SPENDEX 40

SPEECH ENCRYPTION DECRYPTION EQUIPMENT TYPE UA 8251/01

OPERATING MANUAL

NATO RESTRICTED

Document No. 9922 154 13061
Issue date: 13-06-88
Printed in The Netherlands

PHILIPS

PHILIPS

CONTENTS

Abbreviations

CIK	Crypto Ignition Key
DTE	Data Terminal Equipment
Ptt	Press to talk

Definitions

CIK module:
Programmed module, unique per terminal, required for crypto operation.

Net Variable:
Key variable for producing encrypted traffic with a terminal of type SPENDEX 40.

1 INTRODUCTION

1.1 General

This manual contains operating instructions for the digital speech encryption/decryption equipment SPENDEX 40, type 8251/01, for use with Net variables in 2-Wire Full Duplex system.

1.2 Technical Description

The SPENDEX 40 can provide secure speech and secure data communication via standard telephone lines or radio links. For secure communication via a radio link the connection of a special radio modem is required.
The terminal can be used also as a normal telephone for nonsecure speech (no data) communication.

Secure communication is possible in the Net mode using Net variables.

When used in an appropriate network, a call can be set up with a certain precedence level. A choice can be made of four precedence levels: priority, immediate, flash, and flash override.

1.3 Mechanical Construction

The terminal is a compact appliance constructed of modules and primary designed for office use. For mobile use a shock mounting is available.

1.4 Configuration

Terminal	: UA 8251/01
Handset	: UA 8252/00
Line connecting cable	: UA 8240/00
Mains power supply cable	: 5722 660 30670
CIK module	: UA 8247/00
Transport case	: UA 8342/00
Set spare fuses	: 2 x 250 V/500 mA slow (2422 086 01015) 2 x 110 V/1 A slow (2422 086 01021)

2 KEY VARIABLE SETTINGS

2.1 General

For the purpose of secure communication Net variables are available to the terminal.

Net variables are loaded into the SPENDEX 40 from a loading device KYK-13 or a tape reader KOI-18 and are stored in encrypted form in a memory. This memory receives its supply from the battery, so that its contents are not lost in case of a power breakdown.

2.2 Net Variable

A Net variable is a key variable for setting up a secure call with a terminal of type SPENDEX 40. The user can himself choose from the Net variables stored in the memory, on condition, however, that a key variable is selected which is available also to the terminal at the other end. The memory can hold at the most 20 Net variables (compartments 00...19).

3 SECURITY

3.1 Physical Security

The terminal can operate in a secure mode only if the CIK module corresponding specifically to the terminal is connected. In this way the CIK module represents physical security against unauthorised use in the secure mode. Without the CIK module, the terminal can be used only as a normal telephone for nonsecure communication.

The CIK module is tested automatically each time it is connected. If its contents (i.e. the CIK) are valid, then "CIK OK " (terminal loaded) or "NUL.CIK " (terminal empty and CIK=0) appears in the display for 3 s. If the CIK is not valid, then "ILL.CIK " or "ERR.CIK " appears in the display.

3.2 General Zeroise

Pressing of the ZEROIZE push button makes all stored key variables unusable, whether the supply is switched on or off. If the supply voltage is present, "%ALARM " appears in the display and shortly after that "ZEROISED". Furthermore the contents of a CIK module that may be connected will be destroyed.
Only after new key variables have been loaded will it be possible to use the terminal again for secure communication.

4 CONTROLS AND CONNECTIONS (see Fig. 4.1 and Fig. 4.2)

4.1 Switches

4.1.1 On/Off Switch

The function of this switch is to switch the supply voltage on and off.

4.1.2 Hook Switch

The hook switch detects the picking up and replacing of the handset. Picking up leads to going off hook, so that the terminal is switched to the line. Replacing leads to going on hook, so that the terminal is switched off the line. During the replacing of the handset an alarm that may be present is reset.

4.1.3 Ptt Switch

The Ptt switch has no function.

