

SEC-LINE/FAX-2000Xe

Users Manual



Sec-Line/Fax-2000Xe is the latest creation of secure telefax communication equipment from Ardy Electronics. This encryption system is based on Ardy's encryption processor with an algorithm especially designed to meet the high demands of security and reliability.

Sec-Line/Fax-2000Xe is installed between the telephone line and the telefax terminal, and can be installed at all telefax types with group 3 communication.

Key management is according to ANSI standard with input of encryption keys from smart cards or from system keyboard. User smart card contains 100 encryption keys, which can be loaded to the encryption processor from the keyboard.

Sec-Line/Fax-2000Xe have a zeroize function for fast erasure of stored keys. Password or master smart card protects system keyboard from unauthorized use.

Sec-Line/Fax-2000Xe is customized for easy installation at existing telefax networks and gives you an electronic envelope to all your telefax messages, without any delay of the transmission.

Sec-Line/Fax-2000Xe eliminates all possibilities of inadvertent transmission caused by incorrect dialing or by errors in the telephone network.

Sec-Line/Fax-2000Xe is fully compatible with the SLF2000 fax encryption system.

SLF-2000Xe**Technical Data**

Transmission: according to CCITT group 3,T30.
Synchronous speed: 2400, 4800, 7200, 9600 bps.
Communication fully : transparent, or encrypted.
Display: 2x16 character.
Electrical interface: phone-line.

Encryption Data

Encryption: Ardy encryption processor.
Algorithm: Ardy stream cipher.
Key management: manual.
Key distribution: smart cards.
Key length: continuously changed 480 bits.
Key input: manual or smart card.
Synchronization: encrypted initialization vector.
Tamper protection: automatic internal protection.
Radiation protection: option.

General Data

Temperature range operating: 0 to 50 gC.
Temperature range storage: -20 to 60gC.
Power adapter: 240/110V, 50/60Hz, 24 VDC.
Size: 195x150x50mm.
Weight: 1,0 kg.
Cover: plastic.

Accessories

Master Smart card
User Smart card
Key Generator KL-2000

ARDY Electronics AB, P.O.Box 47, S-701 40 Örebro Sweden
Phone:+46 19 247010. Fax +46 19 247011. E-mail: info@ardy.se
www.ardyelectronics.com



Users Manual

For

SEC-LINE FAX 2000Xe
Fax Encryption System

Ardy Electronics AB
P.O. Box 47
SE-701 40 Örebro SWEDEN

Phone +46-19-247010
Fax. +46-19-247011
E-mail: info@ardy.se
www.ardyelectronics.com

Copyright © 1992-2004

1. SLF2000XE Telefax Encryption

- 1.1 General presentation of SLF2000XE Telefax Encryption.
 - 1.2 Functions of the SLF2000XE Telefax Encryption
 - 1.2.1 System Description
 - 1.2.2 Installation
 - 1.2.3 General Operation
 - 1.2.4 Keyboard Function
 - 1.2.5 Smart Card Management
 - 1.2.6 Error Messages
 - 1.2.7 Other Data
 - 1.2.8 Quick Guide SLF2000XE
 - 1.2.9 Appendix 1,2
 - 1.3 Encryption Key Management / Manual / Smart Cards
 - 1.4 Encryption Key Distribution Methods
 - 1.5 Installation of SLF2000XE Telefax Encryption System
 - 1.6 Configuration with Master Card
 - 1.7 Test of the Installation with Telefax machines
 - 1.8 Configuration of SLF2000XE with User Card
 - 1.9 Transmission of Not Encrypted and Encrypted faxmessage
-

1. SLF2000XE Telefax Encryption

1.1 General presentation of SLF2000Xe Telefax Encryption.

1.2 Functions of the SLF2000Xe Telefax Encryption

1.2.1 SYSTEM DESCRIPTION

General Description of the System

Sec-Line/Fax-2000 is an advanced encryption system for facsimile communication. The system can be connected to all types of Group 3 facsimile terminals.

The system shall be installed between the telephone line and the telefax terminal.

The version (3.0) and newer is compatible with CCITT T.30 standard of October 1984.

The encryption system eliminates all special functions which are not included in the CCITT standard.

When the system is installed on the telefax line, all incoming fax that are unencrypted can be received as normal.

When transmitting encrypted fax messages, the transmitting operator choose ENCRYPTION=ON and the receiving system automatically decrypt the message if the same encryption key has been installed.

If different encryption keys are installed in the receiving and transmitting parts the fax message will not be transmitted and the system shows COMM ERROR on the display.

The encryption system does not influence the transmission speed, but if the line quality is poor the system will decrease the speed according to the CCITT standard.

For more general information contact ARDY Electronics Ltd.

1.2.2 INSTALLATION

Power Supply

The main power for Version 2.9 and after is 220-240 Volt / 50 Hz (optional 110V / 50 Hz).

Make sure that the main power is 240V, and for safe operation connect the system to ground.

Activation of the System



When the system is delivered it is not activated with the Master Smart-Card. When the power is turned on the display will show:

Activation = OFF
Insert MSTR Card

Observe that this message will be displayed if the initial self test is passed; if any other message is displayed consult ARDY Electronics.

Put in the Master Smart-Card and wait until the display shows:

SMART-CARD
VALID

This message is a confirmation from the system that the inserted Master Smart-Card is valid. After this message the SLF2000XE unit is ready to accept commands from the keyboard and the display will show:

Activation = OFF
LOADING DATA

Older versions of the system will show:

If you want to activate the system push 'SHIFT' followed by 'SECURE', the display will now show:

Activation = OFF
CONFIRM

To confirm the activation of the system press 'SECURE' once again and the display will show

For versions after V 2:13 the information will be automatically loaded into the system and show

Activation = OFF
LOADING DATA

While the system loads data from the Master Smart-Card. If the loading was successful the display will show

Activation = ON
READY

after a short while. After this the system is activated and can be used by the operator. For further information about the set-up possibilities with the Master Smart-Card see Users Manual section Master Smart-Card.

If you get any Error messages, such as

SMART-CARD
INVALID = 032

consult section Error Messages for more information about the error.

After the activation of the system you shall take out the Master Smart-Card and keep it secure.

If you send the system to other locations you must deactivate the system with the Master Smart-Card. If the system disappears during transportation it can not be used by anyone before it is activated again.

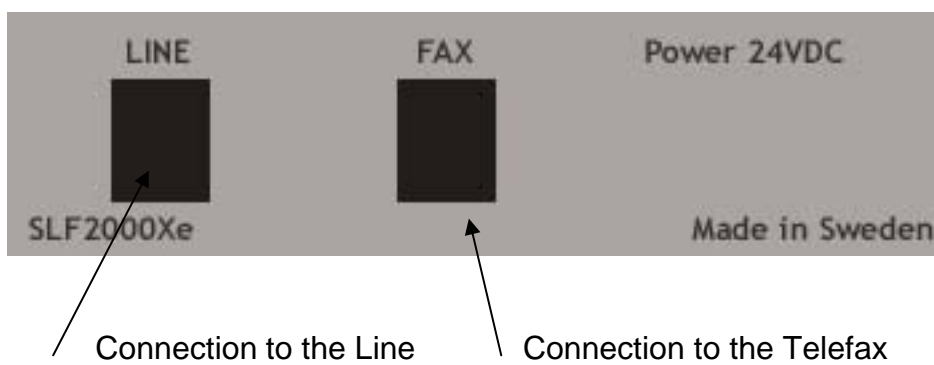
If you like to deactivate the system (Activation = OFF) proceed in the same manner as described above.

E.g. insert Master Smart-Card and press 'SHIFT' + 'SECURE' + 'SECURE' and the display will show:

Activation = OFF
READY

The system is now deactivated and you can take out your Master Smart-Card.

Line installation



Disconnect the telefax terminal from the telephone line and install the encryption system to the line by connecting the telephone-cord to the socket marked 'LINE' on the back of the encryption system. Connect the telefax terminal to the socket marked 'FAX'.

The modular connector is of the model 6/4 with the default connection to the two middle poles. If other connections are required consult ARDY Electronics Ltd for how to change the default connection.

To test if the installation is correct just lift the hook on the telefax terminal and wait for the line connect tone. If you can hear the tone the Encryption system is correctly installed.

If your line connect tone is 425 ± 15 Hz the SLF2000XE will display:

TRANSMITTING=OFF
DIAL TONE DETECT

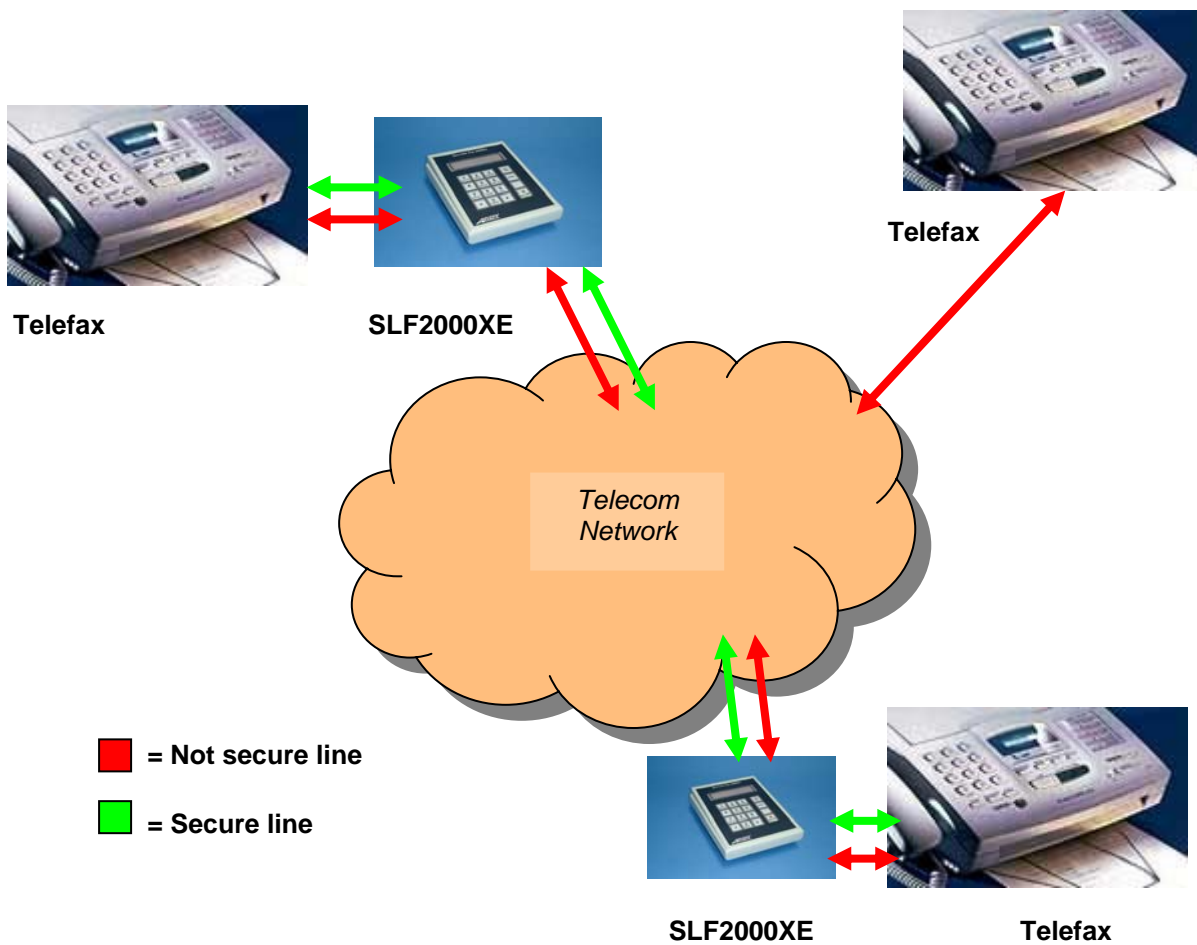
If your line connect tone is any other frequency you will not get any message on the display when you lift the hook on the telefax terminal. Other frequencies than 425 ± 15 Hz will not interfere with the function of SLF2000XE, the only thing that will happen is that the message above will be missing.

