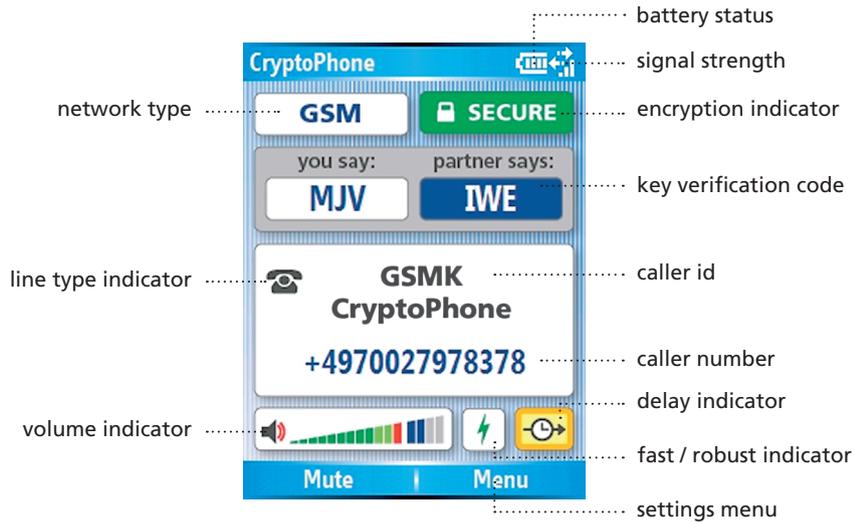




GSMK CRYPTOPHONE G10i







General	4	Changing the volume	24
Inserting SIM card & switching the phone on	5	Mute during call	25
Security Profile Manager	6	General Mobile Phone Security Advice	25
Security Profile Choices	7	Power down	25
Enter your PIN	11	Cold Boot & Emergency Erase	26
Charging	11	Security Advice regarding Flash Storage	27
Standby	13	Using the headset	28
Switching on/off	13	Bluetooth headset	28
Placing an Encrypted Call	14	Sync Contacts and Appointments	29
Key Verification	15	Troubleshooting	30
Redialing	16	Security Updates	30
Calling from the Contacts list	16	Security Advice	32
Call Quality during Secure Calls	16	Storage and Handling	33
Secure Calls while moving	18	Repairs	33
Switching the Call Type	19	Accessories	34
Switching the Linetype	20	3rd Party Software	35
Problems with setting up a Secure Call	21		



General

Your CryptoPhone G10i is based on generic quadband (850 / 900 / 1800 / 1900) GSM Smartphone hardware that is sold under different brand names. The phone's 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 Smartphones are not available on the GSMK CryptoPhone for security reasons. We supply the original Smartphone manuals, license sticker and CD with the GSMK CryptoPhone G10i, but you need to be aware that some functionality has been disabled by us for security reasons and some functions have been changed to better integrate the CryptoPhone functionality.

Note: Do not try to use Microsoft operating system updates as this may destroy the CryptoPhone firmware and void your warranty. Certified CryptoPhone Updates are only provided by GSMK to you in a cryptographically secure manner.



Inserting SIM card & switching the phone on

You need to insert a valid GSM card (SIM) into the GSMK CryptoPhone G10i in order to place calls. To insert the SIM, remove the back cover of the device by sliding the back cover downwards. You will see the SIM card slot in the lower middle of the device. Insert the SIM card with the gold-plated contact area facing down. Now insert the battery (which is stored stored separately in the shipping box). Replace the back cover by sliding it gently upwards onto the device. Now open the lid and push the power/hangup button. The screen will light up and the GSMK CryptoPhone G10i begins its firmware initialization. This may take up to two minutes.





Security Manager



The CryptoPhone is based on the Windows Mobile operating system which contains some potentially vulnerable yet convenient features. Therefore we recommend you to disable some of these features. The security manager helps you select between security and extra features: the more features you enable, the larger the risk of vulnerabilities. Please take your time to read all options.

Back

Security Profile Manager

The CryptoPhone is based on the Windows Mobile 2005 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. Now the phone will install the operating system components according to the profile you selected.

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 26). After each Cold Boot you will be asked for your choice of Security Settings.

