



Mobile Encryption For Secure Communication

CSP-all-en

Quick Start Guide

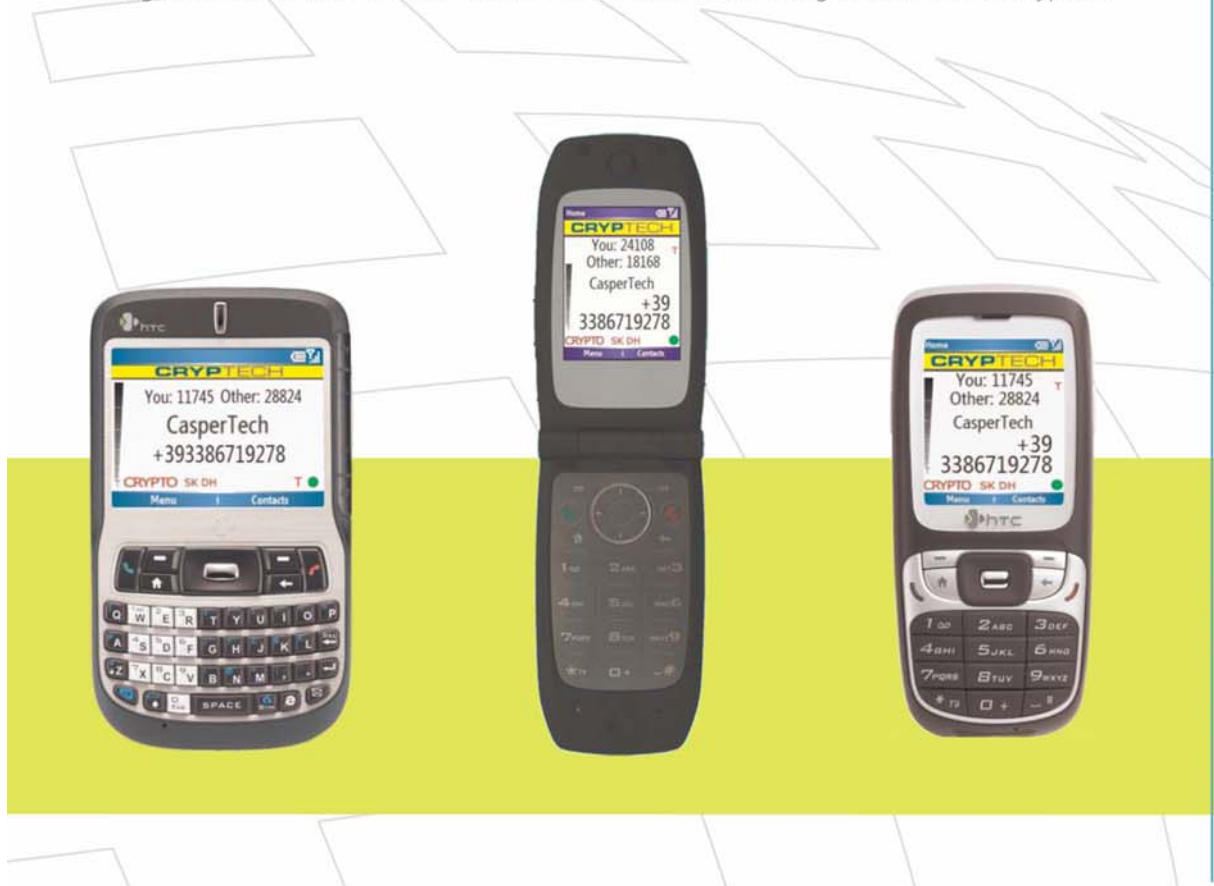
CRYPTTECH[®] MOBILE ENCRYPTION FOR SECURE COMMUNICATIONS

Casptech presents the latest CRYPTTECH release, the ultimate solution for GSM communications protection. Now available on new and most attractive devices, Crypttech benefits from a new audio solution that ensures complete absence of echo and provides best voice quality, comparable to that of a traditional phone call.

Crypttech does not require special installation processes or complex settings. Encryption keys are easy to configure directly by the user, thus ensuring total privacy. The AES256 algorithm, with symmetrical keys, ensures the best protection against any kind of wiretapping.

The encryption key used for the call is generated combining two systems: the 2048 bits Diffie-Hellman protocol provides a session key which is subsequently merged with the symmetrical key formerly set on the device by the user, producing a different encryption key for each call. The encryption keys will be automatically deleted at the end of the call. The encryption keys storage is protected by a password and keys are displayed on the screen in hash format, thus ensuring secrecy in case of device theft. The Diffie-Hellman protocol can also be used alone, in order to make encrypted phone calls between devices without shared keys.

