requirements.

The following settings are pre-selected at the factory:

ISDN	IDSN access type: multi-terminal connection, no MSN
TCP/IP	IP address of the red side: 192.168.0.1 Network mask of the red side: 255.255.0.0
PPP	No PPP connection
SP	No Security Policies
Directory service	No servers, deactivated, storage of the current IP address deactivated
Authorizations	White list: deactivated Black list: empty CUG list: empty System administrator list: empty
Password	No password protection

Standard values for a Security Policy rule

The following settings are pre-selected at the factory:

Name:	ips N
Local side	From: 0.0.0.0 To: 0.0.0.0
Remote side	From: 0.0.0.0 To: 0.0.0.0
Security gateway	0.0.0.0
Certificate number	0
Action	Encrypt
Volume restriction	34000MB
Time restriction	23:59:00 (HH:MM:SS)
Connection behavior	If inactive terminate

Glossary

A

alias list

List of names and certificate IDs of the administered users.

authentication

Proof and verification of identity (through proof of being in possession of a secret, which the communication partner can check).

B

black list

List of certificate IDs of the users who are excluded from communication via the LineCrypt.

C

CA (Certification Authority)

The certificates exchanged during →authentication are signed by the CA as a trusted authority. The check is carried out with the CA’s public key (see also →Trust Center).

CA lists (CA = Certification Authority)

Trust Centers sign certificates with secret RSA keys. The CA lists contain the relevant public keys. The LineCrypt use the CA list published by Deutsche Telekom’s Trust Center to check that the certificates are valid.

certificate

A certificate is an electronic identifier that contains a digital signature created by a certification center (→CA) with a private key. In addition to the digital signature, a certificate contains the name of the issuer and the owner’s identity details. The authenticity of the keys is checked by the recipients. The format for the digital certificates used by the LineCrypt is defined in the ITU recommendation X.509v3.

certificate ID, certificate number

Number in a certificate that uniquely identifies it.

CHAP (Challenge Authentication Protocol)

Optional authentication protocol for the →PPP connection setup. Unlike for →PAP, the user name and password are transferred encrypted.

Company Card

→TCOS chip card that, unlike the →NetKey Card, contains information about a closed user group. Company Cards can be obtained from Deutsche Telekom if required.

configuration

The setting of parameters and the changing of preset values; also the status of the parameter settings.

connection scheme

Schematic diagram of possible connection variants.

contractual use

Restricted area of use and application, declared and explained by the manufacturer.

D

DES (Data Encryption Standard)

Widely used symmetrical encryption method with a key length of 64 bits (56 bits effective). See also →Triple DES.

E

EMC - electromagnetic compatibility

The ability of an appliance, installation, or system to function satisfactorily in the electromagnetic environment without introducing intolerable electromagnetic interference to any appliance or system in that environment (quoted from the EC EMC guideline, article 1, clause 4).

Ethernet

The most widely used →LAN standard (Local Area Network). Supports data rates of up to 10 Mbps (10Base-T) or 100 Mbps (100Base-T).

H

half-duplex operation

Data transmission method whereby terminal stations can send and receive. The half-duplex method allows two-way alternate use of a transmission line. At the interfaces, it is only possible to send or receive at a time.

HDLC (High Level Data Link Control)

Bit-oriented transmission procedure within level 2 of the ISO/OSI reference model, and component of the X.25 recommendation. HDLC is responsible for data link services, and adds synchronizing signals to the data stream.

I

ICMP (Internet Control Message Protocol)

The ICMP is a protocol for transferring status information and error messages of the IP, TCP, and UDP protocols between IP network nodes. Gateways and hosts in particular use ICMP to return reports about problems with datagrams to the original source.

IDEA (International Data Encryption Algorithm)

Encryption method with a128-bit key length; LineCrypt uses IDEA to encrypt the user data.

IKE (Internet Key Exchange)

IKE is used within the framework of →IPSec to transfer and negotiate information necessary for the encryption (algorithm, key, key life, etc.).

IP (Internet Protocol)

The task of the Internet Protocol (IP, layer 3) is to transport data packets from a sender to a receiver across several networks. The transmission is packet-oriented, connectionless, and non-guaranteed. The data packets (also called datagrams) are transported by the IP as independent data packets (even in the case of identical senders and receivers). IP guarantees neither observance of a particular sequence nor delivery to the receiver (that is, datagrams can be lost on account of network overload, for example). There are no receive acknowledgements on the IP layer.

