User Instruction

Instructions about the
The Sec-Line GSM-2002/MW3026.

Ardy Electronics Ltd
P.O.Box 47
S-70140 Orebro Sweden
Phone: +46 19 247010
Fax: +46 19 247011
e-mail: info@ardy.se
www.ardyelectronics.com

GSM phone with encryption function

The Sec-Line GSM-2002/MW3026

The Sec-Line Phone 2002/MW3026 is a dual band GSM 900/1800, composed of a GSM phone equipped with an encryption function.

Plain communications are established, through the voice channel, either with or without the function. This means that the function does not interfere with plain communications.

Encrypted communications require the function to be connected to the GSM phone. The encrypted communication is then transmitted through the data channel provided by the local GSM service provider.

Using the 2002/MW3026 requires subscription on two services, voice services and data services along with their dedicated calling number. It means that one calling number is used for plain communication when the data calling number corresponds to the encrypted call only.

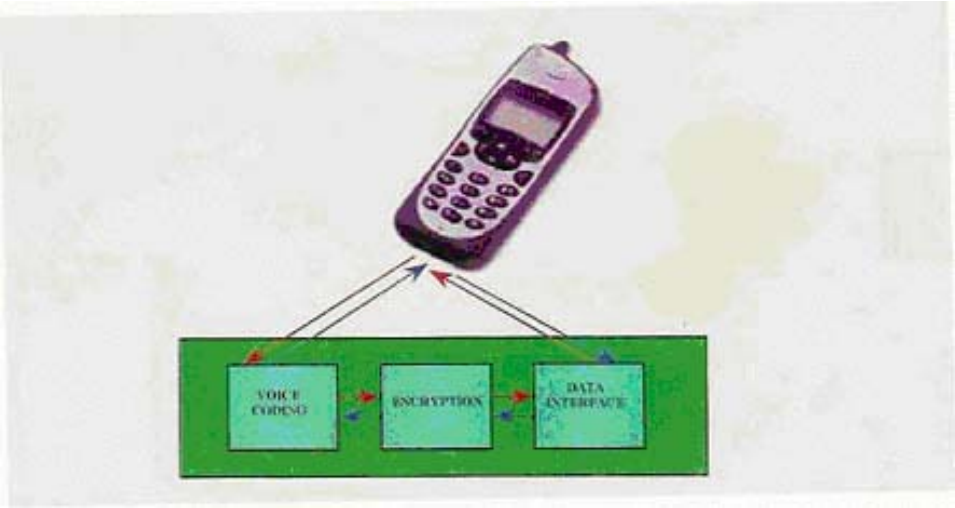
Before the transmission starts in data mode, the voice is digitised, then encrypted, finally transmitted through the data channel. The communication may be established between the two encrypted GSM phones, or from an encrypted GSM phone to a telephone equipped with the 2002/C500 base encryption telephone and reciprocally.

The main advantages of the solution offered by the 2002/MW3026 can be summarised as follows:

- Allow establishing plain communication as any GSM phone.
- Allow establishing encrypted communication.
- High security of encrypted communication by a 128-bit encryption key.
- High secure proprietary algorithm.
- Low cost solution, using the current GSM network infrastructure.
- Encrypted communication independent of the GSM network.
- Working worldwide on any GSM network.
- 900 MHz on GSM standard, 1800 MHz on DCS standard, [1]1900 MHz on PCS (USA and South America) standard, as well as dual standard 900 MHz and 1800 MHz are available.
- The traffic key management allows defining hierarchical cryptographic networks structure.
- New vocoding technology enhances the voice quality.
- As any GSM, easy to use, and operating procedures are user-friendly.

[1] Only available for purchase order over 2000 units.

Description of the encryption function:



Encryption function. (Figure 1)

The encryption function is inbuilt in the GSM phone, the encryption function as figure 1 is composed of:

- **The Vocoder**, which digitises the voice.
- **The encryption component** with a 128-bit encryption key and a proprietary algorithm.
- **The Data interface,** during transmission the encrypted digital signal coming from the data network through the GSM phone is sent to the encryption function, to be decrypted prior to be sent back to the GSM receiver.

Key Management.

Prior to any encrypted call, the voice signal is digitised then encrypted. The encrypted algorithm is using a 128-bit traffic encryption key. Keys are introduced locally by the means of a “Key Management System”. Keys are loaded into the function by using a personal desktop computer with the appropriate software called “ User Station”.

