

CRYPTTECH® LINUX LA TECNOLOGIA PER LA PROTEZIONE DELLE COMUNICAZIONI

Casper Technology ha realizzato CRYPTTECH Linux, la migliore soluzione per la protezione delle comunicazioni mobili su reti GSM.

Questo dispositivo consente la massima difesa da qualunque tipo di intercettazione.

La tecnologia CRYPTTECH è stata sviluppata sul Sistema Operativo Linux. Tale approccio permette il totale controllo dell'apparecchio e delle sue periferiche di comunicazione, consentendo di creare un telefono "hardened" nel quale sono state eliminate tutte le funzioni non rilevanti o che potrebbero mettere a rischio la sicurezza del dispositivo.

Il Bluetooth, il GPRS e la porta USB sono stati chiusi, rendendo il telefono immune da qualsiasi tipo di virus o spy software. Inoltre, sempre grazie al controllo completo offerto dal Sistema Operativo Linux, si può garantire l'assoluta assenza di backdoors anche esterne al software CRYPTTECH.

Il telefono può essere usato sia per le chiamate vocali che per gli SMS in modalità normale o cifrata; l'utente può scegliere di usare solo la modalità cifrata, evitando che vengano effettuate involontariamente chiamate o sms intercettabili. CRYPTTECH Linux è un telefono molto semplice da utilizzare, pur avendo caratteristiche di sicurezza di livello elevatissimo.



CASPERTECH
TRUST IN COMMUNICATIONS



CRYPTTECH®

THE REAL ONE TO ONE CONNECTION

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

Tutto il procedimento avviene in modo rapido, semplice e intuitivo.

Il telefono CRYPTTECH Linux, essendo dotato di un'elevata capacità di calcolo, riesce a fornire alte prestazioni ed una qualità vocale della telefonata cifrata pari a quella di una telefonata normale.

CRYPTTECH Linux permette la comunicazione sicura su tutte le reti GSM 850/900/1800/1900 e garantisce quindi l'utilizzo in tutto il mondo.

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

A scelta, il sistema può utilizzare chiavi simmetriche definite dagli utenti stessi, sia in alternativa alle chiavi generate con il protocollo Diffie Hellman, sia in aggiunta ad esse, garantendo in tal caso un doppio livello di sicurezza. E' anche possibile sostituire ai sistemi di cifrature forniti con il software CRYPTTECH altri algoritmi, quali l'AES256 con protocollo Diffie-Hellman a 4096 bit, oppure algoritmi scelti dal cliente.

Tutta la funzione di cifratura avviene in modo automatico e non richiede alcun intervento da parte dell'utente.

In caso di smarrimento o furto il telefono può essere localizzato e il suo contenuto interamente cancellato da remoto.

Senza la password utente non è comunque possibile estrarre dati, sms o contatti, anche con gli strumenti più sofisticati.

Gli SMS, al pari della voce, sono cifrati. Per la cifratura degli SMS vengono utilizzate chiavi generate automaticamente durante la prima telefonata cifrata con il contatto. Queste vengono associate al contatto stesso e rimangono in uso per tutti i messaggi finché una successiva telefonata non le sostituisce con nuove chiavi.

SPECIFICHE TECNICHE

- Telefono con sistema operativo Linux, trasparente ma chiuso per proteggere da virus, trojan, spy software
- Algoritmo di cifratura: AES 256 bit o algoritmo di cifratura definito dal cliente
- Generazione chiavi con protocollo Diffie-Hellman a Curve Ellittiche a 571 bit (default), oppure Diffie-Hellman a 4096 bit (opzionale)
- Chiavi simmetriche a 256 bit direttamente inserite o generate dall'utente oppure gestite da KMS (Key Management System) e utilizzabili in alternativa al protocollo Diffie-Hellman o in combinazione con esso
- Generazione automatica chiavi per contatto per gli sms cifrati
- Algoritmi conformi alle specifiche FIPS
- Localizzazione del telefono in caso di furto/smarrimento con possibilità di cancellazione remota del contenuto, tramite l'uso del KMS

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