

# CRYPTTECH® LINUX

Casper Technology has developed CRYPTTECH Linux, the best solution for protection of mobile communications on GSM networks.

The device provides the tightest defence against any type of wiretapping. The CRYPTTECH technology has been developed on the Linux Operating System. This approach offers total control of the device and its communication peripherals, enabling the development of a “hardened” phone, from which all functions that are either not relevant or may impair the security of the device have been removed.

Bluetooth, GPRS and the USB port have been locked, making the telephone immune against any type of virus or spyware. Furthermore, thanks to the full control offered by the Linux Operating System, it is possible to guarantee the total absence of back-doors, including outside the CRYPTTECH software.

The telephone can be used both for voice calls and SMS text messages in normal or encrypted mode. The user can choose whether to use the encrypted mode only, thus avoiding the risk of accidentally making calls or sending text messages that could be wiretapped.

CRYPTTECH Linux is very simple to use, and offers at the same time an extremely high-level security.



# CRYPTTECH®

## THE REAL ONE TO ONE CONNECTION

The communication is protected by an end-to-end encryption of the conversation; therefore both interlocutors must be using a CRYPTTECH phone in order to speak securely.

The whole procedure is quick, simple and intuitive.

Thanks to its processing power, the CRYPTTECH Linux telephone offers high performances and an audio quality of the encrypted call equivalent to that of a normal call.

CRYPTTECH Linux enables a secure communication on all GSM 850/900/1800/1900 networks and guarantees worldwide usability. The encryption is performed with the AES 256 algorithm. It normally uses keys generated at each call through Diffie Hellman protocol with Elliptical Curves at 571 bits and immediately destroyed at the end of the call. Optionally, the system can use symmetric keys defined by the users, either in place of the Diffie-Hellman dynamic keys or in addition to them, thus guaranteeing a double level of security.

It is also possible to replace the encryption methods delivered with the CRYPTTECH software with other algorithms, such as AES256 with Diffie-Hellman 4096 bit, or with others defined by the customer. The whole encryption function is automatic and does not require any intervention by the user. In the case of loss or theft, the telephone can be remotely localised and its content completely erased. In any case, without the user password it is impossible to extract data, text or contact information, even with the most sophisticated tools.

SMS, like voice calls, are encrypted. For the encryption of SMS the software uses keys automatically generated during the first encrypted phone-call to a contact. These are associated to the contact itself and remain in use for all SMS, until a subsequent call generates a new set of keys.

#### TECHNICAL SPECIFICATIONS

- Telephone with Linux operating system, hardened for protection against viruses, Trojan horses, spyware
- Encryption algorithm: AES 256 bits or encryption algorithm defined by the client
- Key generation with Diffie-Hellman protocol at 4096 bits or Diffie-Hellman with Elliptic Curves at 571 bits
- Keys 256 bits directly inserted or generated by the user or managed via KMS (Key Management System)
- Automatic key generation per contact for encrypted text messages
- Algorithms in compliance with FIPS specifications
- Remote localisation and content deletion in case of loss/theft via central key management (KMS)

**CASPERTECH**  
TRUST IN COMMUNICATIONS

Casper Technology s.r.l. - [www.caspartech.com](http://www.caspartech.com) - [info@caspartech.com](mailto:info@caspartech.com)

Operation and Sales: via Cardinal Massaia 83 - 10147 Torino - Italia

Tel +390112303634 - Fax +390112303632