Put the telefax terminal on-hook and wait until SLF2000XE shows:

ENCRYPTION = OFF
READY

The System is now ready to use.

1.2.3 GENERAL OPERATION



Transmitting unencrypted Fax messages

It is possible to transmit an unencrypted fax message to all other group 3 telefax terminals on the market with the encryption system installed. When you transmit unencrypted fax messages the receiving side doesn't need to have a SLF2000XE installed. The only thing you have to observe is that the encryption is in the encryption OFF mode. The display must then show:

ENCRYPTION = OFF
READY

During the transmission you can read the transmission speed on the display of the encryption system. If different speeds are displayed from time to another that is because of different line quality. The display will show something like this:

TRANSMITTING=OFF
V.29 9600 bps

The 'OFF' after 'TRANSMITTING' is telling you that the encryption is turned OFF.

When the fax message is being transmitted the display shows different messages for the transmission.

When the fax message has been correctly transmitted to the receiver the display on the encryption system shows:

COMMUNICATION
COMPLETED

And then the display will show:

ENCRYPTION = OFF
READY

Now the system is ready for transmitting or receiving new fax messages.

Transmitting ENCRYPTED Fax messages

When an encrypted fax message shall be transmitted both the transmitting and the receiving side must have an encryption system installed. Both encryption systems must have the same encryption key installed.

When you want to transmit an encrypted fax message push the keyboard 'SECURE ON/OFF' so that the display will show:

ENCRYPTION = ON
READY

Now the system is ready for encrypted fax transmission. Start the transmission from the fax terminal as normal. During transmission the display will show something like this:

TRANSMITTING=ON
V.29 9600 bps

The 'ON' after 'TRANSMITTING' is telling you that the encryption is turned ON.

If different encryption keys are installed in the transmitting and the receiving system, or if the receiving system has no encryption system installed, the transmission will fail and the encryption unit will show:

COMM. ERROR
NO MESSAGE

For more about encryption key management section in this manual.

Receiving encrypted and unencrypted fax messages

Since it is the transmitting operator who decides if the fax message should be encrypted or not, the decryption of encrypted fax messages is automatic, the receiving operator only has to ensure that both the receiving and the transmitting system has the same encryption keys installed. If different keys are installed no fax message will be transmitted or received.

As an information to the receiving operator the transmitting system will put the text '**=CARD ID *** ENCRYPTED by ARDY *****' on the top of the fax message. This message is turned ON by default when encrypted fax messages are sent, but it is possible to turn it off by using the Master Smart-Card.

If the fax message received is unencrypted the encryption system will receive the message as normal.

Encryption key management



The encryption system version 2.14 has both manual key management and key management by using Smart-Card.

For information how to use the key management with Smart-Card

The encryption keys can be entered from the keyboard or loaded from a Smart-Card. Each encryption key is 30 characters long. The system can store 10 keys in its permanent memory as short keys (0-9). For safety these encryption keys should be put in to the system by two different persons, who each know 15 characters.

The 10 short keys can also be loaded from the Smart-Card

The user then only loads one of the 10 different encryption keys according to a preplanned schedule.

The security officer shall have an emergency plan for fast change of encryption keys in all encryption systems. This is in case any system disappears from its normal location.

The encryption system shall be located at a safe place and not exposed to un-authorized people.

In case of emergency all the encryption keys can be zeroized from the system keyboard, just press the keyboard 'SHIFT' and 'KEY ZEROIZE' (followed by password, if required) and the 'KEY ZEROIZE' once again to confirm the destruction of all the keys. All loaded keys will be destroyed, including the 10 short keys.

Self test

When the encryption system is powered up the system runs a self test routine. If this test is correct the display shows:

Self test Running
PASSED

After this test the system is ready for operation, if some error occurs the display will show:

Self test Running
FAILED: xx

xx is an error code that tells more about the error, see Users Manual section Error Messages.

After this message the display will show either:

HARDWARE ERROR
CALL FOR SERVICE

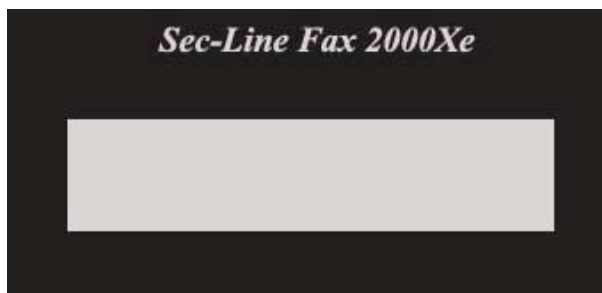
Or:

SV Card Required

In both cases the system needs service from ARDY Electronics Ltd.

The self test routines tests the modem circuits, the RAM memory, the program memory, the resident encryption data and the encryption processor.

Display



The encryption system display is a 2 row, 16 characters alphanumeric display. This display shows different information during the operation of the system.

Normally it is possible to see the transmission speed and the standard designation for the chosen transmission speed.

It is also possible to get more technical information on the display if **'SHIFT' and key '0'** is pressed. The display then shows:

MODE= NORMAL
CONFIRM

If you then press '0' once again the display will show:

MODE = DIAGNOSTIC
READY

Now the display will show all handshaking information that occurs during the fax communication.

To get to normal press 'SHIFT' and '0' twice and you will get normal mode again.

Keyboard



Most of the keys on the keyboard have double functions. To get this second function first press 'SHIFT' and then the wanted function key. With master or user Smart-Card inserted the function of the keys will be different.

All keyboard operations will activate the display which waits for input from the operator.

If input of information to the system is not carried out completely, the system automatically interrupts the input and return to the default state.

If a wrong character has been input it is possible to erase it by pressing 'SHIFT' and '<---'. The function can also be aborted by pressing 'SHIFT' twice.

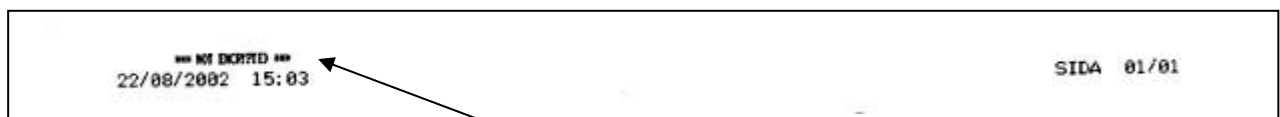
Smart-Card reader

The system is equipped with a Smart-Card reader to make it possible to use Master and Users Smart-Card.

Messages on the FAX

The received and transmitted faXes can be marked with different messages depending on the set-up

A received unencrypted fax message can be marked with: "*** NOT ENCRYPTED ***", this message is added to the fax message by the receiving SLF2000XE.



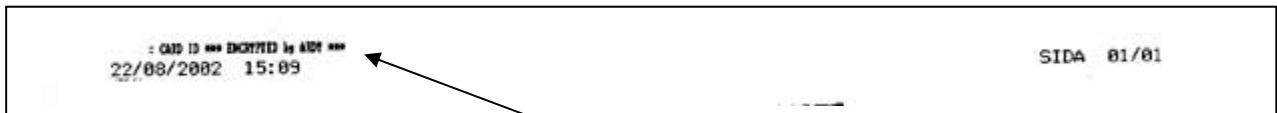
***** NOT ENCRYPTED*****

A transmitted encrypted fax message can be marked with: "XYZW=CARD ID *** ENCRYPTED by ARDY***", this message is added to the fax message by the transmitting SLF2000XE. The "XYZW" is the four least significant digits in the Serial number of an inserted valid User Smart-Card. If no User Smart-Card is inserted these digits will not appear on the fax.



BAN DEMO = CARD ID * ENCRYPTED by ARDY *****

Or if no User Smart Card is installed at the transmitting side:



= CARD ID * ENCRYPTED by ARDY *****

Messages to the Transmitting fax

If parameter 10 is set to 1 the SLF2000XE encryption system will mark the CSI-block of the handshake with a 'E' in all empty positions if the transmitted fax was sent encrypted. This information can later on be examined when a traffic report from the fax is printed. If the SLF2000XE is put in the IDF-2000 mode the CSI-block will be marked with a 'I' in all empty positions.

E.g. all transmitted encrypted faXes can be identified on the traffic report on the sending side.

Example of traffic report with parameter 10 = 1:

No	Date	Time	T/R	ID	
1	10-05	08.53	G3/T	EEEE46E19E270860	<Encrypted
2	10-05	08.54	G3/T	46 19 270860	<Not encrypted

Compatibility with IDF-2000

If parameter 11 is set to 1, the SLF2000XE encryption system will have the possibility to work as an IDF-2000 system when transmitting telefax messages to telefax terminals equipped with an IDF-2000.

When parameter 11 is set to 1 the ID check mode is activated by pressing 'SHIFT' + 'SECURE', the display will then show:

ID. CHECK = ON READY:3100

The four digits after "READY" is the SLF2000XE Master identity, this identity will be sent over the telephone line to make it possible to control that the receiving side have the same identity. The transmitted fax will be marked with "3100= UNIT ID *** CONTROLLED by ARDY ***".

This mode always time-outs to the default start-up state after approx. 5 minutes. For more information about this mode please consult the IDF-2000 Manual.

1.2.4 KEYBOARD FUNCTIONS

Password management

Activation of Password

When the SLF2000XE encryption system is delivered the password function is 'ON' by default. The **default password is '5555'**.

Changing the Password

When the previous stored password is known it is possible to enter a new password from the keyboard without using the Master Smart-Card. If the previous stored password is not known you have to use the Master Smart-Card to change it.

To change a known password follow the steps below.

Enter '**SHIFT**' and then key '**3**', the display will show:

OLD PASSWORD No:

If the password function is OFF the encryption system will respond with 'OPERATOR ERROR' if you try this function.

When you get the message above enter the 5 digit password. If the password entered is correct the display will show:

NEW PASSWORD No:

If the old password entered was incorrect the command will be aborted and the display will show 'INVALID' on line 2.

Enter the new 5 digit password. After the first input of the new password you have to verify the new password.

If the verification was correct the password will be changed and the display will show:

VERIFY PASSWORD PASSWORD CHANGED

If the verification is incorrect the display will show:

VERIFY PASSWORD INVALID

and the new password is not activated and stored; the old password will still be unchanged.

Normal use of the Password

When the password function is activated (see Users Manual 5.1) the commands 'KEY ENTRY' (see Users Manual 4.2), 'KEY ZEROIZE' (see Users Manual 4.3) and 'ENTER SH KEY' (see Users Manual 4.4) will require a correct password entry before it is possible to eXecute the commands. Some of the card functions will also require a correct password entry in some cases.

