

CRYPTTECH® 3G

MOBILE ENCRYPTION

FOR SECURE COMMUNICATIONS

Cryptech® 3G by Casper Technology has been designed for the best protection of mobile VoIP communications from all types of wiretapping. The CRYPTTECH 3G solution enables encryption of voice and data over telecommunications networks such as GSM, EDGE, GPRS, WCDMA, UMTS, HSDPA, HSUPA, WiFi, and Satellite.

The only prerequisite to communicate in secure mode is that both parties use CRYPTTECH 3G phones. The encryption is end-to-end, that is, voice and data are encrypted on the device and can be decrypted only by a phone equipped with the same technology.

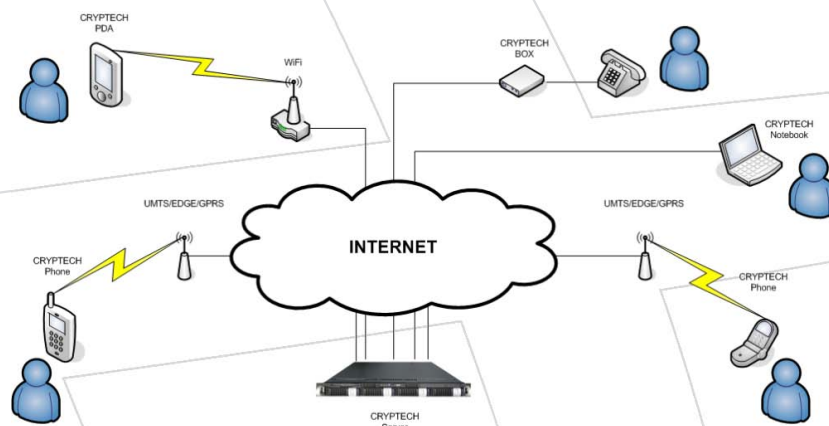
The whole procedure takes place in a quick, simple and intuitive way. The bandwidth offered by new mobile networks enables an excellent quality of voice, equal to that of a normal phone call.

The CRYPTTECH VoIP technology ensures the anonymity of the call, since it does not use a switched phone line, but an Internet IP packet

connection. CRYPTTECH 3G does not use a standard protocol, such as SIP, but has been developed based on a proprietary protocol to offer fast performances and a high security level.

The CRYPTTECH 3G telephones connect to each other through a server that acts as a transparent link. Thanks to the end-to-end encryption, even the unlikely event of an attack to the server would only lead to the wiretapping of an unintelligible data stream. In order to communicate with another user connected to the same server, the caller only needs to know the number (or alias) of the user, whose anonymity and protection of privacy are thus guaranteed. Customers with a limited number of phones can use the CasperTech own server, which will manage the link among the users against payment of a connection fee.

CRYPTTECH 3G can also use WiFi connectivity in offices, homes or public hot-spots. In addition, several network service providers offer flat rates for mobile internet access. In this case, the encrypted calls will be included in the flat rate.



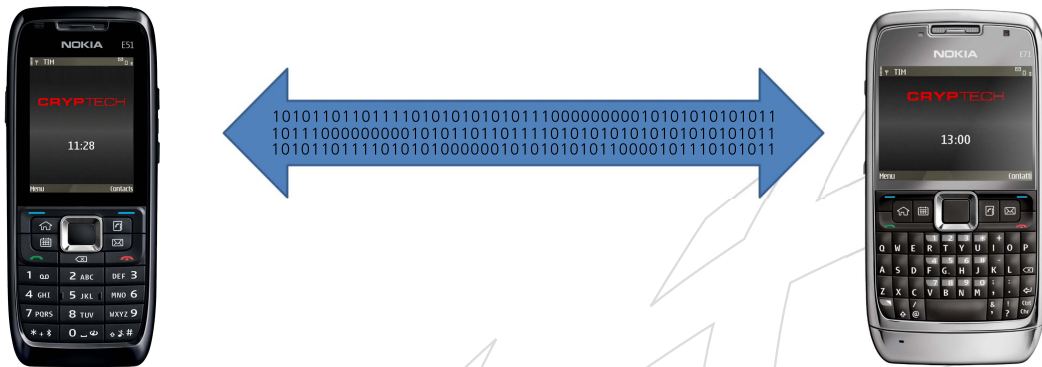
CRYPTTECH® 3G

THE REAL ONE TO ONE CONNECTION

Customers with the need to manage a larger user base, and who want to retain full control of the communication infrastructure, can purchase the compatible solution CRYPTTECH SCS, with an independent server that enables a fully autonomous network management.

CRYPTTECH 3G combines a great simplicity that makes it manageable by every user, with all the security features that meet military-level requirements: dual system for management of encryption key (shared and automatic), possibility to customize the algorithm, compatibility with the Key Management System for remote key distribution and management.

To provide the best quality ever, a new audio coding system was designed that constantly adjusts itself to the properties of the network to which the phone is connected. The system automatically adjusts audio encoding to the type of network (WIFI / UMTS / EDGE / GPRS), thus ensuring at all times the best ratio voice quality/delay. Similarly, the transition from a 3G UMTS network to a 2G GPRS/EDGE during a call is handled automatically, in order to prevent service discontinuity on the network.



- AES 256 bit or encryption algorithm customized/ deployed by user;
- Key generation with Diffie-Hellman 4096 bit protocol or Elliptic curve Diffie-Hellman 571 bit ;
- Keys 256 bit long directly inserted by user or centrally managed by Key Management System;
- SMS text messages encryption key automatically generated per-user during crypto calls;
- Remote localization and wipe of the whole device in case of theft or SIM card unauthorized replacement;
- FIPS compliant AES256, SHA2, RDNG and DH algorithms.
- Available for Symbian Nokia S60 FP1 and FP2, Windows Mobile HTC and soon also for Android and Blackberry

CASPERTTECH
TRUST IN COMMUNICATIONS

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