Unpacking

Your CryptoPhone was packaged using several tamper-evident seals to ensure that nobody manipulated your device while it was in transit. Please take a minute to follow the security verification procedure outlined in the anti-tamper verification instructions that are placed above the CryptoPhone inside the carrying case. To open the carrying case, place it in front of you, so that the handle faces you. Then use a sharp knife to cut the seals. Now open the carrying case by lifting upwards the levers on the front. The levers are robust and at first use might require a bit of force to move. Inside the carrying case you will find your CryptoPhone packaged in a security sealed, transparent plastic film nested in the foam pad. Please also verify the plastic film and seal for tampering. The unevenness of the film and the seal are intentional and a method of individualization to make tampering harder. You can verify the authenticity with the Anti Tamper Verification procedure. You will also find the headset, desk stand, power supply, direct charge adaptor and headset ear clip in the carrying case. (carrying case •3•)
Behind the foam pad in the lid of the carrying case you will find the Admin Policy Password and other printed documentation. We recommend to store this manual in the lid behind the foam as well so it won't get lost.

General

Your CryptoPhone is based on a generic tri-band (900/1800/1900) GSM equipped PDA that is sold under different brands, and uses the PocketPC 2003 operating system. On this device, a few additional applications besides the necessary components for the CryptoPhone are installed, like an address book, a calendar and an unencrypted phone application. The firmware and operating system have been modified to accommodate the CryptoPhone functionality and provide added security, so a number of things that you might know from other PocketPC PDAs are not available on the GSMK CryptoPhone for security reasons. We supply the original PocketPC2003 manuals, license sticker and CD with the GSMK CryptoPhone 200, but you need to be aware that some functionality of the PocketPC OS have been disabled by us for security reasons. Installing 3rd party applications requires an Admin Policy Password. Do not try to use Pocket PC or Windows Mobile system updates as this will destroy the CryptoPhone firmware and void your warranty.

Charging

Before using your CryptoPhone, we recommend that you charge the battery until full. In order to do this, you must connect the power supply to the CryptoPhone. Depending on your location, you may need a plug adaptor to use the power supply if the plug does not fit in your outlet. The power supply is rated 100-240V, which means it will accept your line voltage without conversion as long as it lies within this range. The LED

in the upper right corner of your CryptoPhone will change its color to yellow while the device is being charged, and to green when fully charged. You can either charge the CryptoPhone in the desk stand or use the small direct-charge adaptor (Direct-charge adaptor •5•). You can also see the current battery status by tapping on the clock item on the upper right corner of the CryptoPhone display. The battery of the CryptoPhone allows for a standby time of 180 hours and a talk time of 3 hours 15 minutes in secure mode. Due to the higher power consumption of the built-in computer and the backlit display, this is less than what you might be used to from normal GSM phones. Also please note that these times may vary depending on your distance to the nearest GSM base station: the further away the base station, the more power your phone needs to use to reach it.

If you purchase a second battery for the CryptoPhone, you can charge it in the Desk Stand. Spare batteries are available in normal electronic stores that sell PDAs and mobile phones (Desk Stand •5•).

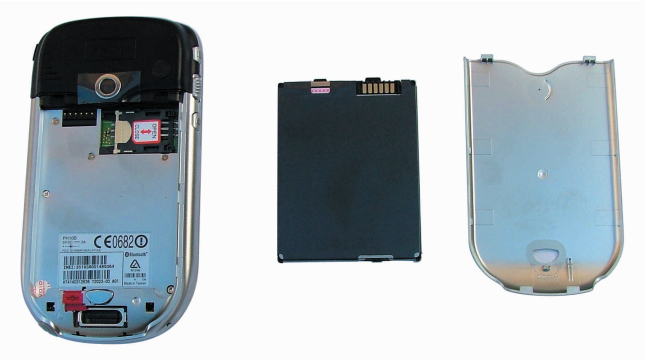
Note: we recommend to charge your GSMK CryptoPhone every night or have a charged spare battery ready, so you will not run out of battery unexpectedly. For security reasons explained later in the chapter ‘Security, Storage and Handling’, we suggest you place the CryptoPhone in your close vicinity such that it is under your permanent supervision while it is charging. If the phone rings or you need to place a call while the phone is charging, you can leave it plugged in while operating the phone.