The User Station software allows renewing the traffic key(s) inside the encryption function, to reload the supervisor and user codes. Keys are stored ciphered in the encryption function. The encryption function is able to manage up to 100 network keys and has a unique base key. Key selection between encryption equipment is done automatically after negotiation of non-confidential key identifiers.

Sec-Line Base Phone 2002/C500

Sec-Line Base Phone 2002/C500 is placed under the connected telephone, the solution is based on the encryption equipment called 2002/C500.

The 2002/C500 unit is installed between the handset and the telephone. The choice of this type of connection has been designed with the concern to propose equipment independent of the telecom network.

The 2002/C500 unit secures voice communication on different type of telephones connected to either PSTN or ISDN networks. Moreover all available functions provided by a PBX are saved.

The 2002/C500 unit extern appearances consist in small box located under the telephone. A keyboard and a large graphic screen equip its front.

The 2002/C500 digitises the voice (vocoder), ciphers the bit stream, then a modem converts the digital signal into an analogue signal being able to be transmitted to the analogue network.

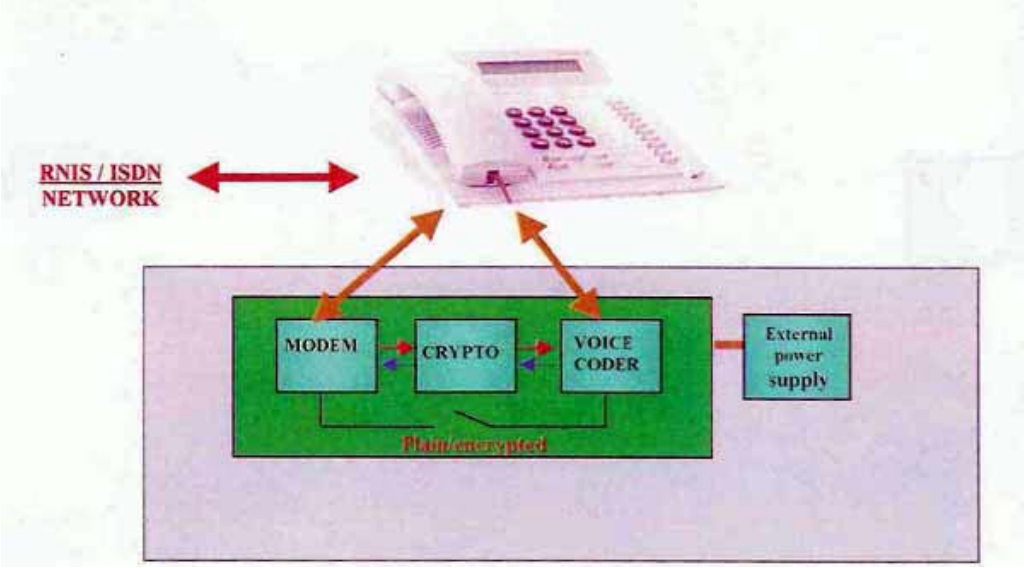
All man/machine interfaces with the standard telephone remains unchanged. However, the 2002/C500 is providing the user with the possibility to establish an encrypted communication, as well as a plain communication. The plain mode to encryption mode, and reciprocally, during the communication.

The main advantages of the 2002/C500 unit can be summarised as follows:

- Allows establishing plain as well as encrypted communication. During a plain communication, the user can switch from plain to encrypted communication and reciprocally. The 2002/C500 of the correspondent will automatically switch from plain to encrypted and reciprocally.
- Very High security of communication, by a 128-bit encryption key and a proprietary algorithm.
- Low cost solution.
- The unit can be connected to any current telephone equipment, does not require the replacing of the existing telephone sets.
- Independent of the network, it is offering an end-to-end high security for confidential communications.
- Works on PSTN and ISDN networks.
- Keeps available all functionality provided by the PBX.

- The traffic key management allows defining a hierarchical structure of the cryptographic network.
- Allows establishing encrypted communication with the 2002/MW3026 GSM phones type.
- New vocoding technology enhances the voice quality.
- Easy to use and operating procedures are user friendly.
- Reliable electronic design.
- Does not require and PTT approval.

Encryption System Description.



Function of the 2002/C500 system.