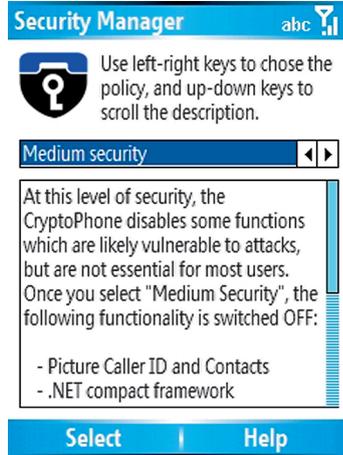


Security Profile choices:

No Added Security

This setting leaves the CryptoPhone with very little protection against potential attacks on the operating system. Some mechanisms to prevent really stupid attacks are activated, but this creates only a base layer of protection that is not sufficient against a skilled adversary. New threats (against any operating system) are discovered from time to time, and we feel selecting “No Added Security” exposes the CryptoPhone to unnecessary 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.

The screenshot shows the Security Manager interface. At the top, there is a blue header with the text "Security Manager" and a small icon of a person with a question mark. Below the header, there is a section titled "No added security" with a blue background and a white question mark icon. To the right of this section, there is a description: "New threats (against any system) are discovered from time to time, and we feel selecting 'No added security' exposes the CryptoPhone to unnecessary risk. Select this 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. (See the...". At the bottom of the screen, there are two buttons: "Select" and "Help".



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
- MIDP and all other Java framework
- MS scripting
- VBscript
- MS terminal services client
- MS Messenger client
- SIM Toolkit
- Remote OS updates
- Downloadable Ringtones
- some media playback features
- WAP and WAP push
- MMS and Video-MMS



Security Manager abc 

 Use left-right keys to chose the policy, and up-down keys to scroll the description.

High security  

Very secure but no Internet functionality and no permanent storage. Like "Medium Security" plus blocking GPRS connections and/or browsing the web, and completely removing the media player. Also, with the "High Security" setting selected, you cannot save contacts or calendar appointments for permanent storage to flash.

Select | Help

High Security

In High Security mode, internet functionality is no longer available. GPRS, PPP data calls, the Internet Explorer and the Windows Media Player are disabled, in addition to the measures taken in Medium Security setting. The following functionality is disabled in High Security mode:

- Bluetooth
- OBEX
- WLAN
- GPRS
- all TCP/IP functionality
- MediaPlayer
- Internet Explorer
- Video Telephony
- email functionality
- ActiveSync
- Infrared
- SD-card functionality



Security Manager abc

Use left-right keys to chose the policy, and up-down keys to scroll the description.

Extreme Security ◀▶

Optimal protection, only encrypted and unencrypted voice calls are possible. Like "High Security" but no transmission or reception of SMS messages, and no synchronization of appointments and/or contact information with a desktop PC is possible.

Select | Help

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 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 indicate a higher than originally assumed vulnerability of this component.



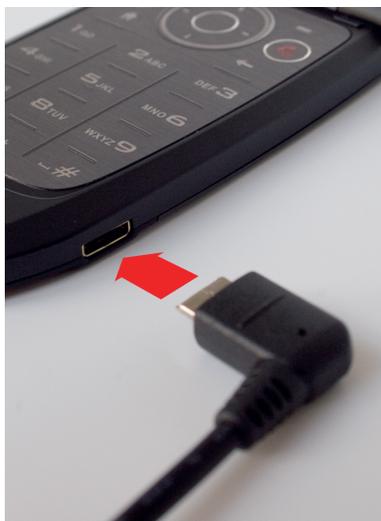
Enter your PIN

Most GSM SIM cards require you to enter a PIN number. After you have switched on the CryptoPhone, you will be asked to enter your PIN. After you entered the PIN, press the “Done” button. The CryptoPhone will finish initialization and present the secure telephony mode interface. If your GSM SIM does not require a PIN, the secure telephony mode will be presented right away.

Note: We recommend that a PIN number is used, as it makes the extraction of information stored on the SIM more difficult for an attacker and prevents you from incurring charges to your account if the phone is stolen.

Charging

Before using your CryptoPhone, we recommend that you fully charge the battery. 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 status LED will change color to yellow while the device is being charged, and to green when fully charged. You can either charge the





CryptoPhone with the power supply (recommended) or with the supplied USB sync cable on a computer. Charging over USB takes considerably more time and is dependent on your computers configuration and setup, so it may not work under some circumstances (e.g. if you have no synchronization software installed on your computer or the USB port is not powered up).

Due to the higher power consumption of the built-in powerful processor and the backlit display, the overall standby time and the talk time in secure mode are slightly less than what you might expect from standard GSM phones. Also please note that the standby and talk 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. Spare batteries are available in normal electronic stores that sell HTC, Qtek or i-mate brand mobile phones.

Note: For security reasons explained in the chapter 'Security Advice' (page 32), we suggest you keep the CryptoPhone with you at all times so that it is under your permanent supervision. 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.