If the password function is activated the encryption system will respond to the mentioned commands with:

ENTER PASSWORD No:

Before it is possible to eXecute the command the 5 digit password has to be entered. If the password entered is correct the command will start

immediately after the password input. To proceed with the command follow the instructions in the following sections.

If the password entered is incorrect the display will show:

ENTER PASSWORD
INVALID

and it will not be possible to proceed with the requested command. If the password function is OFF the commands will start immediately without any password entry.

ENCRYPTION KEY ENTRY



Encryption Processor

1 Encryption Key

Activated from the
Keyboard

System Memory Short Key

10 Encryption Keys

Activated from the
Keyboard

User Smart Card

100 Encryption Keys

Activated from the
User Smart Card

For input of encryption keys directly to the encryption processor press **'SHIFT'** followed by **'KEY ENTRY' (1)**. The display will then show (after password entry, if the password function is ON):

KEY ENTRY
No1:

Now input the first 10 characters of the key from the keyboard, allowed characters is 0-9. After the first 10 characters the display will show:

KEY ENTRY
No2:

Enter the next 10 characters of the key. And when the display shows 'No3:' on line 2, enter the last 10 characters of the key. The encryption unit will then load the key to the encryption processor, this is indicated with:

KEY ENTRY
LOADING KEY

It is only possible to load 3 encryption keys within 10 minutes. If the 10 minute lock is active the display shows:

ENCRYPTION = OFF
(* READY *)

If the operator tries to load new encryption keys when the 10 minute lock is active the display shows:

KEY ENTRY
LOAD NOT ALLOWED

After 10 minutes has passed the display will show:

ENCRYPTION = OFF
READY

and new encryption keys can be downloaded to the encryption processor again.

KEY ZEROIZE

If short keys and encryption keys have to be erased and destroyed, press '**SHIFT**' and '**KEY ZEROIZE**' (2), The display will then show (after password entry, if the password function is ON):

KEYS ZEROIZE
CONFIRM

If you confirm the command by pressing 'KEY ZEROIZE' once again the display will show:

KEYS ZEROIZE
ZEROIZING KEYS

After this all stored keys will be erased, and the security officer has to load new encryption keys and short keys to the system.

ENTER Short KEY

For input of short keys press '**SHIFT**' and then '**ENTER SH KEY**' (5). The display will then show (after password entry, if the password function is ON):

SH KEY ENTRY:_

Now put in the number of the short key to program (0-9) and then the 30 characters in the key (input as in 4.2).

After all 30 characters in the key have been entered the display will show:

SH KEY ENTRY:X
UPDATING SH KEY

Now the operator has stored one short key that later can be loaded to the encryption processor.

GET Short KEY

For loading of stored short keys to the encryption processor press '**SHIFT**' and '**GET SH KEY**' (6). The display will then show:

GET SH KEY:_
Prg: 0123456789

The numbers in line 2 of the displays shows which of the short keys that is programmed. If some or all of the numbers in line 2 isn't shown on the display that indicate that these short keys are not programmed.

Now the operator has to choose one of the ten short keys (0-9) to be loaded to the encryption processor.
If the chosen short key has not been programmed the display shows:

ENCRYPTION = OFF
NOT PROGRAMMED

If the chosen short key is stored in the short key memory the system loads the key to the encryption processor, and the display then shows:

GET SH KEY:X
LOADING KEY

Observe that if the 10 minute lock is active it is not possible to load encryption keys to the encryption processor. The display will then show:

ENCRYPTION = OFF
LOAD NOT ALLOWED

Wait until the display shows:

ENCRYPTION=OFF
READY

now a new short key can be loaded to the encryption processor.

CONTROL SHort KEY

If the operator wants to control which short key that is loaded (if any) to the encryption processor, press '**SHIFT**' and '**CONTROL SH KEY**' (7). The display will then show:

SH KEY CONT.:_

Now choose which short key you would like to control (0-9). If the chosen short key has been loaded to the encryption processor the display shows:

SH KEY CONT.:X
KEY MATCH OK

If the chosen short key has not been loaded the display will show:

SH KEY CONT.:X
KEY MATCH FAIL

Observe that this function only control the chosen short key and never controls the actual encryption key.

Test modes

By pressing '**SHIFT**' and '**8**' it is possible to put the encryption system in different test modes. For more information about the test modes contact ARDY Electronics Ltd.

SHIFT + 8 and diagnostic code 0620 will generate an internal self test. (The display will in this test sometimes stop and wait for the operator to press the keyboard, in these cases press **SECURE** and hold it for more then 1 second and the test will continue).

SHIFT + 0 + 0 will toggle between **Diagnostic** and **Normal** mode during communication. In Normal mode the display will only show normal information about the communication. In Diagnostic mode the display will show the standard telefax handshake signals, which makes it possible for the operator to follow the handshake sequence between the two telefax machines during the communication.

SHIFT

This key is only used to reach the second functions of the keyboard.

Always when the operator wants to use the keyboard functions start with '**SHIFT**' and then the wanted function.

Most of the functions can be aborted by pressing '**SHIFT**' twice.

SECURE ON/OFF/ (AUTO)

When an encrypted fax message is to be transmitted press the '**SECURE ON/OFF**' until the display shows:

ENCRYPTION = ON
READY

This command mode will continue, or automatically return to OFF, depending on the parameter set-up.

Some of the possible set-ups only allow encryption ON or OFF; in these cases the 'SECURE ON/OFF' key has no function.

The default set-up is ENCRYPTION = OFF and with ENCRYPTION = ON with a 5 minute time-out. This means that if no message has been transmitted within 5 minutes from the choice of ENCRYPTION = ON the encryption system automatically will return to ENCRYPTION = OFF mode.

The different ON/OFF modes are:

Value	Start-up with	ON Time-out	OFF Time-out	Remark
0	Encry = OFF	YES *	NO	Encry=ON only with User-Card *
1	Encry = OFF	YES 5 minutes	NO	Default
2	Encry = ON	NO	YES 5 minutes	
3	Encry = OFF	NO	NO	
4	Encry = ON	NO	NO	
5	Encry = ON	NO	--	Only ON allowed
6	Encry = OFF	--	NO	Only OFF allowed
7	Encry = OFF	YES	NO	Transmission only allowed with User-Card see Appendix 1

* Mode 0 is a special mode which allows ENCRYPTION=ON only when a valid User Smart-Card is inserted. E.g. ENCRYPTION=ON will be chosen as soon as a valid User Smart-Card is inserted.

It is, however, possible to put the SLF2000XE in ENCRYPTION=OFF by pressing the SECURE ON/OFF. As soon as the User Smart-Card is deleted the SLF2000XE will return to ENCRYPTION=OFF. After a successful transmission or after 5 minutes the SLF2000XE will return to the default state ENCRYPTION=OFF and no card accepted, even if the

User Smart-Card is still inserted. To get into the ENCRYPTION=ON mode again you have to reinsert the User Smart-Card.

If parameter 9 is set to 1 or 2 it is possible to put SLF2000XE in the state:

ENCRYPTION =AUTO
READY

In this state the SLF2000XE encryption system will automatically turn encryption ON when transmitting fax messages and the receiving fax has a SLF2000XE installed. If parameter 9 is set to 2 the system will turn encryption ON automatically only if the receiving system has the same Master Smart-Card identity as the transmitting system.

REMARK: This function only works when both the receiving and the transmitting system has version 2.4 or higher of the software.

With parameter 9 set to 1 the different ON/OFF/AUTO modes (parameter 2) will function as described below:

Value	Start-up with	Time-out	Remark
0	Encry =AUTO	YES,ON and OFF 5 minutes.	Encry=ON only with User-Card *
1	Encry =AUTO	YES,ON and OFF 5 minutes.	Default
2	Encry = ON	YES,AUTO and OFF 5 minutes	
3	Encry =AUTO	NO	
4	Encry = ON	NO	
5	Encry = ON	NO	Only ON allowed
6	Encry =AUTO	YES,OFF 5 minutes	Only OFF and AUTO allowed
7	Encry =OFF		AUTO not allowed

The automatic turn on of encryption only works when the display shows "ENCRYPTION=AUTO".

In the state ENCRYPTION=ON or OFF will the system stay in the chosen state independent of if there is a system installed or not at the receiving fax.

1.2.5 SMART-CARD MANAGEMENT



The SLF2000 uses 3 kind of Smart Cards

- SV Card (Service & Support)
- Master Smart Card (Security Manager)
- User Smart Card (Users)

SV-Card (Super Visor Card)

The SV card is only used to program the SLF2000XE unit in production with necessary start up functions and is not used in the daily operation.

Master Smart-Card

The Master Smart-Card is used to activate and deactivate the system. With the Master Smart-Card it is also possible to configure the system in different ways.

Activation and Deactivation of the system

Activation and deactivation is described earlier in this manual.

When the system is activated data from the Master Smart-Card is loaded in the encryption systems permanent memory. The configuration of the system will be put in default state when it is activated.

Before it is possible to change the configuration of the system is should be activated, e.g. the display will show (with inserted and accepted Master-Smart Card):

Activation = ON
READY

Every Master Smart-Card has an identity; the identity code of the Master Smart-Card is a 4 digit code of the form '3XXX', where 'XXX' is Hexadecimal digits. If the system, for instance, is activated with a Master Smart-Card with identity '3009' you must have a Master Smart-Card with the same identity to deactivate the system.

For more information about the Master Smart-Card consult ARDY Electronics Ltd.

Changing the Password

When the system is delivered the default password is '55555'. If you want to change the password you can do so without the Master Smart-Card if the old password is known.

If the old password is not known you have to put in a valid Master Smart-Card to be able to change it.

With a valid Master Smart-Card inserted, and Activation=ON, press '**SHIFT**' and then '**3**'. The display will then show:

ENTER PASSWORD
No: _

Enter the 5 digit password that you want the system to have.

After the first input of the password you have to verify the password before it is stored. The display will show:

VERIFY PASSWORD
No: _

Enter the password once again, if the password entered the second time is the same as the first one the password will be changed, and the display will show:

PASSWORD = ON
PASSWORD CHANGED

If the password entered the second time is different than the first one the password will not be changed and the display will show:

VERIFY PASSWORD
INVALID

Selecting Password ON or OFF

The password function is by default ON, but it is possible to turn it off with the Master Smart-Card inserted and with Activation = ON. To turn it OFF (or ON) press **'SHIFT' followed by '4'**, the display will then show:

PASSWORD = ON
CONFIRM

If you confirm the change of the password function press '4' once again, and the display will show:

PASSWORD = OFF

The password function is now turned OFF. To turn it on again proceed as above. E.g. **'SHIFT' + '4' + '4'** and the display will show:

PASSWORD = ON

Configuration of the System

The SLF2000XE encryption system has several different parameters that are programmable by the user. It is possible to change these parameters with the Master Smart-Card inserted and Activation = ON.

Every time the system is deactivated (Activation = OFF) and then activated again (Activation = ON) the parameters will be put in default state, according to the data programmed in the Master Smart-Card. It is possible to order Master Smart-Cards with different parameter values than those that are stated as default, contact ARDY Electronics Ltd for more information.