The 2002/C500 encryption system includes the following components:

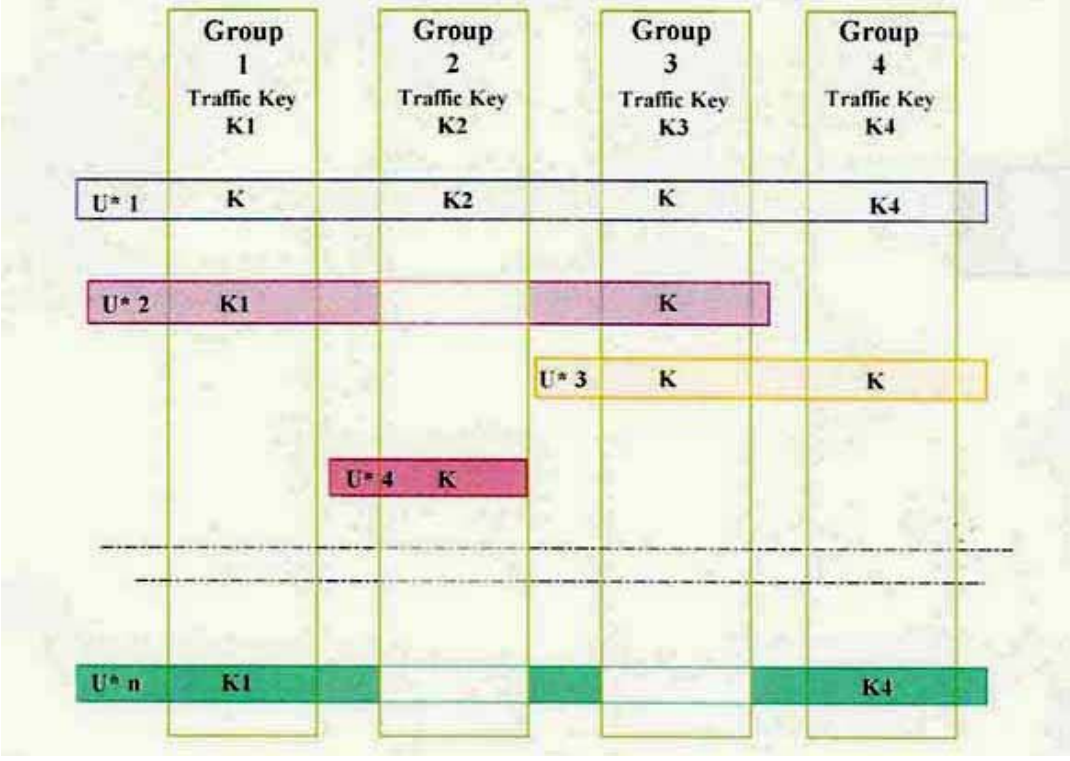
- **The Vocoder**; it digitises the voice signal,
- **The encryption unit**; which encrypts the digital signal.
- **The Modem**; it converts the digital signal to an analogue signal prior to transfer it to the network.

Key Management

Prior any encryption call the voice signal is digitised then encrypted. The encryption algorithm is using 128-bit encryption traffic key. Keys are loaded into the encryption component locally by the means of the “Key management System” Keys are also loaded by using a personal desktop computer with the appropriate software called “User Station”. The User Station software allows renewing the traffic key(s) inside the encryption function, to reload the supervisor and the user codes. Keys are stored ciphered in the encryption component.

The 2002/C500 unit memorises and handles up to 100 traffic keys, allowing the user to define up to 100 cryptographic networks. In addition, each system owns its unique base key. Key selection between the 2002/C500 units is done automatically after negotiation of non-confidential key identifiers.

Key Distribution.



Key distribution (U=Users, K= Keys)

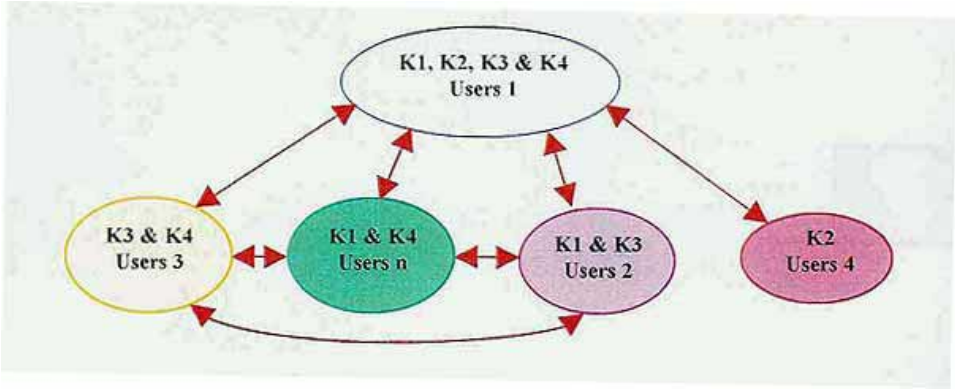
The encryption function for the GSM phone 2002/MW3026, as well as the 2002/C500 base unit (both called encryption devices) store traffic keys, allowing encrypted communication.