Crypttech is based on a high-level encryption technology, nevertheless it's very simple to use thanks to its user-friendly interface. The system turns voice into data, encrypts it and sends it in real-time through the GSM data channel to the other device, ensuring end-to-end encryption.



The **CRYPTTECH®** kit consists of:

- 1 smartphone with pre-configured Cryptech System
- 1 AC adapter
- 1 USB cable for PC connection/synchronization (USB to MINI-USB)
- 1 stereo headset with volume control
- 1 Smartphone User Manual
- 1 Cryptech User Manual and Quick Start Guide

Standard features of **CRYPTTECH®** :

- Available for Microsoft Windows Mobile® 2003/2005 on Pocket PCs and Smartphones
- Secure communications over all GSM networks (850/900/1800/1900 MHz)
- High audio quality of encrypted calls
- User-friendly interface
- Automatic selection of incoming crypto/clear calls
- End-to-end encryption with AES 256 algorithm and keys entered directly by the user
- 2048 bits Diffie-Hellman protocol for session keys generation
- Authentication system customizable by the user
- Secure encryption keys storage




Optional **CRYPTTECH®** features, on demand:

- SmsCRYPTTECH
- File crypto Mobile/Desktop
- Customization of encryption algorithm on user demand
- Application for central Key Management System from Pc
- On-line customer service

CASPERTECH TRUST IN COMMUNICATIONS  **Cryptech® Quick Start Guide**
"how to go crypto in six easy steps"

This quick start guide will help you to start making and receiving encrypted phone calls in six easy steps. Four more steps and you will learn how to manage your security functions. After this quick set up you will be able to perform the basic operations, however we recommend that you read carefully the full documentation that comes with the device.


 To be able to make encrypted phone calls, make sure that the CSD DATA/FAX GSM CHANNEL is enabled for your SIM card. Please check this feature with your mobile service provider (the data channel activation is usually free of charge, and you will often get an additional data number and a fax number).

SIX EASY STEPS TO MAKE YOUR FIRST ENCRYPTED CALL

After completing the six following steps, you will be able to make and receive encrypted calls.

1. Insert SIM card

Ensure that the phone is turned off, then open the battery cover and hold the phone with the front panel facing down in the palm of your hand. With the other hand press down on the battery cover and slide it open. Insert the SIM card into the SIM card slot with its gold contacts facing down.

 Some mobile telecom providers have not yet upgraded their data channels to meet international quality standards. This however does not affect the functionality and security level of the Cryptech technology.

2. Install the battery

When the battery cover is removed, insert the battery by aligning the exposed copper part of the battery pack with the protruding copper conductor of the battery slot. Insert the bottom side of the battery first, then gently push the battery into place and replace the battery cover. To charge the battery, either connect the phone directly to a power supply outlet using the AC adapter, or plug it to the USB port on your PC using the USB cable.

3. Switch on the telephone

Open your phone and locate the power/end button (#22). Press and hold the button to turn on the phone. The same can be done to switch off the phone.

4. Unlock SIM PIN code protection

Most SIM cards are pre-set with a PIN code, provided by the mobile service provider, which must be entered when the unit is turned on. The PIN code is a 4 digits number, usually shipped with the SIM itself: the SIM is unlocked when the PIN code is entered. Cryptech can make and receive calls only once the PIN code has been inserted.

5. Launch the Cryptech application

When you turn on the device, the Cryptech application is automatically launched. During your first use, you will see the message in the picture on the right, informing you that the authentication user password has not yet been set. This alert message does not prevent you from making and receiving encrypted call and it can be bypassed by simply pressing OK. The Cryptech start screen will appear (see picture on the left). However we recommend that you insert your own authentication password. Once the password has been set (see step 7), and the "secure" mode is selected (step 10), this alert will be replaced by a windows asking you to enter your authentication password.

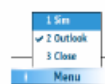


If Cryptech remains inactive for some time, Windows sends it into the background. To reactivate it, simply press the "Back" button (#23) until the Cryptech screen comes back on the display. Alternatively, you can press "Menu" in Windows Mobile Home Screen and select the "Cryptech" icon from the list shown on the display.



6. Make an encrypted call

Once you have the Cryptech start screen on your display, in order to make an encrypted call you can either dial a number directly from the keyboard, or you can import the telephone number from your phone book (select "Contacts" then "Update" to refresh the list, and manage the source – SIM or Outlook with the "Menu" options). Now press the green "call" button (#17): After a synchronization phase, the call will start. The receiver must press the green button to answer the call. To adjust the volume during a call, you may use the up/down arrows buttons (#24). The volume can also be set for all the calls by selecting "Menu" and then "Audio options" in the Cryptech screen.



FOUR MORE STEPS TO MANAGE YOUR SECURITY

You are now able to make and receive encrypted calls which cannot be decoded. However your device is still in a state called "initial use", in which the user authentication password has not yet been set and the keys used to encrypt the phone call are the pre-set default ones delivered with your device. To get full control of your own security settings, we recommend you to perform the following additional steps.