To change (or control) the parameter programming of the system press **'SHIFT' followed by '8'** with the Master Smart-Card inserted (and accepted) and with Activation = ON. The display will then show:

Parameter = 000
Value = 1

This is showing that Parameter 0 has the programmed value 1. If you want to **change the value press '9'** to step the parameter value to the

wanted state. For instance, if you want parameter 0 to have the value 0 press '9' until the display shows:

Parameter = 000 Value = 0

To program this new value into the encryption systems permanent memory press **SHIFT**, the display will then show:

Parameter = 000 Programming:0

The new value is now programmed!

To change the parameter press '0' until the display shows the parameter number you want to change. For instance if you want to **change parameter 3 press '0'** three times and the display will show:

Parameter = 003 Value = 1

Proceed as described above to change the parameter value. To end the Parameter programming routine press 'SECURE' (or wait for the keyboard time-out app. 30 seconds).

The parameter values have the following meanings:

Parameter	Value	Description of function
000	0	Input of keys shown as digits.
000	1	Input of keys shown as '*' -DEFAULT
001	0	Input of password shown as digits.
001	1	Input of password shown as '*' -DEFAULT
002	0-7	Encryption ON/OFF
003	0	Fax messages are not marked.
003	1	Transmitted Encrypted fax messages marked with: "*** ENCRYPTED by ARDY/SLF2000XE ***"
003	2	Received not encrypted fax messages marked with: "*** NOT ENCRYPTED ***"
003	3	Value 1 and 2 combined - DEFAULT
004 ¹	0	UAP not required on USERS card -DEFAULT
004	1	UAP required on USERS card.

005	0-3	Output level of MODEM - DEFAULT = 3 Don't change without consulting the GENERAL MANUAL
006-7	0-255	Output level of MODEM; don't change without consulting the GENERAL MANUAL.
008	0-2	Automatic loading of keys. DEFAULT=0
009	0-2	Automatic ENCRYPTION=ON,. DEFAULT=0.
010	0-1	0 => CSI Block not marked when transmitting encrypted faXes -DEFAULT 1 => See Users Manual
011	0-1	0 => The system will not be able to work like an IDF-2000 - DEFAULT 1 => IDF-2000 mode is available.

The programmed parameter values are stored in permanent memory and will not be lost during power failure.

To reset all parameters to the default state, deactivate the system (Activation = OFF), press 'SHIFT' + 'SECURE' + 'SECURE' with a valid Master Smart-Card inserted.

Then press 'SHIFT' + 'SECURE' + 'SECURE' once again to activate the system (Activation = ON) and load the default configuration from the Master Smart-Card.

User Smart-Card

The User Smart-Card is used for distribution of keys to the SLF2000XE encryption system. When the User Smart-Card is delivered it is "blank", which means that the User Smart-Card has no keys stored and has not been initiated with the Master Smart-Card identification.

The Master Smart-Card identification stored on the User Smart-Card is a protection against unauthorized use in other SLF2000XE encryption system. Once the User Smart-Card has been programmed with Master Smart-Card identification it is only possible to use the User Smart-Card in SLF2000XE encryption systems that are activated with Master Smart-Card with the same identity as the one that is stored on the User Smart-Card.

It is possible to get the User Smart-Card delivered with keys stored, contact ARDY Electronics Ltd for more information.

Each User Smart-Card is able to store 100 keys (0-99). The User Smart-Card can also be programmed with a User Assigned Pin (UAP), if the UAP is programmed the User has to enter a 5 digit code every time he wants to use his card. If the wrong UAP is used 3 times in a row the card

will become locked. If the card is locked it is impossible to use it before it is unlocked, contact ARDY Electronics Ltd for more information.

Using the User Smart-Card the first time

When the User Smart-Card is delivered it is, as mentioned above, "blank". When a "blank" User Smart Card is inserted in a SLF2000XE (with Activation = ON) the SLF2000XE will detect that the card is blank and give you the following question on the display:

Init USER Card?
Confirm (SECURE)

If you confirm this question by pressing 'SECURE' the SLF2000XE will program its Master Smart-Card identity on the User Smart-Card. (The Master Smart-Card identity is stored in the SLF2000XE when it is activated, Activation = ON.) Before you program the Master Smart-Card identity on the User Smart-Card it is not possible to use it.

After the programming of Master Smart-Card identity it is only possible to use the User Smart-Card in units that is activated by Master Smart-Card with the same identity as the one programmed on the User Smart-Card. While the programming is taking place the display will show:

SMART-CARD
Programming:ID

If the programming of the Master Smart-Card identity was successful you will get a question on the display that will ask you if you want to program a User Assigned Pin (UAP) on the card:

Program UAP ?
Confirm (SECURE)

If the configuration of the system requires that every User Smart-Card should have an UAP programmed this question will not be displayed. Instead you will get the message that is shown below, the same message will be shown if you press 'SECURE' as a confirmation that you want to program the UAP:

UAP (5) ENTRY
No: _

Enter the 5 digits (0-9) that you want to have as UAP. After the first input you have to verify the input once again before the UAP is programmed, the verification question will be displayed as:

VERIFY UAP(5)
No: _

Enter the 5 digits in the UAP once again, if both the inputs are equal the UAP will be programmed; this is indicated on the display with:

SMART-CARD
Programming:UAP

If the both inputs are not equal the UAP will not be programmed and the display will show:

VERIFY UAP(5)
INVALID

IMPORTANT:

Programming of UAP can only be done once. If you forget your UAP and give the wrong UAP to the card 3 times the card will become locked. If you don't remember your UAP then the card will be unusable, since it is not possible to unlock a Card when you don't know the UAP.

It is possible to use User Smart-Card without UAP but it is not recommended. If you want to force every User to have User Smart-Card with programmed UAP, program parameter 4 to value 1.

If a User Smart-Card without an UAP is inserted in a SLF2000XE encryption system with parameter 4=1 you will always get the question:

Program UAP?
Confirm (SECURE)

And the card will not be accepted until an UAP is programmed.

How to use the User Smart-Card

As mentioned earlier the User Smart-Card is used for distribution of keys. But when it is delivered it has no keys stored. There is two ways to generate keys to be stored on the User Smart-Card, manual or automatic.

With the normal SLF2000XE encryption system it is only possible to store keys manually or load the 10 short key into a Users Smart Card, if you want to generate and store keys automatically please use the KEY LOADER unit supplied by ARDY Electronics Ltd.

During the use of User Smart-Card you will have to enter the Password (if UAP isn't programmed) or the User Assigned Pin (if UAP is programmed) to be able to load and store data from/to the card. The UAP question:

UAP (5) ENTRY
No: _

When this question is shown on the display always enter the correct UAP, otherwise the command will be aborted with an error message displayed. As mentioned earlier the card will become locked if you give the wrong UAP three times in a row.

When you insert a User Smart-Card in a SLF2000XE encryption system the display will show:

SMART-CARD

If the card has UAP programmed you will then get the UAP question as told above. Enter the correct UAP and the display will show (if UAP is not programmed this message will be shown without any UAP input):

SMART-CARD
VALID

If the User Smart-Card is invalid for some reason, or if you give the wrong UAP the display will show:

SMART-CARD
INVALID =XXX

See Users Manual section Error Messages for more information about the error codes.

If the User Smart-Card is accepted the display will show:

ENCRYPTION = OFF
==>READY:XYZW<==

This is an indication from the SLF2000XE that the card inserted is a valid User Smart-Card. You have to have this message on the display before it is possible to use the different functions supplied for the User Smart-Card. The "XYZW" is the four least significant digits in the User Card

serial number. These four digits will be transmitted as a part of the fax messages if the fax is encrypted and the message "XYZW= CARD ID *** ENCRYPTED by ARDY *** " is turned on.

Number of keys on the Card

If you want to know how many keys that are stored on the User Smart-Card press 'SHIFT' followed by '3' with the valid User Smart-Card inserted. The display will then show (after UAP input if required):

SMART-CARD
No of keys: 030

This is telling you that the inserted User Smart-Card has 30 keys stored. Since the keys always begin with key no. 00 the existing keys on this particular card has the numbers 00-29. Each card can store 100 keys.

Load 10 Keys from Smart-Card to Short-key memory

It is possible to load 10 consecutive keys from the User Smart-Card to the SLF2000XE permanent short-key memory. This is done by pressing 'SHIFT' + '4', the display will then show (after UAP or Password input):

LOAD 10 SH KEYS
From: _

Enter the number of the first User-Card key to store in Short-key memory 0. For instance key no 10, the display will then show:

LOAD 10 SH KEYS
From: 10 to 19?

This question asks you to confirm that key no 10 - 19 on the User-Card will be stored as Short-Key no 0-9 in the SLF2000XE Short-Key memory. If you confirm by pressing '4' the SLF2000XE encryption system will start to load keys from the User-Card to its internal short-key memory. Please note that the programming of Short keys is done backwards, starting by loading key 19 from the card and program Short-key 9. This is indicated on the display with:

LOAD 10 SH KEYS
Programming:09

The digits will then count backwards until it reaches '00' and then end with a 'OK'. Now all 10 Short-Keys are programmed with keys from the User Smart-Card. If you get any Error Messages during this command please see this Users Manual Error section.

GET KEY from User Smart-Card

For loading of keys stored on the User Smart-Card to the encryption processor press '**SHIFT**' and '**GET SH KEY**' (6) The display will then show (after UAP or Password input):

SMART-CARD
GET KEY No: _

Enter the number of the key that you want to load to the encryption processor (2 digits from 00-99). The display will then show:

SMART-CARD
RECEIVING SH KEY

If you get any Error messages after the previous shown message consult the Error section for more information.

If the load was successful the display will show:

SMART-CARD
LOADING KEY

If the 10 minute lock is active the display will show:

ENCRYPTION = OFF
LOAD NOT ALLOWED

When the 10 minute lock is active this is indicated on the display by:

ENCRYPTION = OFF
=(*READY:XYZW*)=

when the User Smart-Card is inserted. After 10 minutes has passed the display will show:

ENCRYPTION = OFF
==>READY:XYZW<==

now a new Smart-Card key can be downloaded to the encryption processor.

CONTROL Smart-Card Key

If a key is loaded from the User Smart-Card with the GET KEY command it is possible to verify which key that is loaded. Press '**SHIFT**' and '**CONTROL SH KEY**' (7). The display will then show:

SMART-CARD
CONT KEY No: _

Now choose which Smart-Card key you would like to control (00-99). If the chosen Smart-Card key has been loaded to the encryption processor the display shows:

SMART-CARD
KEY MATCH OK

If the chosen Smart-Card key has not been loaded the display will show:

SMART-CARD
KEY MATCH FAIL

Observe that this function only control the chosen Smart-Card key number and never controls the actual encryption key.

STORE SHORT KEYS to User Smart-Card

If all 10 short keys are programmed in the encryption systems short-key memory it is possible to store these 10 keys on the User Smart-Card. The use of this command requires that all 10 short keys are programmed and that the inserted User Smart-Card has at least 10 un-programmed Card keys. You activate the command by pressing '**SHIFT**' + '**8**', the display will then show:

STORE SHORT KEYS
CHECKING - WAIT!

The SLF2000XE is then performing a check that all 10 short keys are programmed and that there is at least 10 un-programmed keys on the User Smart-Card. If the check was successful the display will show

STORE SHORT KEYS
As: 030-039?

This question asks you to confirm the programming of the keys number 030 to 039 on the User Smart-Card with the contents of short key number 0-9.