Standby

The GSMK CryptoPhone has three basic modes of operation. It can be either completely switched off, in 'standby mode', or active. In normal operation the CryptoPhone is in 'standby mode'. In standby mode, you can activate the device at any time by opening the lid.

Now the screen will light up. To put the GSMK CryptoPhone G10i back in standby mode, simply close the lid. The GSMK CryptoPhone will still receive incoming calls when it is in standby mode. In other words: standby mode will not disable the radio, it just puts the processor to sleep and switches the display off.

Switching on/off

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 switch off your CryptoPhone G10i by pressing the power/hangup button for a few seconds. To switch it on again, press power/hangup for two seconds. You will be required to enter your PIN again.





**GSMK
CryptoPhone**

+ 49 700 27978835

Placing an Encrypted Call

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

- your partner has a CryptoPhone compatible device up and running
- there is sufficient GSM coverage
- the GSM operator supports 'GSM data calls' (technically called 9600 bit/s Circuit Switched Data or 'CSD')

To place a secure call, you can simply dial from the home screen and press the "Call Secure" softkey on the left side. You can also choose "Contacts", select a contact and press "Call Secure". Further you can switch to the CryptoPhone screen by pressing the home key and dial directly (press the green Call button after entering the number).

The very first call after you switch on the CryptoPhone will take longer to be dialed after you press the green button, as the random number generator needs to be initialized and verified. After this you will hear a bit of comfort noise in the speaker, followed by the normal ringing tone. It may take longer than in unsecure mode before the secure connection is established, 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 30 seconds, but typically 4 seconds, depending on line quality. Once key setup is com-



pleted 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«. The green SECURE indicator is only visible when a secure call has been established. During all other times it is shown in grey with an open lock.

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 session key is different for each call, as no key material is re-used between calls. The letters are mathematically derived from the unique secret key that is generated for 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 could periodically reverify the letter code with your partner during the conversation.



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 by moving the Navigation keys up/down and press the green Talk button once the desired number is shown in the display.

Calling from the Contacts list

To call a contact stored in the contact list, press the right soft key in the home screen labeled "Contacts". Now you see the list of contacts stored on your SIM and on the phone. The left softkey is now labeled "Call Secure". To place the secure call, move the selection bar with the Navigation keys to the contact and press the "Call Secure" softkey. The CryptoPhone G10i now switches to the secure call mode and immediately dials the selected contact number in secure mode.

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. 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.



In general, you will achieve shorter delays by switching the call type to Fast (see Switching the Calltype, page 19).

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 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 rises 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. It often helps to switch the GSM provider to achieve better secure call quality. As a rule of thumb, the larger operators tend to work better than the small ones.

If the Delay indicator becomes reddish or red, please try to find a place



with better GSM coverage. Use the signal strength indicator on the upper right 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.

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 quality, periods of longer delay (especially in Robust call mode) 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.

The GSMK CryptoPhone G10i has been successfully tested traveling at speeds faster than 180km/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 driv-



ing 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.



Call Type Fast



Call Type Robust

Switching the Call Type

The CryptoPhone G10i supports two different types of call. We call them “Fast” and “Robust”.

Technically speaking, the Robust mode uses a special type of error correction in the GSM network, which causes less dropouts (short interruptions) in the conversation, but can cause longer delay under bad conditions and buildup of delay in the network. The Fast mode does not use this error correction and thus has less delay and no delay buildup. However, under certain network conditions it can cause chopped up conversations with lots of dropouts or does not work at all (e.g. on some international calls or calls between different mobile phone operators). We generally recommend to use the Fast mode as it usually gives better call quality. Only if it does not work or gives unsatisfactory results, you should switch to Robust mode.

To switch the call type, in the CryptoPhone mode, select the “Menu”



softkey, choose Settings, and use the Navigation Control and Enter button to change the Calltype to the desired mode. Then leave the Settings page by pressing the softkey labelled "Done". The icon between the volume indicator and the delay indicator will switch according to the chosen Call type to indicate Fast or Robust mode.

Switching the Line Type



Normally, the CryptoPhone uses the V.110 circuit switched data (CSD) - also called digital data call - bearer type to establish a secure connection. To call to an analog landline or to a CryptoPhone on a satellite network or a network with non-standard data-call configuration (like most GSM carriers in the USA), you can switch to the V.32 bearer mode.

To switch the line type, in the CryptoPhone mode, select the "Menu" softkey, choose Settings, and use the Navigation Control and Enter button to change the Line Type to the desired mode. Then leave the Settings page by pressing the softkey labeled Done.

A small desktop phone icon will show up on the CryptoPhone screen if V.32 is activated. The call setup with V.32 takes longer than with V.110, as the modems need some time to synchronize. Incoming calls are not affected by the call type settings.