7. Initialize Cryptech with your own user authentication password

The user authentication password is used both to control access to the Cryptech application and to the storage area of the cryptographic keys which make your conversations secure. Furthermore, once your user authentication password has been set, you will be able to insert and administer your own cryptographic keys and delete the default ones. To set your own user authentication password, select "Menu", then "Security Options", then "Key Management". Choose a password, type it twice in the two required fields and click "Done". You should now be prompted with the "Key Management" window, where in the next step you will be taught how to enter your own cryptographic keys.



Please, remember to initialize the Cryptech user authentication password as soon as you can, as well as to set your own cryptographic keys (see step 8), as phone calls security is strongly enhanced. Do not forget your authentication user password because without it Cryptech can't be launched and you will need to contact Casper Technology for software replacement/restore.

8. Define your own cryptographic keys

Static cryptographic keys are shared by all the devices used to talk in encrypted mode with each other and are used to encrypt the whole conversation. They are often called "symmetrical" or "shared" because they must be identical for both interlocutors. Coming from the previous step, you should already be prompted with the "Key Management" window. Otherwise, click "Menu", then "Security Options" and finally "Key Management". Create at least one cryptographic key by selecting "New", then typing "1" in the "Priority level" field and your password in the field below. Notice that the passwords chosen in this section are used to encrypt the conversations, whereas the user authentication password is used to grant access to Cryptech and to protect/manage the encryption keys storage. The value "1" means "highest priority" and is required in order to bypass the Cryptech test keys. You can see both test keys on the screen, one marked "test", the other anonymous: they are useful when first testing your devices, since you can make encrypted calls even before you decide to create your own keys. Once you have successfully inserted your key/s,

you can delete the Cryptech test keys with the "Delete Key" function: click on each key, select "Menu", then "Manage Key" and "Delete Key". Remember to set the same static shared keys on every device you want to communicate with, or consider using the *Diffie-Hellman* protocol (see step 9) to call in encrypted mode without sharing common keys.

9. Manage your encryption modes

The Cryptech application supports two ways to generate the encryption keys: static (shared) keys and dynamic keys based on the Diffie-Hellman protocol. In step 8 we have explained how you can define and manage static keys. The Diffie-Hellman protocol does not require user intervention. In this case the keys are dynamically created at the beginning of the call and deleted when this is terminated.

Both encryption with static shared keys and with dynamic keys guarantee absolute security, however in both cases there is a "human factor" to consider. Static keys must be shared by all interlocutors and, if their number is large, there is a certain risk that somebody inadvertently discloses the key. In the Diffie-Hellman protocol there is the remote possibility of an intruder intercepting the keys during the initial exchange. Cryptech protects you from this risk by generating unique mutual authentication codes that appear on your screen during the call. Both interlocutors should communicate these codes to each other: if they match, no intruder has interfered with the call.

Since users may forget this additional protection, Cryptech uses by default a combination of both static and dynamic keys that eliminates the risk of "human negligence". However several options are available to provide maximum flexibility of usage.

By default the Cryptech application is pre-configured for highest security, i.e. combination of static and dynamic keys. Five security Levels (also called "restrictivity levels") can be managed in the "Security Level" area ("Menu", "Security Options" then "Security Level"):

1. Only shared keys are used and required, while the Diffie-Hellman protocol is disabled.
2. Either shared keys or the Diffie-Hellman dynamic keys are used, depending upon which ones are activated ("compatibility level"). At this level you can talk with contacts you *do not share secret keys* with.
3. Shared symmetrical keys are required, while Diffie-Hellman is used if available.
4. Shared symmetrical keys are used if available, while Diffie-Hellman is required. At this level you can talk with contacts you *do not share secret keys* with.
5. Both shared symmetrical keys and the Diffie-Hellman protocol are required.



Select your option according to the set-up of your partners. Whenever possible, we recommend the use of level #5.

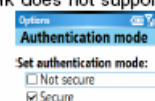
10. Check your network and security options

Press "Menu" and then "Network Options". The Cryptech default network configuration ("v.110" protocol and "transparent mode") is optimised for most situations. However in some cases, for example where the GSM network does not support data roaming or the v.110 protocol, it is advisable to select the "v.32" protocol in the "CSD Line" field.

Concerning user security, you can access the authentication area ("Menu", "Security Options", "Authentication mode") to check/manage the authentication mode. You can choose between "secure" (the user authentication password is required every time Cryptech is launched) and "no secure" (the password will not be required). We strongly suggest keeping the "secure" mode.



For security reasons, we recommend not to enable Bluetooth® and GPRS connections (including those used to send/receive MMS). Also avoid installing or running applications other than those provided with the device.