You confirm the programming by pressing '8'. The display will then show (after UAP input if required):

STORE SHORT KEYS
Programming:030

The digits will then count upwards until the last key is programmed (39), the message on the display will end with 'Programming: No' when the SLF2000XE sends the command to update the number of stored keys to the card.

The 10 short-keys is now stored as key no 30 (short-key 0) to no 39 (short-key no 9) in the User Smart-Card.

By using the ENTER SHort KEY command and this command it is possible for the User to store his own keys on the User Smart-Card. It is also possible to copy keys from one card to another by first using the (LOAD 10 SH KEYS),function and then this command.

The SLF2000XE encryption system always store keys to the first free location on the card (key no 30 in the previous example). It is not possible to erase any keys on the User Smart-Card without using the KEY LOADER unit supplied by ARDY Electronics. Contact ARDY Electronics Ltd for more information.

Automatic loading of keys from User Smart-Card

By programming parameter 8 to 1 or 2 is it possible to get automatic load and reload of keys when a User Smart-Card is inserted or deleted. When parameter 8 is 1 an encryption key from the User Smart-Card will be loaded automatically to the encryption processor when the User Smart-Card is inserted. Observe that this function requires that a reference to the key that is to be loaded automatically is programmed on the User Smart-Card. This reference can be changed by pressing 'SHIFT'+ '5' with a User Smart-Card inserted and parameter 8 set to 1 or 2.

When parameter 8 is set to 2 the previous loaded encryption key will be reloaded when the User Smart-Card is deleted.

For more information about this function contact ARDY Electronics Ltd.

1.2.6 ERROR MESSAGES

After Power On

Error Message	Cause of Error	Action
HARDWARE ERROR CALL FOR SERVICE	Self test routine detects hardware errors.	Contact ARDY Electronics for service.
SV Card Required Turn Power OFF!	Internal encryption data is corrupted.	Turn Power off and contact ARDY Electronics for service.
SV Card Required	Internal encryption data is corrupted.	Contact ARDY Electronics for service.

When the above messages appear on the display you have to send your SLF2000XE to ARDY Electronics for service.

The self test routine will in some cases give you more information about the error with the message:

Self test Running FAILED: XX

Where XX is a hexadecimal combination of the following errors:

Error Code	Hardware Failure
80	Ram memory failure
40	Modem circuit 1 failure
20	Modem circuit 2 failure
10	Modem circuit 1 clock failure
08	Modem circuit 2 clock failure
04	Encryption processor failure

All error codes can be combined and the maximum error code is F8 (Hex).

During RECEIVING and TRANSMITTING of fax messages

Error Message	Cause of Error	Action
COMM. ERROR NO ANSWER	One of the faXes at the receiving or transmitting side does not answer.	Check the faXes.
COMM. ERROR NO MESSAGE	No message received or transmitted.	Check the encryption keys if the fax was to be encrypted, or try again.

During KEYBOARD Operation

If you press the wrong keys when you eXecute a command the display will show:

ENCRYPTION = OFF
OPERATOR ERROR

Action: Read the User Manual about the command you want to eXecute, or try again - maybe you just used the wrong keys.

Other possible errors during KEYBOARD operation are:

Error Message	Cause of Error	Action
ENTER PASSWORD INVALID	The entered password is not correct.	Activate the wanted command once again and enter the correct password.
ENCRYPTION = OFF LOAD NOT ALLOWED	You have tried to load a key when the 10 minute lock is active.	Wait until the 10 minute lock disappears.
ENCRYPTION = OFF KEY LOAD FAILURE	The encryption processor failed to load the wanted key.	Try again, if the error is shown every time you want to load a key contact ARDY Electronics for service.
ENCRYPTION = OFF NOT PROGRAMMED	The short key you tried to load is not programmed.	Load a programmed short key, or program the short key before you try to load it.

When Smart-Card is inserted

Error Message	Cause of Error	Action
SMART-CARD INVALID	The inserted Smart Card doesn't answer correctly.	Your card is not correct. Contact ARDY Electronics.
SMART-CARD CARD LOCKED	The card is locked.	Contact the Security officer or ARDY Electronics.
SMART-CARD INVALID = XXX	Wrong Card, XXX is an error code that is telling more about the error.	See error code list below.

Error Codes for Master Smart-Card

Error Code	Description of Error
001	Invalid Version - Card version and SLF2000XE version incompatible.
002	Invalid MASTER - The Master Card inserted have different identity than the card which activated the system
032	Invalid application-code. The Card is not a Master Card
048-063	The Card doesn't answer correctly.
128-255	Initialisation of card is bad

Error codes higher then 32 are fatal, if such error codes
appear please contact ARDY Electronics.

Error Codes for User Smart-Card

Error Code	Description of Error
001	Invalid Version - Card version and SLF2000XE version incompatible.
006	The submitted UAP is wrong
009	The card is initiated with wrong Master identity and will not work in this system.
032	The card is not a User Card.
128-255	Initialisation of card is bad

Error codes not shown above, or error codes higher then 32 are fatal,
please contact ARDY Electronics.

Errors when Smart-Card command is used

To be able to use the different Smart-Card commands it is necessary that the Card is accepted when it is inserted.

But even if the Card is accepted it is possible that some errors occur during the use of the Card.

Command "Activation ON/OFF" with Master Smart-Card

If the card inserted is accepted as a Master Smart-Card it should be no errors when the encryption is activated (Activation=ON) or deactivated (Activation=OFF).

But it is possible that an error code of the form:

Activation = OFF
FAILED = XXX

is shown on the display. All errors during activation is regarded as fatal, please contact ARDY Electronics if a message like above is displayed.

Command "Number of keys" with User Smart-Card

When this command is used it is possible that an error message as this is displayed:

SMART-CARD
INVALID = XXX

All error codes, except 006 which is the error code for wrong UAP, are regarded as fatal. Please contact ARDY Electronics if such error code is shown.

Command "Load 10 Keys" with User Smart-Card

When this command is used it is possible that an error message as this is displayed:

LOAD 10 SH KEYS
KEY Err: YY/XXX

The meaning of the different error codes are:

Error Code(YY)	Description of Error
01	XXX describes the error. XXX has the same meaning as error codes when the card is inserted. (The only error that should be shown is XXX=006 => Wrong UAP.)
06	The key that you want to load is not programmed. XXX shows the number of keys on the card.
08	XXX is always 255. The key on the card is not correctly programmed. Contact ARDY Electronics!

All other error codes then those above are regarded as fatal; please contact ARDY Electronics if such errors occur.

Command "GET KEY" with User Smart-Card

The error codes shown for this command are the same as the ones shown for the previous command (LOAD 10 SH KEYS).

Command "STORE SHORT KEYS" with User Smart-Card

After the initial message:

STORE SHORT KEYS CHECKING - WAIT!

It is possible that an error message like this is shown:

STORE SHORT KEYS Chk Err: YY/XXX

The meaning of the different error codes are:

Error Code(YY)	Description of Error
01	All 10 short keys are not programmed; XXX shows the number of the first un-programmed short key.
04	The card is in the state XXX numbers of PIN errors. This command only works when the card is in the state 0 errors. Reinsert the card and give the correct UAP.
12	There is no room one the card to store 10 keys. (XXX shows the number of the 10: th key to be stored).

If any other error occurs during the check please contact ARDY Electronics, since all other errors are fatal.

When the short keys are programmed on the Smart-Card it is possible that the error message below will be displayed:

STORE SHORT KEYS Str Err: YY/XXX
--

The meaning of the error codes are:

Error Code(YY)	Description of Error
01	XXX describes the error. XXX has the same meaning as error codes when the card is inserted. (The only error that should be shown is XXX=006 => Wrong UAP.)
02	Error when the key is programmed. Contact ARDY Electronics.

Other Error Messages

If any other Error Message than those shown earlier is displayed, please contact ARDY Electronics since any such error is fatal.

1.2.7 OTHER DATA

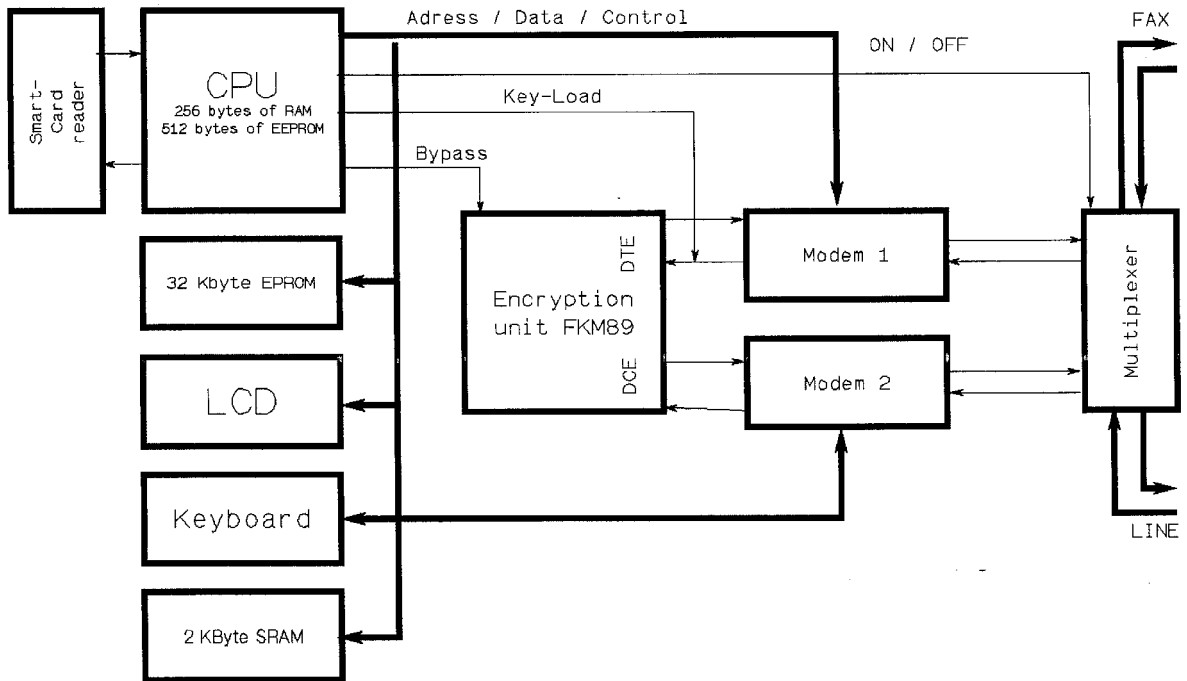
Power supply

The main power for Version 3.1 and later is 110 - 240V 50/60 Hz. Make sure that the main power is correct and for safe operation the system shall be connected to ground.

Fuse

The main fuse is 2 Amp T (surface mounted).

Principal diagram



1.2.8 QUICK GUIDE SLF-2000Xe

Quick guide Master Smart-Card

Insert the Master card to the SLF2000XE and follow the below functions.