Problems with setting up a Secure Call

Your GSMK CryptoPhone G10i is designed to provide you with intuitive, easy-to-use strong voice encryption on GSM networks - out of the box without requiring any configuration. In some countries and on some GSM networks, however, problems might occur which may require some configuration and/or special procedures. This section will guide you through these procedures if you encounter problems with setting up a secure call.

[Call Type / Line Type] If you cannot establish a secure call at all, i.e. if the called party's CryptoPhone does not ring, you may have to select a different Line Type or Call Type. In the USA and Australia, for instance, the Line Type must be set to V.32 and the Call Type to Robust, while in Europe and most Asian countries Line Type V.110 and Call Type Fast works best. Depending on the local GSM provider's network configuration, different Call Type / Line Type combinations may be required. See the two preceding sections for details on how to change call type and line type.

[Data subscription required] Some providers restrict the reception of GSM data calls, such as needed for encrypted calls using the CryptoPhone. Even though this practice is becoming increasingly rare, 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 in order to reach the CryptoPhone in encrypted mode. If your local GSM provider and/or call plan requires such an additional data subscription, you need to order this service from your local GSM provider. If you are assigned a second 'data' phone number, always call this number when making an encrypted call.

[Improper Signalling] Some providers may not recognize that a number you are calling in encrypted mode is a digital GSM data number, and may erroneously try to handle the data call via an analog modem. In this case, incoming calls may erroneously be signalled as analog unencrypted voice calls, and consequently they can not be picked up in CryptoPhone mode. This issue can be recognized by the called party when a modem tone can be heard after picking up the phone. If switching the line type to V.110 is not possible or does not solve the problem, you will either need to get a separate data number as described above, or you may need to switch providers. Very few GSM service providers also may not pass data calls to some or all other providers. If your GSM service provider does not offer cross-network data calls, then encrypted calls are only possible within the same GSM network.



[Never ending key setup] Under certain circumstances, a similar signalling issue at the GSM provider may also result in the “never ending key setup” problem, especially when roaming on GSM networks that are not properly configured. The phenomenon in this case is that the key setup phase takes longer than 30 seconds and never comes to an end. The underlying technical problem resides in the GSM network on which you are roaming. Data calls are sometimes set up but then fail to transport any data. To work around the problem if you are roaming, try switching providers. If secure calling only works in one direction, you can also use an unencrypted call to tell the other party to call you back securely using his or her CryptoPhone. These problems are inherent to using the CSD data call facility and apply to all encrypted telephony over GSM. Under certain rare circumstances, a specific signalling condition in the GSM network may lead to an unclear signalling state in the CryptoPhone’s GSM engine, which may also cause the “never ending key setup” problem or other undesired behavior. This situation can usually be rectified by simply powercycling the CryptoPhone.

[Spotty Coverage] In some countries, GSM coverage is spotty at best and does not offer country-wide coverage. For customers in Europe, North Africa and Asia with GSM coverage problems, we recommend



our Thuraya T2 add-on solution that uses the Thuraya satellite system to provide the added benefit of affordable secure communication outside of your GSM coverage area. A CryptoPhone solution for Inmarsat M4 satellite terminals is also available for operations outside of GSM or Thuraya coverage.

Changing the volume



To change the audio volume during a Secure Call, use the volume control buttons on the left side of the lid. An on-screen indicator will provide you with visual feedback regarding the volume you set.

The CryptoPhone G10i volume can be changed over a very wide range to accommodate for different sound characteristics of the CryptoPhone the other party uses and the noise level of your environment. Beyond the normal audio levels, additional levels provide an extra boost of volume. They are marked blue in the volume indicator.

Note: using the blue audio levels may cause the sound to be very loud. Please use with care.



Mute during call

To mute the microphone during a call, press the softkey labeled “Mute”. To switch the microphone back on again, press the softkey 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

Simply press the power/hangup button for three seconds and the phone switches off. 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 (e.g. several weeks).



Cold Boot & Emergency Erase

Initiating a Cold Boot is recommended in emergency situations, to erase data stored in volatile memory that might compromise your security (like SMS, call history, notes, appointments etc.). Please note that this is not a very secure erasure procedure. Traces of your data might be reconstructed in memory by a skilled adversary by means of advanced computer forensics. 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 on SD memory cards. To initiate a Cold Boot follow the following procedure:

Remove the battery, re-insert the battery, place the phone on a flat surface, hold the softkeys (1) and (2) while pressing briefly the power/hangup button (1 sec), wait till the screen becomes dark, then release the softkeys simultaneously, press 0. Now the re-initialization process takes place and the phone will boot up again after a while.