Inserting your SIM card and switching the phone on for the first time

You need to insert a valid GSM card (SIM) in the GSMK CryptoPhone 200 in order to be able to place calls. To insert the SIM, remove the back cover of the device by pressing the silver button on the backside and sliding the cover downwards. (back cover •6•)

SIM card slot •6•

back cover •6•



battery •6•

You will see the SIM card slot in the upper right corner of the device (SIM card slot •6•). Lift up the SIM card cover and insert the SIM. Then push the SIM card cover down and push it towards the "closed" position. Now insert the battery (which is stored in the carrying case on the left hand side of the phone) and push the red battery lock upwards to secure the battery. (battery •6•)

This will power up the device. Replace the back cover by sliding it gently upwards onto the device.
Now the screen will lighten up and the GSMK CryptoPhone 200 begins its firmware initialization. This may take a moment. You will then be requested to calibrate the touchscreen of the GSMK CryptoPhone 200 by tapping the center of a cross with your stylus as it moves around the screen and go through a brief tutorial on how to do Copy & Paste on the device. Simply follow the instructions on the screen. After the calibration and tutorial, the Security Profile Manager will boot up.

Security Profile Manager

The CryptoPhone is based on the Windows Mobile (PocketPC 2003) operating system which contains some potentially vulnerable, yet convenient features and applications. To reduce the risk of attacks against your CryptoPhone's integrity, we recommend to disable some of these features. The Security Profile Manager helps you to select between security and extra features: the more features you enable, the larger the risk of vulnerabilities. In the following section, the different settings of the Security Profile Manager are explained in detail. Please take your time to read all the options to make an informed decision. After you have selected a Security Profile, click the OK button on the screen (Security profile selector •7•). Now the phone will install the operating system components according to the profile you selected.

Security profile selector •7•

The default setting is "Medium Security" which provides a good balance of convenience and security for most users.

> Note: You can always change the Security Profile setting by performing a Cold Boot (see page 14). After each Cold Boot you will be asked for your choice of Security Settings.

Security Profile choices:

No Added Security

This setting leaves the CryptoPhone unprotected against potential attacks on the operating system. New threats (against any system) are discovered from time to time, and we feel selecting "No Added Security" exposes the CryptoPhone to unneccessary risk. Choose this setting only if you really need one of the services that would otherwise be disabled in the "Medium security" setting and if doing so matches your risk profile.

Medium Security

At this level of security, the CryptoPhone disables a number of functions which are likely vulnerable to attacks, but are not essential for most users. Once you select "Medium Security", the following functionality is disabled:

- Picture Caller ID and Picture Contacts
- .NET compact framework
- Javascript
- MS scripting

- VBscript
- MS terminal services client
- MS Messenger client
- SIM Toolkit
- AvantGo
- WAP and WAP push
- MMS or Video-MMS

High Security

In High Security mode, Internet functionality and permanent storage to flash memory are no longer available. GPRS, data calls, the Internet Explorer and the Windows Media Player are disabled, in addition to the measures taken in Medium Security mode. Also permanent storage to flash memory is disabled, so you cannot save contacts or calendar appointments for permanent storage to flash.

Extreme Security

This setting is intended for customers who only use the CryptoPhone and normal unsecure call functionality, but wish to have all other means of communication disabled. This security level offers optimal protection against attacks that potentially could be performed using SMS messages or the synchronization with a desktop PC. PocketOutlook, SMS sending and receiving, Active Sync and the Inbox are disabled in this setting, in addition to the measures taken in High Security mode. We recommend this setting for situations where a highly skilled adversary has to be assumed.

Note: Depending on how you obtained your CryptoPhone, not all Security Profiles might be available or the described choices might be different in detail. GSMK provides customized Security Profile configurations as part of volume purchases for larger companies and organizations. So if you received your CryptoPhone from your organization, please consult with the appropriate corporate security manager regarding the choice of Security Profiles available to you. Also, GSMK may, without notice, remove certain components from the default installation, if we receive information that indicates a higher vulnerability of these components than originally assumed. Please check the CryptoPhone website for details.