SHIFT + SECURE + SECURE	System activation ON/OFF
SHIFT + 0	Not Used
SHIFT + 1	Not Used
SHIFT + 2	Not Used
SHIFT + 3	Change of Password
SHIFT + 4 + 4	Password ON/OFF
SHIFT + 5	Not Used
SHIFT + 6	Not Used
SHIFT + 7	User Card Stop Codes (10 cards)
SHIFT + 8	System Security Function Parameter Settings
SHIFT + 9	Not Used

**System Security Function Parameter Settings:
SHIFT + 8**

Parameter programming using the keyboard

0 = Change parameter

9 = Change value

SHIFT = Store value

SECURE = Quit setup

000 = Encryption keys on display
Value 0 = show as characters
Value 1 = show as "**"

Parameter = 000 Value = 0-1

001 = Password on display
Value 0 = show as characters
Value 1 = show as "**"

Parameter = 001 Value = 0-1

002 = Encryption ON/OFF mode

Parameter = 002 Value = 0-7

Value	Power On	Encryption ON/OFF Function
0	Encryption OFF	User Smart-Card ON,time-out to OFF.
1	Encryption OFF	Manual ON with time-out to OFF
2	Encryption ON	Manual OFF with time-out to ON
3	Encryption OFF	Manual ON/OFF, No time-out
4	Encryption ON	Manual ON/OFF, No time-out
5	Encryption ON	Only ON allowed
6	Encryption OFF	Only OFF allowed
7	NO Transmission	User Smart Card ON/OFF, time out.

003 = Encryption text ON/OFF mode
 0 = no fax is marked
 1 = Encrypted fax is marked
 2 = Not encrypted fax is marked
 3 = Both 1 & 2 above

Parameter = 003
 Value = 0-3

004 = User assigned Pin code
 0 = UAP not required
 1 = UAP required

Parameter = 004
 Value = 0-1

005 = Don't change ! (Modem levels)
 006 = Don't change ! (Modem levels)
 007 = Don't change ! (Modem levels)

008 = Automatic load/reload of keys
 0 = No automatic load
 1 = Automatic load of encryption key from User Smart-Card to encryption processor.
 2 = As 1 above but with reload of old encryption key when the user card is deleted.

Parameter = 008
 Value = 0-2

009 = Automatic choice of encryption ON/OFF during transmission.
 0 = No automatic ON/OFF function
 1 = Automatic choice possible when ENCRYPTION = AUTO.
 2 = As 1 above, but the same Master Smart-Card identity required in the receiving and transmitting system to turn encryption ON.

Parameter = 009
 Value = 0-2

When this AUTO function is set to 1 or 2 the Encryption ON/OFF modes (parameter 002) will get the following functions:

<u>Value</u>	<u>Power On</u>	<u>Encryption ON/OFF/AUTO Function</u>
0	AUTO	User Smart-Card ON Manual ON & OFF, time-out to AUTO
1	AUTO	Manual ON & OFF, time-out to AUTO
2	ON	Manual AUTO & OFF with time-out to ON
3	AUTO	Manual ON/OFF No time-out
4	ON	Manual ON/OFF No time-out
5	ON	Only ON allowed
6	AUTO	Only OFF & AUTO allowed OFF with time-out to AUTO
7	No Transmission	User Smart Card, Manual ON/OFF

010 = Marking of CSI-string when fax is sent encrypted.
 0 = CSI-string not marked
 1 = CSI-string marked with 'E' or 'I' in all empty positions when a fax message is sent encrypted or in the IDF mode.

Parameter = 010 Value = 0-1

011 = IDF-2000 Compatibility
 0 = The system is not able to work like an IDF-2000.
 1 = IDF-2000 mode available.

Parameter = 011 Value = 0-1

Quick guide for User Smart-Card

Insert the User Card to the SLF2000XE and follow the below functions.

SHIFT + 3	Show how many encryption keys that are stored on the Smart-Card
SHIFT + 4 + 4	Download 10 encryption keys from the Smart-Card to the System Memory.
SHIFT + 5...5	If auto load is chosen with the Master-Card (para. 008 = 1 or 2) it is possible to change the key to be loaded automatically with this command.
SHIFT + 6	Download 1 encryption key from the Smart-Card direct to the encryption processor (00-99).
SHIFT + 7	Verify the loaded key (00-99).
SHIFT + 8 + 8	Store 10 encryption keys from the Systems Memory to the Smart-Card.

Quick guide for use of the System Memory

These commands do not need any smart card to be installed to the SLF2000XE unit.

SHIFT + 5	Input 1 complete encryption key to one of the 10 positions in the System Memory (short key 0-9).
SHIFT + 6	Download 1 encryption keys from the System Memory to the encryption processor (0-9).
SHIFT + 7	Verify the loaded short key (0-9).

Quick guide for other commands

SHIFT + 1	Input of encryption key from the keyboard direct to the encryption processor (30 characters).
SHIFT + 2	Erasure of all encryption keys in the System Memory and in the encryption processor. Not in Smart-Card.
SECURE	Encryption ON/OFF/AUTO
SHIFT + SECURE	IDF-2000 mode (para. 011 must be set to 1)

-

Appendix 1

User-Card required for transmission

If parameter 2 is set to 7 the SLF2000XE system require an inserted User-Card to allow transmission. When parameter 002 is set to 7 the display will show:

ENCRYPTION = OFF
Insert USER Card

In this state it is not possible to transmit any fax messages without inserting a User-Card; if the user tries to transmit a fax message the SLF2000XE system will abort the transmission.

The SLF2000XE system receives fax messages as normal in this state.

When a valid User-Card is inserted the SLF2000XE turns ENCRYPTION ON and allows transmission, the user has the possibility to turn off the ENCRYPTION by pressing the 'SECURE' key as normal.

When a fax message has been transmitted, or after 5 minutes, the SLF2000XE will return to the state above ('Insert USER Card'). To send a new fax message the user has to reinsert the User-Card.

User-Card stop-codes

It is possible to block up to 10 different User-Card to use a specific SLF2000XE system. This is done by inserting a valid Master-Card and pressing 'SHIFT' + '7', the display will then show:

USER STOP CODES
CODE[0]:=----

If the stop-code is un-programmed it is indicated with '----', if the stop-code is programmed this is indicated with 'CODE [0]:=XYZW'. XYZW is the User-Card serial-number which is shown on the display when the card is inserted.

To see the next stop-code press '0'. The stop-codes are numbered 0 to 9.

If you like to change a stop-code press the 'SHIFT'-key, the display will then show:

```
USER STOP CODES
CODE[0]:=-----
```

This is the User Stop-code edit-mode which is indicated by a line under the current serial number digit position. If you enter the 4 digits of the serial-number you want to block the display will show:

```
USER STOP CODES
CODE[0]:=XYZW
```

and the User-Card with serial-number XYZW will not be valid in the SLF2000XE system.

If you want to erase a stop-code press 'SHIFT' while you are in the User Stop-code edit-mode.

The 'USER STOP CODES' -mode is finished by pressing 'SECURE'.

When a User-Card is in the stop-code list you will get the message 'INVALID = 011' if the User-card is inserted.

1.3 Encryption Key Management / Manual / Smart Cards



It is of most importance that the Key Management is handled with great care. The encryption keys shall be not be exposed to anyone and can for the SLF2000 system is done in 2 different ways.

The encryption keys can be entered from the keyboard or loaded from a Smart-Card. Each encryption key with manual input is 30 characters long and for Smart Cards 480 bits long.

The system can store 10 keys in its System Memory as short keys (0-9).

For safety these encryption keys can be put in to the system by two different persons, who each knows a part of the total characters.

The 10 short keys can then also be loaded from the Smart-Card.

The user then only loads one of the 10 different encryption keys into the encryption processor according to a preplanned schedule.

The security officer shall have an emergency plan for fast change of encryption keys in all encryption systems. This is in case any system disappears from its normal location. The encryption system shall be located at a safe place and not exposed to un-authorized people.

In case of emergency all the encryption keys can be zeroized from the system keyboard, just press the keyboard 'SHIFT' and 'KEY ZEROIZE' (followed by password, if required) and the 'KEY ZEROIZE' once again to confirm the destruction of all the keys. All loaded keys will be destroyed, including the 10 short keys.

Key Management over view.



Manual Key Management

For input of encryption keys directly to the encryption processor press **'SHIFT' followed by 'KEY ENTRY' (1)**. The display will then show (after password entry, if the password function is ON):

KEY ENTRY No1:

Now input the first 10 characters of the key from the keyboard, allowed characters is 0-9. After the first 10 characters the display will show:

KEY ENTRY No2:

Enter the next 10 characters of the key. And when the display shows 'No3:' on line 2, enter the last 10 characters of the key. The encryption

unit will then load the key to the encryption processor, this is indicated with:

KEY ENTRY
LOADING KEY

It is only possible to load 3 encryption keys within 10 minutes. If the 10 minute lock is active the display shows:

ENCRYPTION = OFF
(* READY *)

If the operator tries to load new encryption keys when the 10 minute lock is active the display shows:

KEY ENTRY
LOAD NOT ALLOWED

After 10 minutes has passed the display will show:

ENCRYPTION = OFF
READY

and new encryption keys can be downloaded to the encryption processor again.

KEY ZEROIZE

If short keys and encryption keys have to be erased and destroyed, press **'SHIFT' and 'KEY ZEROIZE' (2)**, The display will then show (after password entry, if the password function is ON):

KEYS ZEROIZE
CONFIRM

If you confirm the command by pressing **'KEY ZEROIZE'** once again the display will show:

KEYS ZEROIZE
ZEROIZING KEYS

After this all stored keys will be erased, and the security officer has to load new encryption keys and short keys to the system.

ENTER Short KEY

For input of short keys press **'SHIFT' and then 'ENTER SH KEY' (5)**. The display will then show (after password entry, if the password function is ON):

SH KEY ENTRY:_

Now put in the number of the short key to program (0-9) and then the 30 characters in the key.
After all 30 characters in the key have been entered the display will show:

SH KEY ENTRY:X
UPDATING SH KEY

Now the operator has stored one short key that later can be loaded to the encryption processor.

GET Short KEY

For loading of stored short keys to the encryption processor press **'SHIFT' and 'GET SH KEY' (6)**. The display will then show:

GET SH KEY:_
Prg: 0123456789

The numbers in line 2 of the displays shows which of the short keys that is programmed. If some or all of the numbers in line 2 isn't shown on the display that indicate that these short keys are not programmed.

Now the operator has to choose one of the ten short keys (0-9) to be loaded to the encryption processor.

If the chosen short key has not been programmed the display shows:

ENCRYPTION = OFF
NOT PROGRAMMED

If the chosen short key is stored in the short key memory the system loads the key to the encryption processor, and the display then shows:

GET SH KEY:X
LOADING KEY

Observe that if the 10 minute lock is active it is not possible to load encryption keys to the encryption processor. The display will then show:

ENCRYPTION = OFF
LOAD NOT ALLOWED

Wait until the display shows:

ENCRYPTION=OFF
READY

now a new short key can be loaded to the encryption processor.

CONTROL SHort KEY

If the operator wants to control which short key that is loaded (if any) to the encryption processor, press '**SHIFT**' and '**CONTROL SH KEY**' (7). The display will then show:

SH KEY CONT.:_

Now choose which short key you would like to control (0-9). If the chosen short key has been loaded to the encryption processor the display shows:

SH KEY CONT.:X
KEY MATCH OK

If the chosen short key has not been loaded the display will show:

SH KEY CONT.:X
KEY MATCH FAIL

Observe that this function only control the chosen short key and never controls the actual encryption key.

Smart Card Key Management.

User Smart-Card is used for storage and distribution of encryption keys. When new User Smart Cards are delivered it has no keys stored. There is two ways to generate keys to be stored on the User Smart-Card, manual or automatic.