4.2 Push Buttons

4.2.1 SECURE Push Button

After a clear call has been set up, pressing the SECURE push button will establish a secure call providing a Net variable has been selected.

4.2.2 ZEROIZE Push Button

When the ZEROIZE push button is pressed, all key variables that are stored will be rendered useless. If the supply voltage is present, then moreover the contents of a possibly present CIK module will be destroyed.

4.3 Keyboard

The terminal is equipped with a keyboard consisting of four rows of four keys each. The keys have the following functions:

4.3.1 Numerical Keys 0...9

The numerical keys 0...9 are used for introducing the numerals 0...9.

4.3.2 P Key (P = Precedence)

By means of this key a precedence level can be selected. This is only possible when the transmission network is suited for precedence level selection. The P key is also used to terminate an update action.

4.3.3 KDC Key

This key is reserved for a function in the KDC mode.

4.3.4 NET Key

Pressing of the NET key indicates that a compartment number will be dialled in.

4.3.5 DTE Key

Pressing of the DTE key during secure traffic changes the operating mode of the terminal from speech to data or from data to speech. The DTE key is also used to interrupt an update action.

4.3.6 * Key

Pressing of the * key in the on hook condition indicates that an update action follows.

4.3.7 # Key

This key has no function.

4.4 Indications

4.4.1 LED

The LED is located behind the display window. When illuminated, the LED indicates that the terminal is operating in the secure data mode. The LED has also an alarm function. It will flash as soon as a fatal hardware alarm is detected during the self-test; an acoustic signal is also produced.

4.4.2 Display

The terminal is provided with an eight-character alphanumeric display. This display provides information for the user about the state of the terminal.

4.5 Connections

4.5.1 Fill-gun Connector

Connector for connecting a key variable loading device.

4.5.2 CIK Connector

Connector for connecting the CIK module.

4.5.3 Handset Connector

Connector for connecting the handset.

4.5.4 Data Connector

Connector for connecting a data terminal equipment (e.g. a facsimile).

4.5.5 Line Connector

Connector for connecting the line connecting cable.

4.5.6 Modem Connector

Connector for connecting a radio modem.

4.5.7 Mains Connection

Connection for the 110/220 V mains voltage.

4.5.8 Earth Connection

Terminal connection for "security" earth.

4.6 Mains Voltage Selector

The function of the mains voltage selector is to set the power supply to the appropriate input voltage (110 V or 220 V).

4.7 Fuse Holders

Fuses : 2 x 110 V/1 A slow or
2 x 250 V/500 mA slow

4.8 Battery Compartment

The battery compartment contains a penlight battery, which retains the key variables during a power breakdown.