Booting

After pressing OK in the Security Profile Selector, the Operating System will be installed according to the choice you made. This may take a moment and you will see multiple progress bars that disappear after a minute. Please do not try to use the touchscreen or any button during the installation. After the installation, the CryptoPhone automatically reboots (you see the full screen CryptoPhone logo) and displays the unencrypted telephone application. You need to choose your Security Profile only once before beginning to use your CryptoPhone, but can change it anytime by performing a Cold Boot.

Note: under certain rare circumstances, the installation of the operating system may not continue properly to the point where you see the full screen CryptoPhone logo again. If after the installation is finished, the automatic restart does not happen, please Cold Boot the device again and confirm your Security Profile setting again. You can always change the Security Profile setting by performing a Cold Boot (see page 14). After each Cold Boot you will be asked for your choice of Security Profile Settings.

Enter your PIN

Most GSM SIM cards require you to enter a PIN number. After you have initialized the CryptoPhone, the application for unencrypted phone calls shows up and asks you to enter your PIN. After you entered the PIN, press the green Enter button. The CryptoPhone will finish initialization and provide the secure telephony mode. If your GSM SIM does not require a PIN, the secure telephony mode will be enabled right away.

Standby

The GSMK CryptoPhone has four basic modes of operation. It can be either completely switched off, in 'standby mode', switched on, or in 'flight mode'. In normal operation the CryptoPhone is in 'standby mode'. In standby mode, you can switch the device on at any time by briefly pressing the button on top of the device. (Standby button •11•)

Standby button •11•

Now the screen will light up. To put the GSMK CryptoPhone 200 back in standby mode, press the button again, and the screen will go dark. Please note that pressing the Standby button for an extended period of time will toggle the backlight of the screen, but not put the phone into Standby. The GSMK CryptoPhone will still receive incoming calls when it is in Standby mode. In other words: standby mode will not disable the radio.

Flight Mode

It is not safe to enter an airplane, hospital or other no-phone area with the GSMK CryptoPhone switched on or in standby mode. To ensure the radio is off, you need to enter 'flight mode'. To enter flight mode hold the volume slider on the left side of the phone for 5 seconds downwards. (Volume slider •12•)

Volume slider •12•

You will now get the message "GSM is OFF" in the CryptoPhone display. In unencrypted mode you will see a little x next to the antenna symbol when flight mode is active and the GSM is switched off..
To switch the radio back on again, move the volume slider upwards and hold it there for at least 5 seconds. You will get a "GSM is turning on" message from the CryptoPhone and you will be required to enter your PIN again.

General Mobile Phone Security Advice

The use of mobile phones and other radio transmission equipment in certain areas is prohibited or restricted. Because of the risk of interference with life-support equipment, the use of mobile phones is also banned in most hospitals. Using a mobile phone in an airplane is a felony in most countries. You are responsible for complying with local laws and regulations.

Power down

To completely power down the CryptoPhone, open the back cover and push the red battery lock downwards to the Open position and remove the battery. Since the CryptoPhones memory is buffered by a small back-up battery, the contents of the phone (SMS, notes, appointments etc.) are not immediately erased. However, depending on age and charging state of the backup battery the contents might be lost after a while. The GSMK CryptoPhone firmware is unaffected by a power-down as it resides in non-volatile memory. It is recommended to store the CryptoPhone with the battery removed if it is not used for prolonged periods of time (several weeks).

Cold Boot / Emergency Erase

Initiating a Cold Boot is recommended in emergency situations when the capture of the device by an adversary is imminent, to get rid of any data stored in volatile memory that might compromise your security (like SMS, call history, notes, appointments etc.). Cold Boot will not erase the contacts and SMS messages stored on your SIM card. Also, a Cold Boot does not erase any information that you may have stored in Flash (Storage) or on SD memory cards. To initiate a Cold Boot, press the stylus into the Reset hole while simultaneously pressing the Standby button. (Cold Boot •14•)

Cold Boot •14•

Note: no key material that might compromise the security of your past calls is stored anywhere on your device. Upon completion of a secure call, all key material for the call is destroyed and permanently erased. The recommendation for a Cold Boot in emergency situations only relates to other data stored on the device like notes, contacts, SMS, call history etc.