CRYPTTECH® MOBILE ENCRYPTION FOR SECURE COMMUNICATIONS

Casptech presents the latest CRYPTTECH release, the ultimate solution for GSM communications protection. Now available on new and most attractive devices, Crypttech benefits from a new audio solution that ensures complete absence of echo and provides best voice quality, comparable to that of a traditional phone call.

Crypttech does not require special installation processes or complex settings. The user only needs to enter his authentication password and, if desired, the static shared keys. The AES256 algorithm, with symmetrical keys, ensures the best protection against any kind of wiretapping.

The keys used to encrypt a call are generated according to two methods: when the static keys method is used, these are entered by the user, while with the Diffie - Hellman 2048 bit protocol, dynamic session keys are automatically generated at every call and deleted at the end of it. Both methods can be used to generate a single combined key. It is also possible to make an encrypted call using only one method, either shared keys or the Diffie - Hellman protocol. This latter enables, for instance, encrypted calls between users from different organisations who have no opportunity to define shared keys. The static keys storage areas is password-protected and the keys are always displayed in hash form only, thus ensuring full protection in case of theft or accidental loss of the device.

Crypttech is based on a high-level encryption technology, nevertheless it's very simple to use thanks to its user-friendly interface. The system turns voice into data, encrypts it and sends it in real-time through the GSM data channel to the other device, ensuring end-to-end encryption.



CRYPTTECH®

THE REAL ONE TO ONE CONNECTION

The CRYPTTECH® kit consists

- 1 smartphone with pre-configured Crypttech System
- 1 AC adapter
- 1 USB cable for PC connection/synchronization (USB to MINI-USB)
- 1 stereo headset with volume control
- 1 Smartphone User Manual
- 1 Crypttech User Manual and Quick Start Guide

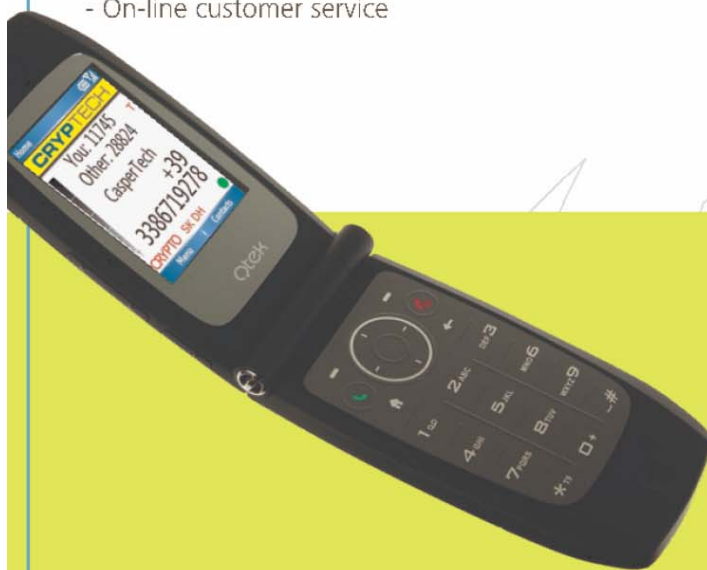


Standard features of CRYPTTECH®:

- Available for Microsoft Windows Mobile® 2005 on Pocket PCs and Smartphones
- Secure communications over all GSM networks (850/900/1800/1900 MHz)
- High audio quality of encrypted calls with Echo Suppression
- User-friendly interface
- Automatic selection of incoming crypto/clear calls
- End-to-End encryption with AES 256 algorithm and any of the following options
 - o Static Keys personally inserted by customer
 - o Dynamic Keys generated with Diffie-Hellman 2048 bit protocol
 - o Integration of both systems
- Authentication system customizable by the user
- Secure encryption keys storage

Optional CRYPTTECH® features, on demand:

- SmsCRYPTTECH
- File crypto Mobile/Desktop
- Customization of encryption algorithm on user demand
- Application for central Key Management System from Pc
- MicroSD with physical random number generator according to FIPS 140-2, certified EAL5+
- On-line customer service



Processor TI OMAP™ 850 195 Mhz
 Quadriband GSM/GPRS/EDGE
 Memory 64/128Mb ROM, 64Mb RAM
 Memory expansion miniSD/microSD
 Camera: CMOS 1.3/2.0 Mpixel
 Wi-Fi® IEEE 802.11 b/g
 Bluetooth® 1.2/2.0 e infrared

Smartphone





If you would like further Information about ELAMAN,
or would like to discuss a specific requirement or project, please contact us at:

Elaman GmbH
German Security Solutions
Seitzstr. 23
80538 Munich
Germany

Tel: +49-89-24 20 91 80
Fax: +49-89-24 20 91 81
info@elaman.de
www.elaman.de