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

On the GSMK CryptoPhone some information, such as contacts and SMS, is stored in Flash Storage. 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 sophisticated 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”) may make it possible for a forensic intelligence laboratory to reconstruct the former content of Flash memory, even if it has been erased or overwritten once. The same problem holds true for (mini)SD memory cards, because they are also based on flash memory technology. We therefore recommend that any potentially compromising information is not stored in Flash Storage memory if there is a risk that the device may fall into the wrong hands.



Using the headset

For hands free operation, a stereo headset is included with the GSMK CryptoPhone. You can plug it in any time, before or during a call, however you may terminate an ongoing call under some conditions when inserting the headset plug off-angle. The headset cable connector socket is on the right side of the device. GSMK does not provide support for problems caused by using headsets other than the one supplied with your CryptoPhone.

Bluetooth headset

The CryptoPhone G10i has a Bluetooth interface. While it is possible to use a Bluetooth headset for making normal unencrypted phone calls, a bluetooth headset can not be used during 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 and decrypted 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.



Sync Contacts and Appointments

The CryptoPhone supports in principle the synchronization of contact and calendar entries with a computer. You need to be aware that in theory it might be possible to attack the operating system of the CryptoPhone by supplying manipulated data to your PC or exploiting unknown problems in ActiveSync. GSMK does not recommend to sync your CryptoPhone with a PC, especially if the PC is connected to a network, for security reasons. If you have high security demands and need to assume a very sophisticated adversary, avoid to sync your CryptoPhone with a PC. To initiate a sync, connect the CryptoPhone to the computer using the enclosed USB cable. When you sync your CryptoPhone with a PC, we strongly recommend to physically disconnect the PC from any network connection as a precautionary measure. In the Security Profile “Extreme”, ActiveSync is completely deactivated .

Note: Depending on your Security Profile setting, sync over IrDa (Infrared) and Bluetooth may be deactivated on the CryptoPhone as a precautionary security measure. The main risk is that an adversary could potentially gain wireless access to your device while it is in your pocket or just on the desk in front of you. See page 6 for details on the Security Profile Manager.



Troubleshooting

In the event that the CryptoPhone reacts unexpectedly i.e., device response becomes very slow, key-lock can not be unlocked, or the phone does not connect to a GSM network, you can quickly reset it by removing and re-inserting the battery. The GSMK CryptoPhone will restart without erasing the memory.

In the unlikely event such a problem persists, you can Cold Boot the device (see page 26). This will however delete all information in memory.

Security Updates

GSMK continually seeks to improve the security and quality of operation of the CryptoPhone G10i. In the event anyone discovers a flaw in the CryptoPhone, we will provide a firmware update, as well as a detailed 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 helps us to identify and counter potential threats based on their intimate knowledge of the latest academic research and 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 your local authorized CryptoPhone distributor.

If you receive a notice about an upcoming security update, please verify it by contacting us directly. The contact details are on our website <http://www.cryptophone.com/> to prevent attackers from slipping you a malicious »update«.

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 unannounced 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 Questions and Answers section (Q&A) on the website <http://www.cryptophone.com/>



phone.com/ for further detailed information on the benefits of published source cryptography.

Security Advice

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 temporary 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. Keep the handset with you securely at all times. 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.

If you have »lost« the CryptoPhone and »find« it back again, it has to be regarded as compromised. Never lend your CryptoPhone. Major intelligence agencies are known for a wide variety of high-tech 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.



Storage and Handling

The CryptoPhone is specified and designed for use in normal business, home and other general conditions. It is not reinforced 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. Sitting on the CryptoPhone or submitting the device to other heavy mechanical loads may damage parts of the phone, especially the display and keyboard. Damage to the keyboard, battery and display as well as any kind of other 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 acknowledgment 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 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 etc.) can therefore be easily obtained by buying a kit that is designed for i-mate Smartflip or Qtek 8500 devices.



3rd Party Software

In theory it is possible to install Microsoft Smartphone 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. Please be aware that installing 3rd party software might irrevocably compromise the security of your CryptoPhone or damage its functionality.

GSMK does not provide any support for installing 3rd party software and will not provide support for problems caused by installing 3rd party software. Any and all problems caused by 3rd party software are not covered by warranty or support.

You have been warned.

If you require large number of custom CryptoPhones that include certain software components of your choice by default, please contact sales@cryptophone.de to discuss your requirements.



GSMK
Marienstraße 11
10117 Berlin
<http://www.cryptophone.de>

© 2006 GSMK