Security Advice regarding Flash Storage

With the GSMK CryptoPhone you have the choice to store information in Flash Storage, if it is not disabled by the Security Profile you have chosen. Flash type storage is safe against failure of the backup-battery. You must however be aware that there is no way to securely erase information stored in flash memory in a way that it cannot be possibly reconstructed by methods of computer forensics. Even if you erase the

information and overwrite it with other data, it cannot be considered safely destroyed when stored on Flash Storage. Flash memory uses its own way of managing files that is beyond the control of the operating system. So files that are no longer visible after deletion in the file manager may still exist in some unused part of the Flash memory. In addition, esoteric physical effects ("memory burn in") make it possible for a forensic laboratory to reconstruct the former content of Flash memory, even if it has been erased or overwritten. The same problem holds true for SD memory cards, because they are also based on flash memory technology. We therefore recommend not to store any potentially compromising information on Flash Storage, if there is a risk that the device may fall into the hands of an adversary. You should store sensitive information in volatile memory, where it can be quickly erased by a Cold Boot in the event of an emergency.

Switching between Secure and Unsecure interface

You can switch fast between the normal unencrypted telephony mode and the secure GSMK CryptoPhone interface by pressing the Center Key. (Center Key •15•) Please make sure that you press only the center of the key, not the directional corners (left, right, up or down), as they may activate other functions (like call register) unsecure telephone interface. By pressing Center you can always quickly switch to the secure telephone interface, also while using other applications on the CryptoPhone. If some other application is blocking the Center-key while you are using PDA-functions, choose CryptoPhone from the Menu in the upper left corner.

Center Key •15•

Placing a Secure Call

Hash •16•

Display •16•

Secure •16•

Unsecure •16•

In order to place a secure call, the following conditions need to be met:

- your partner has either a CryptoPhone GSM or a CryptoPhone for Windows up and running
- there is sufficient GSM coverage
- the GSM operator supports 'GSM data calls' (technically called 'CSD')

Now enter the number of your partner and press the green Talk button (lower left corner). You will hear a bit of comfort noise in the speaker, followed by the normal ringing tone. It may take a bit longer than normal before the other end picks up, so please let it ring. After your partner has pressed the Talk button on his end, you will hear a ditt-dutt ditt-dutt sound that signals to you that the 'key setup' procedure for the secure connection is in progress. Key setup may take from 3 to 15, but typically 4 seconds, depending on line quality. Once key setup is completed you hear a »Ping« sound and can start talking to your partner. In order to verify the authenticity of the key, Please take a look at the display and read the three letters under »you say« to your partner and verify the three letters under »partner says«. Then press the OK button. (Hash •16•) After you pressed OK, the display will look like this: (Display •16•) The green SECURE indicator (Secure •16•) is only visible when a secure call is established. During all other times it is shown in grey with a open lock. (Unsecure •16•)

Key Verification

Reading the three letters and verifying what your partner says is meant to protect you against so-called ‘man-in-the-middle attacks’ on the secret session key. The letters are mathematically derived from the unique secret key that is used during each call. By reading and verifying them with your partner, you make sure that you are indeed communicating using the same key. Please pay attention to the voice of your partner when he reads his three letters. To be completely on the safe side against very sophisticated voice impersonation during the key verification, you can just read your letters unexpectedly in the middle of your call again and ask him to verify.

Call Quality during Secure Calls

The call delay indicator changes color in five steps between green over yellow to red. Green indicates the best call quality, red the worst. (Quality •17•) Delay describes the period of time it takes for your voice to reach your partner. This time gets longer if the transmission of the encrypted voice over the telephone network takes longer, or transmission errors occur. Reasons for longer than normal delay are usually either bad GSM coverage or network congestion. Network congestion can often be circumvented by setting up the call again, sometimes you just get a »bad line«. The GSM data call mode, used by the CryptoPhone to transport the encrypted voice data during a call, has a certain delay, caused by the architecture of the GSM network. The GSM network handles data with

Quality •17•

lower priority than voice transmissions. So even if the delay indicator is green, there is always a certain noticeable delay, much like on some transcontinental phone calls.