With the normal SLF2000XE encryption system it is only possible to store keys manually or load the 10 short key into a Users Smart Card, if you want to generate and store keys automatically please use the KEY LOADER unit supplied by ARDY Electronics Ltd.

During the use of User Smart-Card you will have to enter the Password or the **User Assigned Pin** (if **UAP** is programmed) to be able to load and store data from/to the card. The UAP question:

UAP (5) ENTRY
No: _

When this question is shown on the display always enter the correct UAP, otherwise the command will be aborted with an error message displayed. As mentioned earlier the card will **become locked if you give the wrong UAP three times in a row.**

When you insert a User Smart-Card in a SLF2000XE encryption system the display will show:

SMART-CARD

If the card has UAP programmed you will then get the UAP question as told above. Enter the correct UAP and the display will show (if UAP is not programmed this message will be shown without any UAP input):

SMART-CARD
VALID

If the User Smart-Card is invalid for some reason, or if you give the wrong UAP the display will show:

SMART-CARD
INVALID =XXX

If the User Smart-Card is accepted the display will show:

ENCRYPTION = OFF
==>READY:XYZW<==

This is an indication from the SLF2000XE that the card inserted is a valid User Smart-Card. You have to have this message on the display before it is possible to use the different functions supplied for the User Smart-Card. The "XYZW" is the four least significant digits in the User Card serial number.

These four digits will be transmitted as a part of the fax messages if the fax is encrypted and the message "XYZW= CARD ID *** ENCRYPTED by ARDY *** " is turned on. The four digits can also be programmed with an 8 character word for identification of the sending person.



BAN DEMO = CARD ID * ENCRYPTED by ARDY *****

Number of keys on the Card

If you want to know how many keys that are stored on the User Smart-Card press 'SHIFT' followed by '3' with the valid User Smart-Card inserted. The display will then show (after UAP input if required):

SMART-CARD
No of keys: 030

This is telling you that the inserted User Smart-Card has 30 keys stored. Since the keys always begin with key no. 00 the existing keys on this particular card has the numbers 00-29. Each card can store 100 keys.

Load 10 Keys from Smart-Card to Short-key memory

It is possible to load 10 consecutive keys from the User Smart-Card to the SLF2000XE permanent short-key memory. This is done by pressing '**SHIFT**' + '**4**', the display will then show (after UAP or Password input):

LOAD 10 SH KEYS
From: _

Enter the number of the first User-Card key to store in Short-key memory 0. For instance key no 10, the display will then show:

LOAD 10 SH KEYS
From: 10 to 19?

This question asks you to confirm that key no 10 - 19 on the User-Card will be stored as Short-Key no 0-9 in the SLF2000XE Short-Key memory. If you **confirm by pressing '4'** the SLF2000XE encryption system will start to load keys from the User-Card to its internal short-key memory. Please note that the programming of Short keys is done backwards, starting by loading key 19 from the card and program Short-key 9. This is indicated on the display with:

LOAD 10 SH KEYS
Programming:09

The digits will then count backwards until it reaches '00' and then end with a 'OK'. Now all 10 Short-Keys are programmed with keys from the User Smart-Card. If you get any Error Messages during this command please see Users Manual section Error Messages for more information.

GET KEY from User Smart-Card

For loading of keys stored on the User Smart-Card to the encryption processor press '**SHIFT**' and '**GET SH KEY**' (**6**) The display will then show (after UAP or Password input):

SMART-CARD
GET KEY No: _

Enter the number of the key that you want to load to the encryption processor (2 digits from 00-99). The display will then show:

SMART-CARD
RECEIVING SH KEY

If you get any Error messages after the previous shown message consult section Error Messages in the user manual for more information.

If the load was successful the display will show:

SMART-CARD
LOADING KEY

If the 10 minute lock is active the display will show:

ENCRYPTION = OFF
LOAD NOT ALLOWED

When the 10 minute lock is active this is indicated on the display by:

ENCRYPTION = OFF
=(*READY:XYZW*)=

when the User Smart-Card is inserted. After 10 minutes has passed the display will show:

ENCRYPTION = OFF
==>READY:XYZW<==

now a new Smart-Card key can be downloaded to the encryption processor.

CONTROL Smart-Card Key

If a key is loaded from the User Smart-Card with the GET KEY command it is possible to verify which key that is loaded. Press **'SHIFT'** and **'CONTROL SH KEY' (7)**. The display will then show:

SMART-CARD
CONT KEY No: _

Now choose which Smart-Card key you would like to control (00-99). If the chosen Smart-Card key has been loaded to the encryption processor the display shows:

SMART-CARD
KEY MATCH OK

If the chosen Smart-Card key has not been loaded the display will show:

SMART-CARD
KEY MATCH FAIL

Observe that this function only control the chosen Smart-Card key number and never controls the actual encryption key.

STORE SHORT KEYS to User Smart-Card

If all 10 short keys are programmed in the encryption systems short-key memory it is possible to store these 10 keys on the User Smart-Card. The use of this command requires that all 10 short keys are programmed and that the inserted User Smart-Card has at least 10 un-programmed Card keys. You activate the command by pressing '**SHIFT**' + '**8**', the display will then show:

STORE SHORT KEYS
CHECKING - WAIT!

The SLF2000XE is then performing a check that all 10 short keys are programmed and that there is at least 10 un-programmed keys on the User Smart-Card. If the check was successful the display will show

STORE SHORT KEYS
As: 030-039?

This question asks you to confirm the programming of the keys number 030 to 039 on the User Smart-Card with the contents of short key number 0-9.

You **confirm the programming by pressing '8'**. The display will then show (after UAP input if required):

STORE SHORT KEYS
Programming:030

The digits will then count upwards until the last key is programmed (39), the message on the display will end with 'Programming: No' when the SLF2000XE sends the command to update the number of stored keys to the card.

The 10 short-keys is now stored as key no 30 (short-key 0) to no 39 (short-key no 9) in the User Smart-Card.

By using the ENTER Short KEY command and this command it is possible for the User to store his own keys on the User Smart-Card. It is also possible to copy keys from one card to another by first using the command (LOAD 10 SH KEYS), and then this command.

The SLF2000XE encryption system always store keys to the first free location on the card (key no 30 in the previous example). It is not possible to erase any keys on the User Smart-Card without using the KEY LOADER unit supplied by ARDY Electronics. Contact ARDY Electronics Ltd for more information.

Automatic loading of keys from User Smart-Card

By programming parameter 008 to 1 or 2 is it possible to get automatic load and reload of keys when a User Smart-Card is inserted or deleted. When parameter 008 is set to 1 an encryption key from the User Smart-Card will be loaded automatically to the encryption processor when the User Smart-Card is inserted. Observe that this function requires that a reference to the key that is to be loaded automatically is programmed on the User Smart-Card. This reference can be changed by pressing '**SHIFT**' + '**5**' with a User Smart-Card inserted and parameter 008 set to 1 or 2.

When parameter 008 is set to 2 the previous loaded encryption key will be reloaded when the User Smart-Card is deleted.

For more information about this function contact ARDY Electronics Ltd.

1.4 Encryption Key Distribution Methods



The distribution of encryption keys to the different locations have to be secure. The most secure way to distribute and reload encryption keys is if the persons doing this doesn't know the keys.

Manual Key distribution

Distribution of encryption keys can be done manually by a person travelling to the different locations and loading the keys manually into the encryption processor or into the System Memory with 10 complete encryption keys.

If the manual loading of encryption keys shall be more secure it is required for two different persons to input the manual key from the keyboard. One person can then input 20 characters and the other person 10 characters for each key. With this method one complete encryption key is never known by the same person.

Smart Card Key distribution.

To distribute encryption keys with no person knowledge of the keys, User Smart Card shall be used. One User Smart Card can be programmed with 10 encryption keys direct from the SLF2000XE System Memory. This smart card can then be distributed to each location for input of the 10 encryption keys into each SLF2000XE system. With this method it is not necessary to keep the User Smart Card at each location, only one User Smart Card can be used to load 10 encryption keys into all SLF2000XE systems.

The User Smart Card can also be used to store up to 100 encryption keys. These 100 keys can be generated with the Key Loader System KL2000 and stored into the User Smart Card. With this method of generating keys and store these keys into the User Smart Card it is not possible for the user to know the encryption keys.

The User Smart Card can be used to store up to 100 encryption keys and also be used as authentication method with the personal pin code (UAP).

The User Smart Cards can be protected with a personal Pin Code (UAP) and if a User Smart Card is lost it is only possible to try the UAP code three times before the card is locked. The only possibility to unlock a User Smart Card is to use a Key Loader System KL2000 and to know the correct UAP code.

When the User Smart Card is used for authentication all the transmitted fax pages are marked with the users numeric or alphanumeric identification number or name. In this case all the users need one User Smart Card each. If these User Smart Card shall include encryption keys or not is up the local Security Officer to decide.

1.5 Installation of SLF2000XE Telefax Encryption System

Power Supply

The main power for Version 2.9 and after is 240 Volt / 50 Hz (optional 110V / 50 Hz).

Make sure that the main power is 240V, and for safe operation connect the system to ground.

Activation of the System



When the system is delivered it is not activated with the Master Smart-Card. When the power is turned on the display will show:

Activation = OFF
Insert MSTR Card

Observe that this message will be displayed if the initial self test is passed; if any other message is displayed consult ARDY Electronics.

Put in the Master Smart-Card and wait until the display shows:

SMART-CARD
VALID

This message is a confirmation from the system that the inserted Master Smart-Card is valid. After this message the SLF2000XE unit is ready to accept commands from the keyboard and the display will show:

Activation = OFF
LOADING DATA

Older versions of the system will show:

If you want to activate the system push 'SHIFT' followed by 'SECURE', the display will now show:

Activation = OFF
CONFIRM

To confirm the activation of the system press 'SECURE' once again and the display will show

For versions after V 2:13 the information will be automatically loaded into the system and show

Activation = OFF
LOADING DATA

While the system loads data from the Master Smart-Card. If the loading was successful the display will show

Activation = ON
READY

after a short while. After this the system is activated and can be used by the operator. For further information about the set-up possibilities with the Master Smart-Card see Users Manual section Master Smart-Card, or the Quick Guide for SLF2000XE Master Smart Cards.

If you get any Error messages, such as

SMART-CARD
INVALID = 032

consult section Error Messages in the Users manual for more information about the error.

After the activation of the system you shall take out the Master Smart-Card and keep it secure.

If you send the system to other locations you must deactivate the system with the Master Smart-Card. If the system disappears during transportation it can not be used by anyone before it is activated again.

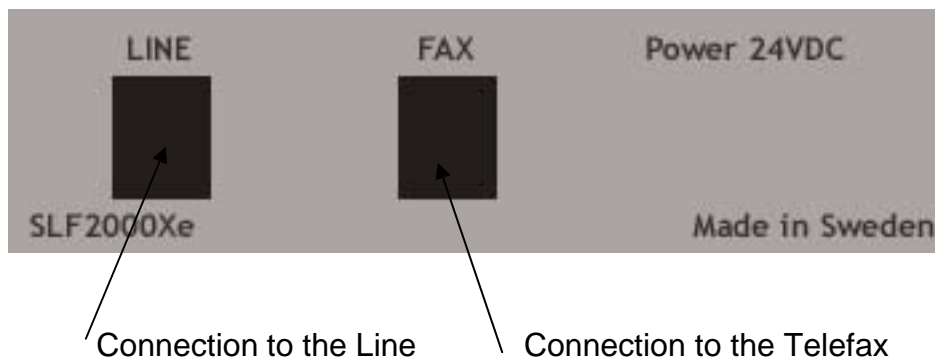
If you like to deactivate the system (Activation = OFF) proceed in the same manner as described above.

