

CRYPTTECH[®] 2G AGAINST EAVESDROPPING **THE SECURE ANTI SPY MOBILE**

Casper Technology developed the CRYPTTECH 2G solution for mobile phones to guarantee the maximum security against tapping.

In order to engage a secure communication, both parties involved in the conversation must use a Crypttech device, because the voice is encrypted and sent through the CSD data/fax channel of the standard GSM network to the other phone that decodes and plays the voice in real time.

Nobody will be able to steal your private contacts or encryption keys employed for secure communications. Crypto SMS messages sent from this phone cannot be decoded by anyone except you and your partner.

Using and configuring Crypttech is simple and intuitive. When a crypto call is being received, the phone starts a silent data exchange for the generation of the encryption keys, at the end it starts ringing and showing the Crypttech interface that confirms to the user that the call is secured.



CRYPTTECH®

THE REAL ONE TO ONE CONNECTION

The security of the communication is set at the highest level. The encryption is made with AES 256 and the keys are generated with Elliptic Curve Diffie Hellman 571 bit protocol. Keys are generated at the beginning of each call and destroyed as soon as the call ends. As well as dynamic keys generated during each call, users can set the phone to encrypt conversations with pre-shared keys directly keyed in and mixed by the software with the dynamic key. This process takes the benefit of Diffie-Hellman and generates different encryption keys for each call, but with the additional authentication provided by the pre-shared key.

SMS messages are encrypted with a password generated automatically during the first crypto call with the contact and assigned to it in the crypto phonebook. In this way users do not need to mess with encryption passwords, they only have to write the text and the phone will do it all automatically.

The Cryptech 2G solution can be used all over the world where GSM network and CSD data service are available. The solution is available for Symbian , Windows Mobile and Linux operating systems



- Available for Nokia Symbian S60 FP1 and FP2, HTC Windows Mobile and Linux
- AES 256 bit or custom algorithm defined by customer
- Elliptic Curve Diffie-Hellman 571 bit key generation protocol
- Key 256 bit long directly insert by user or trough KMS
- Authomatic key generation per contact for sms encryption
- Algorithm AES256, SHA2, RDNG, DH compliant to FIPS specifications

CASPERTECH
TRUST IN COMMUNICATIONS

Casper Technology s.r.l. - www.caspertech.com - info@caspertech.com
Operation and Sales: via Cardinal Massaia 83 - 10147 Torino - Italia
Tel +390112303634 - Fax +390112303632