IP network

Network based on the Internet Protocol. Every device in the network is addressed through an IP number.

IPSec

IPSec is a standardization proposal of the IEFT, in which methods and protocols are defined for cross-manufacturer, secure and protected data exchange using the IP protocol.

IP tunnel

A connection between two subnetworks, which conceals the precise addresses of the communication partners. At the start of the tunnel, all data packets receive an additional header that refers to the tunnel end. Here the external frame is removed and the original data packet is forwarded to its actual receiver.

ISDN - Integrated Services Digital Network

Integrated telecommunications services like telephone, fax, and data communications in a network.

ISDN basic access

ISDN access comprising two speech/data channels (B channels) each of 64 KB/s and a control channel (D channel) at 16 KB/s. The two B channels can be used independently of one another for every service offered in the ISDN.

L

LAN (Local Area Network)

A spatially restricted network. The most widely used LAN standard is →Ethernet.

LED – light-emitting diode

For displaying the operational status of the device and of the connection.

LineCrypt Company Card

Special chip cards with information on closed user groups. Can be obtained from Deutsche Telekom if required.

log file

Records the processes in the LineCrypt.

local management

Configuring the LineCrypt using a PC and the LineCryptConfig software via the serial interface.

M

multi-terminal connection

ISDN basic access with three call numbers and two channels as standard for direct connection of the telecommunications terminals at the NTBA.

MD5 (Message Digest 5)

Hash algorithm that calculates a 128-bit-long digital signature from a data stream of any length. MD5 is used by →IKE for packet authentication.

MSN - Multiple Subscriber Number

Up to ten Multiple Subscriber Numbers can be allocated to a multi-terminal connection. The subscriber numbers are used for targeted addressing of the connected terminals. Several Multiple Subscriber Numbers can be allocated to ISDN terminals.

N

NAT

Abbreviation for "Network Address Translation"; method of translating (normally private) IP addresses of a network to other (normally public) IP addresses of a different network. NAT thus enables several PCs in a LAN to use the IP address of the Internet access router for Internet access, and conceals the LAN behind the router's IP address registered on the Internet.

NetKey Card

Smart card with → TCOS operating system. The private asymmetrical key and a certificate for →authentication published by the Deutsche Telekom →Trust Center are stored on the →NetKey Card.

NTBA - Network Termination Basic Access

Network termination device – small box for converting a two-wire line into a company-internal four-wire line to the SO interface for connecting ISDN terminals or a PABX.

P

PAP (Password Authentication Protocol)

Optional authentication protocol for the →PPP connection setup. Unlike for →CHAP, the user ID and password are transferred unencrypted.

PPP (Point to Point Protocol)

The Point to Point Protocol (PPP) is designed to encapsulate datagrams over serial lines, and supports the transfer of LAN protocols like the → IP protocol.

preshared secret

Secret character string used with → IKE for authentication. The preshared secret must only be known to authorized communication partners.

Private automatic branch exchange (PABX)

A private switching system connected with the public telecommunications network for external communication. PABXs are not restricted to the telephone service, but offer transport services for all office communication (voice, text, data, and image transfer).

R

remote management

Remote maintenance of your LineCrypt by an authorized system administrator via the ISDN channel or the network.

RIP (Routing Information Protocol)

Protocol for exchanging routing tables between routers.

RSA

Asymmetrical encryption method. The LineCrypt devices use RSA for authentication and for exchanging the session keys.

S

Security Policy

In a →VPN protected by →IPSec, a Security Policy defines a range of IP addresses, and how IP packets in this range are to be handled (discard, forward without handling, or forward encrypted).

session keys

Used for encryption of the user data. New session keys are generated for every session with the random number generator on the chip card.

SHA-1 (Secure Hash Algorithm 1)

Hash algorithm that calculates a unique 160-bit-long digital signature from a data stream of any length. SHA-1 is used by →IKE for packet authentication.

SNMP (Simple Network Management Protocol)

Protocol for the management and monitoring of network devices. UDP is normally used as the transport protocol.

SOHO (Small Office Home Office)

Name for small branches that are linked to a company network via the Internet and dial-up connections.

SPD (Security Policy Database)

Table of →Security Policies.

T

TCOS (TeleSec Chipcard Operating System)

Operating system for processor-controlled chip cards (smart cards).

TCP

TCP is a connection-oriented transport protocol for use in packet switched networks. The protocol builds on the IP protocol, supports the functions of the transport layer, and establishes a reliable connection between the entities before data transfer.