If the overall line quality becomes bad, the delay raises and you may experience »drop outs«. Note that the quality on international calls might not be as good as on domestic calls. The multiple operators involved in an international call often try to minimize their costs by technical measures that can affect the quality of the call. If the call quality is unacceptable, please try calling again. Call quality can also be adversely affected when using certain GSM providers or while driving fast in a car or train. If the Delay indicator becomes reddish or red (Indicator.a •18•), please try to find a place with better GSM coverage. Use the signal strength indicator on the left side of the display to find a better spot. If the delay indicator turns and stays solid red, please hang up and set up the call again. When no call is in progress, the delay indicator is shown grey. (Indicator.b •18•)

Indicator.a •18•

Indicator.b •18•

Problems with setting up a Secure Call

Some providers restrict the reception of GSM data calls, such as needed for the CryptoPhone. The practice is becoming increasingly rare, but a GSM-provider may only allow incoming data calls to subscribers that have a special ‘data subscription’, which comes with a special second phone number to call to reach the CryptoPhone. Some providers may not recognize that a number you are calling is a GSM/ISDN number, and erroneously try to handle the call via a modem. This can be recognized

by the called party because he/she hears a modem sound when picking up the phone. Some providers may not pass data calls to certain other providers at all.

Under certain circumstances, especially when roaming in GSM networks that are not properly configured, the "never ending key setup" problem may occur. The phenomenon is that the key setup phase takes longer then 20 seconds and never comes to an end. The underlying technical problem resides in the GSM network. Data calls are sometimes set up but then fail to transport any data.

All of the above conditions may make it impossible to use the CryptoPhone in one or both directions between two CryptoPhones. As a work-around if you are roaming try switching providers. If secure calling only works in one direction, you could use an unencrypted call to tell the other party to call you using CryptoPhone. These problems are inherent to using the CSD data call facility and apply to all encrypted telephony over GSM. For customers in Europe, North Africa and Asia who experience such problems we recommend our CryptoPhone 200T solution that uses the Thuraya satellite system to provide affordable secure communication also in areas that are outside GSM coverage or have no suitable GSM network setup for data calls.

Sometimes a specific condition of the GSM network leads to an unstable state of the GSM part of the CryptoPhone, which also might cause the "never ending key setup"-problem or other undesired behaviour. This condition can sometimes be fixed by soft-resetting the CryptoPhone.

Changing the volume

To change the audio volume during a Secure Call, use the volume control slider on the left side of the device. A row of colored dots gives you a graphic indication of the selected volume. Choosing the higher volumes (orange and red dots) is only recommended if you use the headset. If you set the volume too high without using a headset, your partner may experience an echo because his voice from the speaker gets fed back into your microphone. In noisy environments the use of the included headset is recommended. With the headset, you can set the volume to any desired level without experiencing noticeable echo.
When not placing a call, the Volume control slider changes the Ringing volume. The lowest level changes the ringing to vibrator only. In vibrator mode, the little speaker (Speaker) icon on the top bar changes to a vibrator icon (Vibrator).

Button up •20•

Button down •20•

Alternatively you can use the Up (Button up •20•) and Down (Button down •20•) buttons to change the in-call volume.

> Note: when holding the volume control slider for more than 4 seconds in one direction, you will toggle the flight mode switch. See page 12 for details.

Mute during call

If you need to switch off the microphone during a call, press the mute button. To switch the microphone on again, press the mute button again. The mute button (Mute •21•) can be used only during a secure call.

Mute •21•

Using the headset

For hands free operation, a professional quality headset is included with the GSMK CryptoPhone. You can plug it in any time, before or during a call. The headset cable connector socket is on the lower right side of the device.

You will notice that the headset is connected through a small adaptor cable. If you wish to use a different headset, connect it to this adaptor. Please note that standard 2.5 mm headset plugs will fit mechanically directly into the GSMK CryptoPhone, but that the headset will not work if plugged in without the adaptor cable. GSMK does not provide support for problems caused by using headsets other than the one supplied with your CryptoPhone.

Bluetooth

The CryptoPhone 200 has a Bluetooth interface. While it is possible to use a Bluetooth headset for making normal unencrypted phone calls, this feature is disabled for encrypted calls. The reason is that with a Bluetooth headset you would broadcast the contents of your confidential calls before they have reached the encryption engine in the CryptoPhone. Bluetooth radio signals can be received over several hundred meters with moderately sophisticated equipment, so an attacker could listen to your calls easily. The encryption used with Bluetooth is no hurdle for a determined adversary and does not offer sufficient protection. We recommend using a wire based headset when placing secure calls.