Each encryption device belongs to a given user. Each user belongs to one or several groups of users. A group is closed and dedicated to a specific entity: for instance a group can be dedicated to the Air Forces, of to the Navy, or to the Special Forces etc.

A user may be authorised to establish encrypted communication inside one group, or from one group to another. It means that the encryption device may be loaded with only one traffic key belonging to one group, or with several traffic keys corresponding to several groups. The figure above illustrates the structure of the groups and the distribution of the traffic keys to different users.

For instance, as showed on the figure above, the user 1 have an encryption device loaded with four traffic keys, corresponding to groups 1,2,3,4 allowing the user 1 to communicate in encrypted mode with the users of the four groups. User 4 have an encryption device with only one traffic key, they can communicate with the users of the same group2, however, they also are authorised to communicate with users 1 who have a common key.

From the above figure we define the corresponding cryptographic network as follows:



Cryptographic network

The security agent is in charge of defining the cryptographic network, by the means of the key management system called “Key Management System”.

Algorithm.

The proposed algorithm is a pseudo random generator based on set of non.-linear functions associated linear shift registers with maximum period feedback.

The traffic key length is 128 bits and allows 10^{38} values of key that avoids possibility of systematic tries. In addition a 64 bits message key is exchanged at each time communication, this key modifies the binary sequence issued from the same key.

The entropy of the traffic key is 128 bits. The cardinal (cardinal number) of the key is $3{,}4x10^{38}$, equivalent to 2^{128} combinations. The proprietary algorithm is using real 128 bits traffic key.

System Specifications.

End to end encryption on fixed and on GSM mobile phones.

The Encryption function 2002/MW3026 has been designed with the aim to provide an end-to-end encrypted communication over 900 MHz, 1800 MHz, 1900 MHz GSM networks. Independent of the network, the encrypted communication is established trough the data channel network. The 2002/C500 base unit has been designed for end-to-end communication over the PSTN/ISDN network and encrypted communication is established from an encrypted GSM phone and reciprocally. Through the ordinary network an encrypted communication is established from an encrypted GSM phone to a telephone base and reciprocally.

The 2002/MW3026 and 2002/C500 structure.

As shown on the picture of the 2002/MW3026 unit it is composed of two sub-assemblies; the mobile GSM phone and the encryption function. A shown on the picture of the 2002/C500 unit, it is a small box located under an ordinary telephone. It is connected between the handset and the base of the telephone. Independent of the line, the 2002/C500 can be used on PSTN as well as on ISDN lines. Moreover the method of its connection allows keeping all functionality provided by the PBX.

The proprietary algorithm (non published) developed, using a real 128-bit encryption key allows to encrypt the digitised signal of the voice. The same algorithm is used on both the 2002/MW3026 and the 2002/C500 systems. A common key loaded on the both side of the communication allows the establishment of an encrypted communication.

The 2002/MW3026 and 2002/C500 plain override facility.

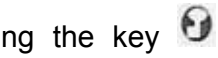
The 2002/MW3026 GSM mobile unit as any kind of GSM mobile phone allows communicating in plain mode with every other GSM phone with or without the encryption function connected. The 2002/C500 base unit is transparent during a plain communication.

Plain or Encrypted mode on the 2002/MW3026 GSM phone.

Easy to use, the encryption GSM phone offers different choices of the communication mode. The encryption mode in the GSM phone is set using the ENCRYPTION menu and may be in the following modes:

"By Default Encryption Mode"
The standard display of the GSM mobile phone shows: "CRYPTO", but pressing the key  makes it possible to switch alternately from encrypted mode to plain mode. After a plain mode communication, the encryption unit returns automatically to encryption mode after the phone call.

"On Request Encrypted Mode"
The standard display of the GSM Mobile phone shows "PLAIN", but pressing the key  makes it possible to switch alternately from plain mode to encrypted mode. After an encrypted mode communication, the encryption unit returns automatically to plain mode after the phone call.

"Systematic encryption".
In this mode the plain communication is not possible. The standby display of the GSM mobile phone shows "ENCRYPTION". Pressing the key  has no effect. Only encrypted communications are authorised.

