



CRYPTO CALL

Gen-3 Cellular Encryption

EXTRA SECURE MOBILE COMMUNICATION & SMS



Instant Secure Communication

The Crypto-Call ensures that VOICE & SMS information can be sent from anywhere in the world to other Crypto-Call cellphone within a few seconds. With Crypto-Call, a simple call is to be placed to HQ and a conversation can take place to aid instant decision making.

Non Tapping Solution

The data transferred over the GSM networks is HEAVILY encrypted, where the users can be assured that **no one will be able to listen in** as they are over a data line which is heavily encrypted. At no point is any data sent over a voice channel or is in clear text type transfer.

Security

The Secret Keys can be changed by users at any time, to ensure that keys cannot be hacked by a listening party. The Secret keys can be entered by the users at any time, changing the key regularly will help in maintaining a high level

1st IN THE WORLD

Crypto VOICE & SMS on Nokia E90 & Other New Nokia handphnes

Changable Secret KEY

WITHOUT CRYPTO-CALL SOMEONE MAYBE LISTENING TO YOU



Features :

- Absolutely no back doors - encryption keys are CHANGABLE UP TO 36 CHARACTER
- Call & sms log protected by private password
- Certification - Crypto-Call™ Group Ltd are certified by the Israeli Ministry Of Defense
- Complete end to end protection, from phone to phone, for Cellular conversation
- Dual combination of asymmetric and symmetric encryption
- Automatic generation of RSA 1024 / AES 256 encryption keys on the phone itself
- Low audio latency (low delay)
- High audio quality 1024 RSA Bit asymmetric master key pairs AES 256 Bit symmetric data protection algorithm implemented
- Diffie-Hellman Key exchange algorithm
- 1024 Bit random master key automatically generated per contact
- 1024 Bit random master key automatically replaced at every call start
- 256 Bit random session key, replaced every second

Layer 1:

1024 bit RSA asymmetric encryption.
According to a study conducted by the University of British Columbia, the number of MIPS years required to crack a 1024-bit key would come to an amazing 300,000,000,000!

Layer 2:

256 bit AES symmetric encryption.
"The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths." (The USA government finds AES 256 secure enough for data classified up to TOP SECRET).