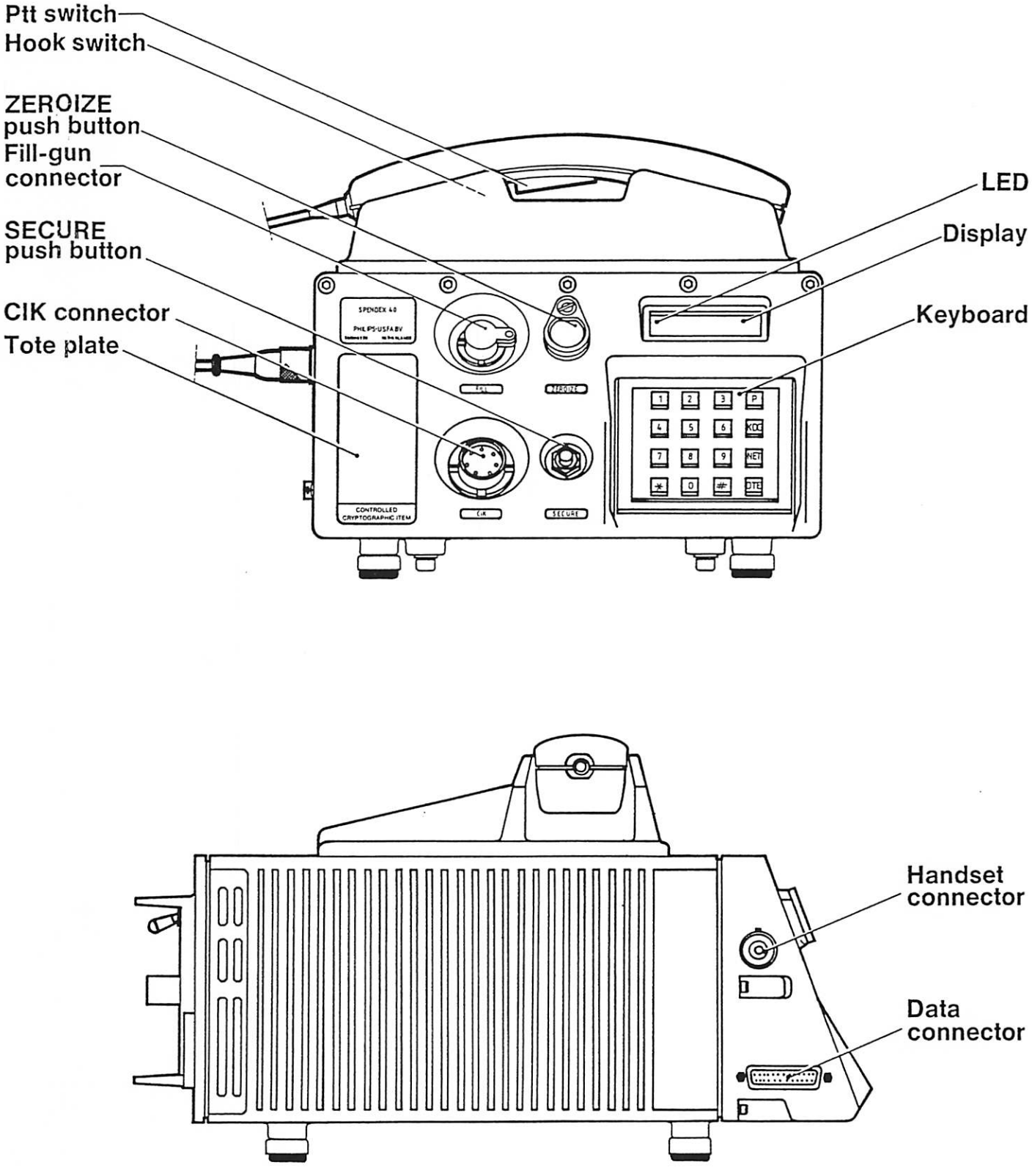

Fig. 4.1: Controls and connections on front and left-hand side

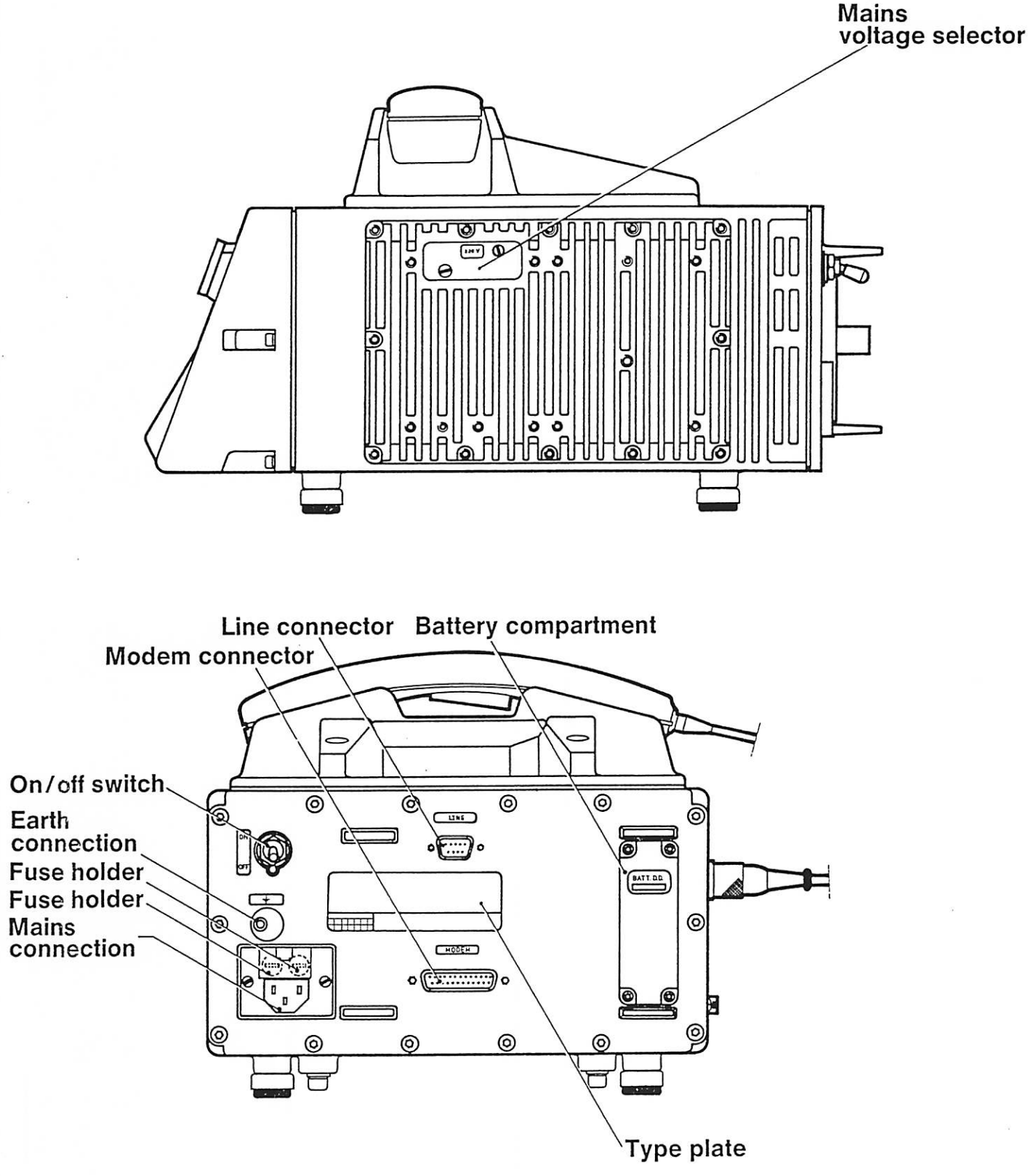

Fig. 4.2: Controls and connections on rear and right-hand side

5 OPERATING INSTRUCTIONS

5.1 General

This chapter contains the operating instructions at the user's level. The operation at the user's level is limited to:
- the setting up of a clear call;
- the setting up of a secure call on the basis of a Net variable;
- the setting up of a secure data connection;
- inspection of whether a valid Net variable is present;
- the updating of a single Net variable;
- the updating of all Net variables simultaneously.

5.2 Switching on of the Terminal

The terminal is switched on by putting the on/off switch in the "ON" position. After the switching on, the terminal commences with an initiation procedure, which is followed by an automatic self-test. During the self-test procedure "TESTING " appears in the display (not implemented in all terminals). If during the self-test no errors are detected, "* " appears in the display and the terminal is ready for operation. If self-testing does reveal an error, a report depending on the cause appears in the display. If a fatal hardware alarm is concerned, then furthermore the LED will start flashing and an alarm signal will become audible.

5.3 Setting up of a Clear Call

This section describes the actions to be performed in order to set up a clear call.