Moreover, when the "On Request Encrypted Mode" is set, it is possible to perform a encrypted call by choosing an encryption telephone number memorised either in the memory, or in the redial memory without having to switch the encryption function from PLAIN mode to ENCRYPTED mode. Actually the encryption telephone number contains a "C" prefix, which automatically switches the encryption mode from PLAIN to ENCRYPTION. After the communication, the encryption units return automatically to plain mode.

When receiving a call the 2002/MW3026 GSM phone will be set automatically in PLAIN mode for a plain call, on ENCRYPTION mode for a encrypted call. If the encryption function is not connected to secure the GSM phone during an encrypted call the following message will be displayed:

"Crypto Call"
"Connect Your Crypto Unit"

The 2002/C500 base telephone unit.

Easy to use, the 2002/C500 unit will automatically switch to "CRYPTO" mode for any incoming encrypted communication. The 2002/C500 unit is transparent during plain communication.

During a plain communication, it is possible to switch at any time the communication from "PLAIN" mode to "CRYPTO" mode by pressing the key  the 2002/C500 of the correspondent will automatically switch to "CRYPTO" mode. It is also possible to switch an encrypted communication from "CRYPTO" mode to "PLAIN" mode without interrupting the communication. Calling encrypted GSM number will switch automatically the 2002/C500 unit to "CRYPTO" mode.

The 2002/MW3026 GSM phone unit.

Tamper proof security facility.

Two secret codes restrict the access to the encrypted communication. The access known by the user, is required prior any encrypted call, the security code, known only by the security supervisor, is required prior to display the security menu of the encryption function.

Prior delivery the encryption function is customised in the factory with default factory codes value. Prior using the secure GSM phone it is required to replace the access and security default codes by the user own codes. Among other functions, the "Key Management System" allows to manage these codes. The access and security default code values are confidential, they are sent separately from the equipment.

In addition the 2002/MW3026 GSM phone "LOCK K.PAD" feature allows locking the keypad to prevent any attempt of dialling.

Good Intelligibility and Good recognition at encryption Mode.

The encryption function is equipped with a very high quality level vocoder. It is working at 5600 bd (baud) with only 4800 bd are used for the digitalisation of the voice. The remaining 800 bd are used to correct error of the transmission.

Resistant to bit error.

In addition to the bit error correction of the encryption function, the GSM phone is equipped with bit error correction useful for plain communication.

Battery level & network status indicator.

The 2002/MW3026 GSM phone displays dynamically the status of the battery, moreover the user may choose to set the warning beep emits when the battery is low. In addition, the menu allows checking of the battery's voltage. A dynamic network status indicator displays permanently allows at any time to check the level of the signal of the base station of the GSM network.

Mobile lock code.

The 2002/MW3026 GSM phone includes several levels of security features. The PIN code which is usually the access code, after three wrong attempt, the encryption function will be locked, no more encrypted communication will be authorised. The PHONE CODE is a secret code designed to protect the GSM phone from theft. It is automatically linked to the SIM card.

Memory Battery back up.

The 2002/MW3026 GSM phone provides the user with a "SAVING MODE" feature. The mobile phone will be set to a special standby mode, thereby further increasing the available call time.

Vibrating Ringer.

It is possible to set the 2002/MW3026 GSM phone when receiving a call and/or message to vibrating mode. A wide variety of melodies are available (including a silent ringing) as well as a number of settings, including a crescendo.

Operator dependent services:

- Call forwarding
- Call restriction
- Short message, send, receive, multi send,
- Conference call
- Call waiting
- Call Hold
- Call ID
- Prepaid calls
- Advise of charge
- Fixed dialling
- Phase II approved
- EFR

Features.

- Dual band GSM900/1800
- Built in data /Fax modem
- Built in hands free speaker phone
- Vibrating device
- Easy message "T9"^{tm}
- Current converter
- Navigator Key
- International Access Key
- Two user programmable keys
- Directory of 100 numbers on the handset
- Alphabetic sorting of the phone book by name.
- Quick call function
- Phone book matching, (display the name of the caller).
- Memorisation of the last 20 numbers called.
- Graphic display
- Automatic redial
- Battery charge display
- Field level display
- Call during counter
- Direct access pull-down menus
- Keyboard locking
- Anti Theft code.
- Calculator, date, time, alarm, timer.
- Choice of language
- Volume and ringer tune adjustment
- Network led indicator.