

# CRYPTTECH® 2G

## LA TECNOLOGIA

### PER LA PROTEZIONE

### DELLE COMUNICAZIONI

Casper Technology ha realizzato CRYPTTECH® 2G, la soluzione per la protezione delle comunicazioni mobili su reti GSM.

Con questo sistema è possibile difendere la propria privacy dalle intercettazioni.

La protezione avviene mediante la cifratura end-to-end della conversazione; entrambi gli interlocutori devono utilizzare un telefono CRYPTTECH® per parlare in modalità sicura.

CRYPTTECH® è sistema molto semplice da utilizzare, pur avendo caratteristiche di sicurezza di livello militare. Il software si integra completamente con il telefono; per telefonare in modalità crypto basta richiamare l'interfaccia CRYPTTECH® con il pulsante assegnato, inserire il contatto per mezzo della rubrica cifrata o digitandolo sulla tastiera e premere il tasto verde. Per la ricezione di una telefonata cifrata, Crypttech si attiva automaticamente e mostra all'utente l'interfaccia che distingue in modo chiaro il tipo di telefonata.

I dispositivi CRYPTTECH® sono tutti compatibili indipendentemente dal sistema operativo utilizzato, sia esso Symbian, Linux o Windows Mobile.



# CRYPTTECH®

## THE REAL ONE TO ONE CONNECTION

CRYPTTECH® permette la comunicazione sicura su tutte le reti GSM 850/900/1800/1900 tramite il canale dati/fax CSD e garantisce quindi l'utilizzo in tutto il mondo.

La cifratura è effettuata con l'algoritmo AES 256 e vengono utilizzate chiavi generate ad ogni telefonata con il protocollo Diffie Hellman a Curve Ellittiche a 571 bit, chiavi che vengono distrutte immediatamente alla fine di ogni conversazione.

Oltre alle chiavi generate sul momento (quindi imprevedibili e non ripetibili) il sistema utilizza chiavi simmetriche definite dagli utenti, garantendo così un doppio livello di sicurezza.

Tutta la funzione di cifratura non richiede alcun intervento da parte dell'utente. Senza la password utente non è comunque possibile modificare le impostazioni o leggere gli sms e i contatti protetti.

Gli SMS, al pari della voce, sono cifrati. Le chiavi di cifratura vengono generate automaticamente durante la prima telefonata cifrata ad un contatto ed associate al contatto stesso. Ad ogni telefonata successiva le chiavi vengono rinnovate. In questo modo viene anche garantita l'autenticazione dei messaggi inviati e ricevuti.



- Disponibile per telefoni NOKIA Symbian S60 FP1 e FP2, HTC Windows Mobile e telefono Linux dedicato
- AES 256 bit o algoritmo di cifratura definito dal cliente
- Generazione chiavi con protocollo Diffie-Hellman a 4096 bit o Diffie-Hellman a Curve Ellittiche a 571 bit
- Chiavi a 256 bit direttamente inserite o generate dall'utente o gestite da KMS
- Generazione automatica chiavi per contatto per gli sms cifrati
- Algoritmi AES256, SHA2, RDNG, DH conformi alle specifiche FIPS

**CASPERTECH**  
TRUST IN COMMUNICATIONS

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