Actions	Calling terminal		Called terminal	
	LED	Display	LED	Display
Start conditions: - Terminals on hook		"* "		"* "
Calling terminal:				
1. Go off hook (see Note 1).		" X"		"* "
2. Wait for dialling tone.		" X"		"* "
3. Select, if required, a precedence level by pressing the P key once, twice, three or four times (see Note 2): - pressing once: - pressing twice: - pressing three times: - pressing four times:		"PRIORITY" "IMMEDIAT" "FLASH " "FLSH OVR"		"* "
4. Dial in telephone number.		"NNNNNNNN"		"* " (ringing signal)
Called terminal:				
1. Go off hook.		"NNNNNNNN"		"PLAIN "
Nonsecure speech possible (see Note 3)				
NNNNNNNN = last eight digits of telephone number (N = 0...9)				

Note 1: Before setting up a clear call in preparation for setting up a secure call, check first that the relevant Net variable is present (see section 5.6).

Note 2: Selection of a precedence level is possible only if the transmission network is suitable for precedence level selection. A precedence level can be chosen only once. Correction of the precedence level is possible only after going on hook again, then going off hook and selecting the appropriate level.

Note 3: A rapid intermittent signal during conversation indicates pre-emption; finish conversation immediately and go on hook.

5.4 Setting up of a Secure Call on the basis of a Net Variable

This section describes the actions to be performed in order to change from a clear call to a secure call based on a Net variable. The transition to a secure call based on a Net variable is possible only if the terminal at the other is provided with the same Net variable. The initiative to go over to a secure call can be taken only by the calling party.

Actions	Calling terminal		Called terminal	
	LED	Display	LED	Display
Start conditions: - CIK modules connected - Clear call connection		"NNNNNNNN"		"PLAIN "
Calling terminal: 1. Press NET key.		"COMPART?"		"PLAIN "
2. Dial in compartment number (00...19).		"NETAB AB" "SECURE ?" (See Note 1)		"PLAIN "
3. Press SECURE push button. (within 5 seconds).		"WAIT " "SYNCAQ " "SYNC ? " "CRYPTO " (See Note 2)		"WAIT " "* NET " ("* EMG ") "SYNC " "CRYPTO "
Secure speech possible (see Note 3)				
AB = compartment number (AB = 00...19)				

Note 1: If one wishes to correct the compartment number, then the selected compartment number can be cancelled by pressing of the NET key twice in succesion. In the display, "NO COMP " then appears.

Note 2: If the attempt to achieve synchronisation fails, both terminals revert automatically to clear traffic (both displays exhibit "PLAIN ").

Note 3: A rapid intermittent signal during conversation indicates pre-emption; finish conversation immediately and go on hook.

5.5 Setting up of a Secure Data Connection

This section describes the actions to be performed in order to change from a secure call to a secure data connection. The initiative to go over to a secure data connection can be taken only by the calling party.

Actions	Calling terminal		Called terminal	
	LED	Display	LED	Display
Start conditions: - Data terminal equipment connected and switched on - Secure call connection		"CRYPTO "		"CRYPTO "
Calling terminal: 1. Press DTE key.	X	"SYNCAQ " "SYNC ? " "CRYPTO "	X	"RESYNC " "* --- " "SYNC " "CRYPTO "
		(See Note 1)		
Secure data transmission possible (see Note 2)				
In case a secure call is wanted again, proceed as follows:				
Calling terminal: 1. Press DTE key.		"SYNCAQ " "SYNC ? " "CRYPTO "		"RESYNC " "* --- " "SYNC " "CRYPTO "
		(See Note 1)		
--- = NET or EMG				

Note 1: If the attempt to achieve synchronisation fails, both terminals revert automatically to clear traffic (both displays exhibit "PLAIN ").

Note 2: A rapid intermittent signal during data transmission indicates pre-emption; finish data transmission immediately and go on hook.

5.6 Inspection of Whether a Valid Net Variable is Present

This section describes the actions to be performed in order to check whether the terminal contains a valid Net variable.

Actions	LED	Display	Remarks
Start conditions: - Terminal on hook - CIK module connected		"* "	
1. Press NET key.		"COMPART?"	
2. Dial in compartment number (00...19).		"NETAB "	
		"NETAB ZZ"	Net variable valid.
		"AB NOKEY"	No Net variable.
		"ERR KEY "	Net variable not valid.
AB = compartment number (AB = 00...19) ZZ = update number (ZZ = 01...99)			

5.7 Updating of a Single Net Variable

The selecting of a single Net variable takes place on dialling in the compartment number under which the key variable is stored. Furthermore the possibility is provided of putting in also the number of update steps by dialling in the desired update number.