E.g. insert Master Smart-Card and press 'SHIFT' + 'SECURE' + 'SECURE' and the display will show:

Activation = OFF
READY

The system is now deactivated and you can take out your Master Smart-Card.

Line installation



Disconnect the telefax terminal from the telephone line and install the encryption system to the line by connecting the telephone-cord to the socket marked 'LINE' on the back of the encryption system. Connect the telefax terminal to the socket marked 'FAX'.

The modular connector is of the model 6/4 with the default connection to the two middle poles. If other connections are required consult ARDY Electronics Ltd for how to change the default connection.

To test if the installation is correct just lift the hook on the telefax terminal and wait for the line connect tone. If you can hear the tone the Encryption system is correctly installed.

If your line connect tone is 425 ± 15 Hz the SLF2000XE will display:

TRANSMITTING=OFF
DIAL TONE DETECT

If your line connect tone is any other frequency you will not get any message on the display when you lift the hook on the telefax terminal. Other frequencies then 425 ± 15 Hz will not interfere with the function of SLF2000XE, the only thing that will happened is that the message above will be missing.

Put the telefax terminal on-hook and wait until SLF2000XE shows:

ENCRYPTION = OFF
READY

Installation of Encryption keys.

The SLF2000XE is now ready to operate in NOT Encrypted mode, to be able to transmit and receive encrypted fax messages the operator need to install encryption keys.

Use the **Manual mode** or the **User Smart Card** to load the encryption keys. See Encryption Key management section above.

1.6 Configuration with Master Smart Card

Master Smart-Card

The Master Smart-Card is used to activate and deactivate the system. With the Master Smart-Card it is also possible to configure the system in different ways.

Activation and Deactivation of the system

Activation and deactivation is described earlier in this manual, see Users Manual section Activation and deactivation.

When the system is activated data from the Master Smart-Card is loaded in the encryption systems permanent memory. The configuration of the system will be put into default state when it is activated. Each Master Smart Card can be programmed by Ardy Electronics Ltd to have different default settings according to the customers need.

It is also possible to change the configuration of the system with the Master Smart Card after the SLF2000XE is activated, e.g. the display will show (with inserted and accepted Master-Smart Card):

Activation = ON
READY

Every Master Smart-Card has an identity; the identity code of the Master Smart-Card is a 4 digit code of the form '3XXX', where 'XXX' is Hexadecimal digits. If the system, for instance, is activated with a Master Smart-Card with identity '3009' you must have a Master Smart-Card with the same identity to deactivate the system. For more information about the Master Smart-Card consult ARDY Electronics Ltd.

Changing the Password

When the system is delivered the default password is '5555'. If you want to change the password you can do so without the Master Smart-Card if the old password is known.

If the old password is not known you have to put in a valid Master Smart-Card to be able to change it.

With a valid Master Smart-Card inserted, and Activation=ON, press '**SHIFT**' and then '**3**'. The display will then show:

ENTER PASSWORD
No: _

Enter the 5 digit password that you want the system to have.

After the first input of the password you have to verify the password before it is stored. The display will show:

VERIFY PASSWORD
No: _

Enter the password once again, if the password entered the second time is the same as the first one the password will be changed, and the display will show:

PASSWORD = ON
PASSWORD CHANGED

If the password entered the second time is different than the first one the password will not be changed and the display will show:

VERIFY PASSWORD
INVALID

Selecting Password ON or OFF

The password function is by default ON, but it is possible to turn it off with the Master Smart-Card inserted and with Activation = ON. To turn it OFF (or ON) press **'SHIFT' followed by '4'**, the display will then show:

PASSWORD = ON
CONFIRM

If you confirm the change of the password function press '4' once again, and the display will show:

PASSWORD = OFF

The password function is now turned OFF. To turn it on again proceed as above. E.g. **'SHIFT' + '4' + '4'** and the display will show:

PASSWORD = ON

Configuration of the System

The SLF2000XE encryption system has several different parameters that are programmable by the user. It is possible to change these parameters with the Master Smart-Card inserted and Activation = ON.

Every time the system is deactivated (Activation = OFF) and then activated again (Activation = ON) the parameters will be put in default state, according to the data programmed in the Master Smart-Card. It is possible to order Master Smart-Cards with different parameter values than those that are stated as default, contact ARDY Electronics Ltd for more information.

To change (or control) the parameter programming of the system press **'SHIFT' followed by '8'** with the Master Smart-Card inserted (and accepted) and with Activation = ON. The display will then show:

Parameter = 000
Value = 1

This is showing that Parameter 0 has the programmed value 1. If you want to **change the value press '9'** to step the parameter value to the wanted state. For instance, if you want parameter 0 to have the value 0 press '9' until the display shows:

Parameter = 000
Value = 0

To program this new value into the encryption systems permanent memory **press 'SHIFT'**, the display will then show:

Parameter = 000
Programming:0

The new value is now programmed!

To change the parameter press '0' until the display shows the parameter number you want to change. For instance if you want to **change parameter 003 press '0'** three times and the display will show:

Parameter = 003
Value = 1

Proceed as described above to change the parameter value. To end the Parameter programming routine press 'SECURE' (or wait for the keyboard time-out app. 30 seconds).

The parameter values have the following meanings:

Parameter	Value	Description of function
000	0	Input of keys shown as digits.
000	1	Input of keys shown as '*'-DEFAULT
001	0	Input of password shown as digits.
001	1	Input of password shown as '*'-DEFAULT
002	0-7	Encryption ON/OFF
003	0	Fax messages are not marked.
003	1	Transmitted Encrypted fax messages marked with: "*** ENCRYPTED by ARDY/SLF2000XE ***"
003	2	Received not encrypted fax messages marked with: "*** NOT ENCRYPTED ***"
003	3	Value 1 and 2 combined - DEFAULT
004	0	UAP not required on USERS card -DEFAULT
004	1	UAP required on USERS card.
005	0-3	Output level of MODEM - DEFAULT = 3 Don't change without consulting Ardy

006-7	0-255	Output level of MODEM; don't change without consulting Ardy
008	0-2	Automatic loading of keys. DEFAULT=0
009	0-2	Automatic ENCRYPTION=ON. DEFAULT=0.
010	0-1	0 => CSI Block not marked when transmitting encrypted faXes -DEFAULT 1 => See Users Manual
011	0-1	0 => The system will not be able to work like an IDF-2000 - DEFAULT 1 => IDF-2000 mode is available.

The programmed parameter values are stored in permanent memory and will not be lost during power failure.

To reset all parameters to the default state, deactivate the system (Activation = OFF), press 'SHIFT' + 'SECURE' + 'SECURE' with a valid Master Smart-Card inserted.

Then press 'SHIFT' + 'SECURE' + 'SECURE' once again to activate the system (Activation = ON) and load the default configuration from the Master Smart-Card.

1.7 Test of the Installation with Telefax machines

To test if the installation is correct just lift the hook on the telefax terminal and wait for the line connect tone. If you can hear the tone the Encryption system is correctly installed.

If your line connect tone is 425 ± 15 Hz the SLF2000XE will display:

TRANSMITTING=OFF DIAL TONE DETECT

If your line connect tone is any other frequency you will not get any message on the display when you lift the hook on the telefax terminal. Other frequencies than 425 ± 15 Hz will not interfere with the function of SLF2000XE, the only thing that will happened is that the message above will be missing.

Put the telefax terminal on-hook and wait until SLF2000XE shows:

ENCRYPTION = OFF READY

1.8 Configuration of SLF2000XE with User Smart Card

Using the User Smart-Card the first time

When the User Smart-Card is delivered it is, as mentioned above, "blank". When a "blank" User Smart Card is inserted in a SLF2000XE (with Activation = ON) the SLF2000XE will detect that the card is blank and give you the following question on the display:

Init USER Card?
Confirm (SECURE)

If you confirm this question by pressing 'SECURE' the SLF2000XE will program its Master Smart-Card identity on the User Smart-Card. (The Master Smart-Card identity is stored in the SLF2000XE when it is activated, Activation = ON.) Before you program the Master Smart-Card identity on the User Smart-Card it is not possible to use it.

After the programming of Master Smart-Card identity it is only possible to use the User Smart-Card in units that is activated by Master Smart-Card with the same identity as the one programmed on the User Smart-Card. While the programming is taking place the display will show:

SMART-CARD
Programming :ID

If the programming of the Master Smart-Card identity was successful (see Users Manual section Error Messages if you get an error) you will get a question on the display that will ask you if you want to program a User Assigned Pin (UAP) on the card:

Program UAP ?
Confirm (SECURE)

If the configuration of the system requires that every User Smart-Card should have an UAP programmed this question will not be displayed. Instead you will get the message that is shown below, the same message will be shown if you press 'SECURE' as a confirmation that you want to program the UAP:

UAP (5) ENTRY
No: _

Enter the 5 digits (0-9) that you want to have as UAP. After the first input you have to verify the input once again before the UAP is programmed, the verification question will be displayed as:

VERIFY UAP(5)
No: _

Enter the 5 digits in the UAP once again, if both the inputs are equal the UAP will be programmed; this is indicated on the display with:

SMART-CARD
Programming: UAP

If the both inputs are not equal the UAP will not be programmed and the display will show:

VERIFY UAP(5)
INVALID

IMPORTANT:

Programming of UAP can only be done once. If you forget your UAP and give the wrong UAP to the card 3 times the card will become locked. If you don't remember your UAP then the card will be unusable, since it is not possible to unlock a Card when you don't know the UAP.

It is possible to use User Smart-Card without UAP but it is not recommended. If you want to force every User to have User Smart-Card with programmed UAP, program parameter 004 to value 1.

If a User Smart-Card without an UAP is inserted in a SLF2000XE encryption system with parameter 004=1 you will always get the question:

Program UAP?
Confirm (SECURE)

And the card will not be accepted until an UAP is programmed.

1.9 Transmission of Not Encrypted and Encrypted fax message

Transmission of Not Encrypted fax messages.

To send an unencrypted telefax message the user first have to make sure that the SLF2000XE display show:

ENCRYPTION = OFF
READY

When the encryption function is OFF the user can transmit fax messages to any telefax machine as normal unprotected fax messages.

If the display shows Encryption ON the transmission will require an SLF2000XE encryption unit on the receiving side with the same encryption key loaded as on the transmitting side.

Transmission of Encrypted fax messages.

To send an encrypted telefax message the user first have to make sure that the SLF2000XE display show:

ENCRYPTION = ON
READY

If the display shows Encryption ON the transmission will require an SLF2000XE encryption unit on the receiving side with the same encryption key loaded as on the transmitting side.

When the encryption function is ON the user can transmit fax messages to any telefax machine with an installed SLF2000XE unit as an normal fax messages, but fully protected.

During the transmission of the telefax the operator can check the SLF2000XE display if the transmission is ENCRYPTED, the display shall then show:

TRANSMITTING=ON
V.29 9600 bps

End of SLF2000XE Manual.