TCP/IP (Internet Protocol and Transmission Control Protocol)

→ TCP and → IP are protocol standards on which the Internet is based.

telework

Any activity aided by information and communications technology that is always or only sometimes done at a workstation located outside the central workplace. This workstation is connected with the central workplace electronically.

Triple DES

Variant of the →DES encryption method with improved security. The key length is tripled to 168 bits, and DES is executed three times in a row.

Trust Center

→CA (Certification Authority); trusted authority that generates keys and issues →certificates.

TTL (Time To Live)

Life of an entry in the →directory service.

U

UDP (User Datagram Protocol)

The User Datagram Protocol is a transport protocol (layer 4) of the OSI reference model and supports connectionless data exchange between computers. UDP was defined to also give application processes the direct possibility of sending datagrams and thus fulfill the requirements of transaction-oriented traffic. UDP builds directly on the →IP protocol beneath.

UDP (User Datagram Protocol)

The User Datagram Protocol is a transport protocol (layer 4) of the OSI reference model and supports connectionless data exchange between computers. UDP was defined to also give application processes the direct possibility of sending datagrams and thus fulfill the requirements of transaction-oriented traffic. UDP builds directly on the →IP protocol beneath.

user group list

Closed user group list; requires a LineCrypt Company Card.

W

white list

List of certificate IDs of the users who are authorized for communication via the LineCrypt.

Index

alias name 37
authentication 7f., 27, 29, 32f., 79f., 84ff.
black list 36f., 79
black zone 6
CA list 7, 35, 79
certificate ID 79f., 88
certificate numbers 36, 42f.
chip card 7f., 11, 13, 30, 34, 37, 39, 42, 56f., 80, 86
Company Card 36f., 80, 83, 88
Configuration Security Policies 30
CUG 36, 72ff.
delivery 82
directory service 22, 25f., 28, 31, 51ff., 59, 61, 65, 67
end number 17, 19, 28
Ethernet 21, 24, 31, 49, 81, 83
GSM 5, 9, 16, 72f.
ICMP 26, 32, 81
IDEA 4, 8, 33, 82
IKE 8, 33
Internet Control Message Protocol 81
IP address 21ff., 29ff., 45ff., 51f., 54, 56ff., 62, 64ff., 68, 74ff., 84, 86
IP network 77, 81f.
IPSec 31ff., 46, 82, 86
LAN 83ff.
LED 83
Local network configuration 21
log data 29, 40f.
log file 21, 35, 37, 40, 83
MSN 17f., 28f., 72f., 77, 84
NAT 26, 32, 84
NetKey Card 6, 84
network configuration 21, 24
numbering plan 19
operating error counter 6
operating mode 13, 15f., 18f.
operating system 84
PABX 14f., 19, 28, 84f.
partner certificates 35, 74ff.
password 13, 27, 29, 39, 42, 44, 72ff., 80, 85

permanent IP address 31, 45f., 62, 68
plaintext 27, 73
PPP 13f., 17, 24ff., 31, 42, 46, 51, 59f., 65f., 76f., 85
prefix number 16, 73
Prefix number 16f.
red zone 6
remote management 42, 85
RIP 23, 85
route 23, 46
router 22, 84
RSA 7, 79, 85
security gateway 31
Security Policy 30f., 34, 48f., 77f., 86
session key 7f., 32, 85f.
settings 5, 10ff., 20, 26, 29, 33, 72ff., 80
SNMP 23f., 86
software update 41
TCP 13, 21, 24, 26, 30, 34, 42, 46, 74ff., 81, 87
terminal 6, 35, 84
user group characteristic 36f.
user group list 36f., 88
user interface 10
V.110 15f.
V.32 15, 17
version number 41
VPN 45f., 51
white list 36f., 88

Important telephone numbers

In the event of malfunctions:

Sales enquiries:

Please enter the telephone number
when handing over the unit.

The LineCrypt fulfils the requirements of the following EU Directive:
1999/5/EG

For this reason, the LineCrypt bears the CE mark.

Responsible for content: T-TeleSec Products
Further information: http://www.telekom.de/t-telesec,
e-mail: to T-Telesec@telekom.de, or
telephone at Freecall: 0800-Telesec (0800-8353732)

Issued by:
Deutsche Telekom AG

Edition: 16.09.03
Subject to change without notice
Printed on environmentally friendly paper