Actions	LED	Display	Remarks
Start conditions: - Terminal on hook - CIK module connected		"* "	
1. Dial in code 24111.		"* "	The digits do not become visible.
2. Press * key.		"UPD XX? "	
3. Dial in compartment number (00...19).		"UPD AB " "U AB.ZZ "	See Note 1.
4. Dial in the new update number, unless one update step is required.		"U AB.FF " "AB ZZ-FF"	See Note 1.
5. Press P key.		"ABYYYYFF"	Update action successful. See Note 2.
6. Press DTE key.		"* "	

AB = compartment number (AB = 00...19)
FF = new update number
YYYY = control group (Y = A...P)
ZZ = previous update number (ZZ = 01...99)

Note 1: The update procedure can be interrupted by pressing the DTE key. Then the terminal returns to the start condition and "* " appears in the display again.

Note 2: After the update action the terminal remains in the update substate. Another compartment can now be selected by dialling in a new compartment number immediately.

5.8 Updating of All Net Variables Simultaneously

All Net variables, with the exception of the Net variable in compartment 00, can be updated simultaneously by dialling in of code 96. There will be one update step per key variable.

Actions	LED	Display	Remarks
Start conditions: - Terminal on hook - CIK module connected		"* "	
1. Dial in code 24111.		"* "	The digits do not become visible.
2. Press * key.		"UPD XX? "	
3. Dial in code 96.		"UPD 96 " "U 96.-- "	See Note 1.
4. Press P key.		"96.-----"	Update action successful.
5. Press DTE key.		"* "	

Note 1: The update procedure can be interrupted by pressing the DTE key. Then the terminal returns to the start condition and "* " appears in the display again.

6 ERROR AND ALARM INDICATIONS

6.1 Error Indications

This section summarises the possible error indications and their meanings. The indications will remain in the display until a correcting procedure is performed.

6.1.1 Miscellaneous Errors

Display	Meaning
"ERR.CIK "	Activity/parity check on CIK failed
"ERR IZK "	Encryption/decryption of key variable failed
"ERR KEY "	Activity/parity check on key variable failed
"ILL.CIK "	CIK not valid (belongs not to the terminal)
"ILL CODE"	Illegal code selected
"ILL COMP"	Illegal compartment selected
"NO CIK "	CIK module not connected
"NO KEY "	Selected compartment contains no key variable
"NOCRYPTO"	No crypto functions available due to key generator failures detected during the self-test
"NUL.CIK "	Terminal empty and CIK = 0

6.1.2 Sync Acquisition Errors

Sync acquisition errors can only occur at the called terminal.

Display	Meaning
"? EMG " or "? NET "	Error during sync acquisition based on a Net variable

6.1.3 Errors During Secure Traffic

Display	Meaning
"DTE OFF "	Data terminal equipment not ready or switched off
"RESYNC "	Terminal returns to sync acquisition

6.1.4 Key Variable Update Errors

Display	Meaning
"-EMPTY- "	Terminal empty
"AB ALARM"	Activity/parity check on updated Net variable failed (AB = compartment number (01...19))
"ALARM "	Activity/parity check on updated Net variable failed
"U ERR 50"	Activity/parity check on Net variable failed
"U ERR 51"	Encryption or storage of Net variable failed
"UABERR50"	Activity/parity check on Net variable failed (AB = compartment number (01...19))
"UABERR51"	Encryption or storage of Net variable failed (AB = compartment number (01...19))

6.2 Alarm Indications

If an error is detected, an alarm report depending on the cause will appear in the display (%XXXXXXX). If a fatal hardware alarm is concerned (during self-test), then furthermore the LED will start flashing and an alarm signal becomes audible.
Alarms can be reset only by going off/on hook. If any alarm cannot be reset, report crypto alarm.