Secure Calls while moving

When using the GSMK CryptoPhone while moving fast in a car or a train, you may experience a degradation in call sound quality, periods of longer delay and short dropouts during a call. These effects are the result of a so called handover that occurs when you move from the coverage zone of one GSM tower (also called 'GSM cell') to the next. During the handover the data connection is briefly interrupted. To prevent important call contents from getting lost, the GSMK CryptoPhone, unlike other encrypted voice systems, accelerates the speed of decoding for a moment after the dropout, to catch up with the lost transmission time. This results in the voice of your partner rising in pitch (the »Mickey Mouse effect«) for a moment. After a short time the pitch returns to normal. The GSMK

CryptoPhone 200 has been successfully tested up to speeds of 180 km/h. The frequency and intensity of disturbances is primarily determined by the GSM network. In rural areas, the network consists of fewer and bigger cells, resulting in less frequent handovers and less disturbances. In urban areas the network has typically a high density of small cells, resulting in many handovers when moving and thereby causing more disturbances.

> Note: In many countries the use of mobile phones while driving is regulated or completely prohibited. You are responsible for complying with local laws and regulations on telephone use while driving a car. We strongly recommend the use of the enclosed headset while driving, even if local regulations may not require this.

Redialing

The CryptoPhone has access to a call history comprising the last 10 outgoing calls.. You can redial a number by scrolling through the last dialed numbers with the Up/Down keys and press the Talk button (Talk button •23•) once the desired number is shown in the display.

Talk button •23•

Calling from the Contacts list

Contacts list •24•

The Contacts list can be accessed by pressing the button on the CryptoPhone that is placed to the left of the speaker (Contacts list •24•). To place a secure call to a contact, tap and hold on it with the stylus and select the entry 'CryptoPhone' from the small menu that appears. The selected contact's phone number is now copied into the CryptoPhone. Now press the talk button to establish the secure connection.

Calling contacts stored on SIM card

To use phonebook entries stored on your SIM card, you first need to copy them into the main contacts database on the CryptoPhone. To do so, switch to the unencrypyted phone mode by pressing the Center Key (Center Key), then click on the CryptoPhone symbol in the upper left corner and select SIM Manager from the pulldown menu. The SIM Manager will now load all contact information from the SIM. After this is completed, select the 'Tools' menu on the lower screen menu and tap 'Select All'. Then select the Tools Menu once more and tap 'Save to Contacts'. Now all contacts will be copied into the volatile memory of the GSMK CryptoPhone, and you can call them as described above (in the chapter »Calling from the Contacts List«). Note that storage of contact information on the CryptoPhone is not encrypted. See page 14 for security information regarding permanent storage in Flash memory.

Troubleshooting

In the event the CryptoPhone shows unexpected behaviour, device response becomes very slow, or it does not connect to a GSM network, you can quickly reset it by pushing the stylus into the reset hole on the left underside of the device. The GSMK CryptoPhone will restart without erasing the memory.
(Cold Boot •25•) In the unlikely event such a problem persists, you can Cold Boot the device (see page 14). This will however erase all information in volatile memory.

Soft Reset •25•

Security Updates

In the event anyone discovers a flaw in the CryptoPhone, we will provide a firmware update, as well as a detailed and honest report on the possible security impact. As bad as security problems with cryptographic products can be, we believe the only way to handle them properly is open and transparent communication with our customers. You are the one best suited to determine potential damage to your interests, so we will provide you with all the known facts. Security is not a state but a process. And this process requires constant checking against emerging risks and new attack methods. Since the CryptoPhone comes with full published source code, the chances are much higher for a flaw to be discovered and fixed quickly than with any closed-source cryptographic product. Our advisory board of distinguished cryptographers and security researchers aids us in identifying and countering potential threats based on their intimate

knowledge of upcoming academic research and new emerging cryptanalysis methods. In case a firmware update is needed for security reasons, you will get notified either via the e-mail address that you supplied when purchasing the CryptoPhone online, or directly by the distributor. If you receive a notice about an upcoming security update, please verify it directly at our website htttp://www.cryptophone.de/ to prevent attackers from slipping you a malicious »update«. Please note that we will describe the details of the update procedure directly on the website. The firmware update mechanism is cryptographically secured using a 4096 bit public key signature system, which ensures only signed CryptoPhone updates will be accepted by your CryptoPhone. If you receive suspicious communication regarding CryptoPhone updates (such as an e-mail with an update file as attachment), please inform us immediately, as this may be an attempt to insert malicious firmware into your CryptoPhone. Please see our Frequently Asked Questions (FAQ) section on the website http://www.cryptophone.de/ for further detailed information on the benefits of published source cryptography.

Security, Storage and Handling

Your CryptoPhone is a Communication Security (COMSEC) device. It can only be regarded as secure as long as you have permanent and uninterrupted physical control over the CryptoPhone. Once an adversary could have gained physical possession of the CryptoPhone, it must be regarded as compromised. There is a variety of potential methods that would allow an adversary to listen into your calls after he manipulated the CryptoPhone

and gave it back to you. So never let the CryptoPhone fall into his hands. Have it always with you, in your immediate personal sphere of control. Optimally, you should take it with you to the bathroom, put it beside your bed when you sleep and not leave it alone in the hotel room. The black plastic carrying case the CryptoPhone is shipped in is watertight and you could even take it with you while swimming (although any damages resulting from doing so are not covered by the warranty. Check the rubber lips on the carrying case for sand and other objects that could impair the watertight sealing before using it for transport in wet or damp environments.)

If you have »lost« the CryptoPhone and »find« it back again, it has to be regarded as compromised. Never lend or borrow your CryptoPhone to anyone. Major intelligence agencies are known for a wide variety of hightech manipulation methods that are impossible to detect without a massive scientific effort (several months of analysis at the cost of several 100.000 Euros per device). If in doubt and your security depends on it, consider purchasing a fresh unit. The CryptoPhone is specified and designed for use in normal office/home environments. It is not ruggedized or specially sealed against water and other harsh environmental conditions. (For ruggedized versions of the CryptoPhone that comply with military specifications, contact us at sales@cryptophone.de). Submitting the CryptoPhone to excessively high or low temperatures (like in the outside pocket of an overcoat in cold climates) might temporarily or permanently damage the display and lead to accelerated battery aging, affecting the ability of the battery to store power and thereby reducing the standby time of your CryptoPhone. Damage to the battery and display as well as any kind of mechanical damage is not covered by the warranty.

Repairs

Because of the manipulation risk, we do not take back any CryptoPhones from customers, except for repairs. There is no such thing as a »restocked«, »refurbished« or »second hand« CryptoPhone. All sales are final. If your CryptoPhone is defective, we will either repair it or swap the electronics for a new factory fresh device. No parts that have been in the hands of other customers will be used in repairs.

If you need a repair, please mail us at service@cryptophone.de, so we can instruct you about the proper shipping and security procedures. Shipments that arrive for repair without prior acknowledgement and/or in ignorance of the advised shipping method and security precautions will be ignored. Please understand that it is in your own interest to adhere to the security measures, since only this will enable us to fulfill your security requirements.

> Note: the built in high-power Lithium-Polymer rechargeable battery of the CryptoPhone is a wear-and-tear part and not covered by the warranty. Replacement batteries are available in normal PDA or mobile phone stores.

Accessories

The GSMK CryptoPhone is based on a device manufactured by HTC, sold under different brand names. Additional accessories for your CryptoPhone (like holsters, car kits, external antennas etc.) can therefore be easily obtained by buying kit that is destined for XDA 2, MDA 2 or Qtek 2020 devices.

3rd Party Software Install

In theory it is possible to install Microsoft PocketPC 2003 compatible 3rd party software on your GSMK CryptoPhone device. You should know that 3rd party software of any kind can be used to attack the integrity and security of your GSMK CryptoPhone. Installing additional software on Communication Security equipment like the CryptoPhone is a grave security risk that you should only take if it is absolutely necessary. If you really need to install additional software on your GSMK CryptoPhone, you need to enter the Admin Policy Password in the Settings → System Menu. The password can be found in the sealed envelope behind the foam pad in the lid of the CryptoPhone carrying case. Again, please be aware that installing 3rd party software might irrevocably compromise the security of your CryptoPhone or damage its funtionallity.

> Any problems that result from installing any 3rd party software on the CryptoPhone are not covered by warranty or support. You have been warned.