



1. Prerequisiti

Per poter eseguire telefonate cifrate, assicurarsi di avere il canale dati UMTS attivo e configurato rispetto alla propria scheda SIM (verificare presso il proprio operatore telefonico). Assicurarsi di aver un contratto conveniente per la trasmissione dati.

2. Avvio dell'applicazione

L'applicazione Cryptech si avvia automaticamente all'accensione del dispositivo. Apparirà la schermata di Cryptech. Se l'applicazione rimane inattiva per troppo tempo, verrà inviata in secondo piano dal sistema operativo Windows Mobile (cioè non vedrete la schermata di Cryptech sullo schermo del dispositivo). Per riattivarla, è sufficiente selezionare "Menu" dalla Home Screen di Windows Mobile e cliccare sull'icona Cryptech disponibile sul display.

3. Impostazione account voip

Per collegarsi alla rete voip ed essere raggiungibili si dovrà prima di tutto impostare il nome utente (generalmente il numero di telefono con prefisso internazionale) e la password relativa all'account. Per fare ciò si premerà menù>Voip>impostazioni. Se si utilizza Cryptech 3G sporadicamente o si vuole essere raggiungibili solo in certi momenti della giornata si consiglia di togliere la spunta a "connetti all'avvio" se non si vuole che il sistema si connetta automaticamente ad ogni avvio del telefono, consumando di conseguente batteria e traffico dati.

4. Connessione server Voip

Per poter chiamare o essere raggiungibili in modalità crypto, Cryptech 3G deve essere collegato al server Voip. Se il sistema è impostato su "connetti all'avvio", all'avvio del telefono si aprirà automaticamente una connessione dati e verrà confermato dalla scritta VOIP in verde sulla schermata principale di Cryptech 3G. Se la scritta appare in grigio vuole dire che si è sconnessi o che è disabilitata la connessione all'avvio; in tal caso premere menù>Voip>connetti. Se al posto della scritta voip appaiono dei puntini verdi, vuol dire che il sistema sta tentando di connettersi. Se lo stato dei puntini persiste significa che c'è un problema con la connessione (verificare configurazione rete operatore o traffico disponibile). La connessione con il server Voip serve solo a mettere in comunicazione gli utenti, la cifratura avviene sempre e solo tra i telefoni stessi.

5. Consumo e traffico dati

Quando si è in comunicazione si consumano all'incirca 3,5 KB al secondo sotto rete umts/wifi, sotto copertura gprs/edge all'incirca 2KB al secondo. Quando Cryptech 3G è a riposo ma connesso al server voip il consumo dati è di circa 1 KB al giorno. E' importante considerare i suddetti parametri per poter stipulare un contratto dati adeguato e non rischiare di spendere in modo eccessivo inconsapevolmente. Si suggerisce di attivare una tariffa flat dati con il proprio operatore. Il consumo della batteria può risentire dell'utilizzo di Cryptech 3G anche quando a riposo, si suggerisce quindi la connessione al server voip solo nel periodo di utilizzo.

6. Esecuzione di una chiamata cifrata

Nella schermata di Cryptech, per eseguire una chiamata cifrata, è sufficiente digitare il numero direttamente sulla tastiera o importarlo dalla rubrica (selezionare "Contatti" e scegliere il contatto desiderato tra quelli di Outlook Mobile). Premere quindi il tasto verde di chiamata, dopo una breve fase di sincronizzazione, la chiamata sarà attiva. Durante la sincronizzazione verrà visualizzata una barra di avanzamento, al riempimento della stessa la comunicazione cifrata avrà inizio. Se la barra diventa rossa significa che si sta effettuando una ritrasmissione di dati a causa di errori nella connessione.

Per modificare il volume durante la chiamata utilizzare le frecce su/giù del tasto laterale. Il volume può anche essere impostato per tutte le chiamate selezionando Menu>Audio nella schermata Cryptech.

7. Ricezione di una chiamata cifrata

Per rispondere alla chiamata cifrata è sufficiente premere il tasto verde quando si sente lo squillo. Dopo pochi secondi in cui viene generata la chiave di cifratura ed al completamento della barra di riempimento sullo schermo si potrà iniziare a parlare in modo sicuro.

8. Generazione automatica chiave per SmsCryptech

Ad ogni telefonata crypto viene generata automaticamente una chiave associata al contatto in modo da potersi scambiare successivamente sms criptati con il contatto senza doverla concordare.

Durante la connessione sullo schermo apparirà una chiave verde che conferma la generazione e il salvataggio della chiave nella rubrica cifrata di SmsCryptech da entrambe le parti. Ad ogni nuova chiamata crypto la chiave per l'sms verrà rinnovata.

9. Utilizzo rete UMTS,EDGE,GPRS,WIFI

Cryptech 3G è stato progettato per poter utilizzare qualunque rete di comunicazione internet disponibile sul telefono. E' importante configurare prima di tutto le impostazioni per la rete umts in modo che si possa essere sempre raggiungibili. Quando si è in vicinanza di router wifi (ad esempio in ufficio o in un hotspot pubblico) basta accendere sul telefono il wifi, configurare eventualmente la chiave di accesso, ed utilizzare Cryptech 3G su tale rete. In questo modo il traffico generato non influirà sulla bolletta telefonica. Si possono avere anche più connessioni attive (umts e wifi) in tal caso il telefono farà automaticamente passare il traffico sul wifi e tornerà ad utilizzare l'umts appena il wifi non è più disponibile. Cryptech 3G si può utilizzare anche in movimento ma in tal caso ci possono essere dei problemi di trasmissione relativi all' HANG OVER tra una cella e l'altra. questi problemi si manifestano come dei buchi nella comunicazione o dei ritardi nella trasmissione, che vengono recuperati non appena possibile. La qualità dell'audio e del ritardo si adattano continuamente ed in tempo reale in relazione alle prestazioni della rete. Se ci si trova in una zona con copertura GPRS o EDGE, la qualità sarà leggermente inferiore dovendosi adattare alla banda disponibile ed il ritardo sarà superiore per poter rendere la conversazione fluida nonostante l'irregolarità della trasmissione. In particolare il passaggio da una cella UMTS ad una GPRS e viceversa può generare un buco di diversi secondi.

10. Impostazione password di autenticazione utente

La password di autenticazione utente è utilizzata per controllare l'accesso all'applicazione Cryptech. Si raccomanda di impostare una password sicura (almeno 8 caratteri) Per impostare la password di autenticazione utente selezionare dalla schermata Cryptech la voce Menu>Opzioni>Password Utente. Verrà richiesto di inserire la password due volte quindi cliccare su "Fatto".

E' ora possibile impostare il dispositivo in maniera che venga chiesta la password ad ogni avvio, selezionando Menu>Opzioni>Modalità di autenticazione. In questa finestra è possibile scegliere tra "sempre" (la password di autenticazione verrà chiesta ad ogni avvio di Cryptech o del dispositivo) e "mai" (la password non verrà più chiesta).

In questa sezione è possibile anche abilitare/disabilitare l'autenticazione alla lista chiamate ed ai contatti cifrati



Non dimenticare assolutamente la password di autenticazione utente poiché senza di essa Cryptech non potrà funzionare e sarà necessario contattare la Casper Technology s.r.l. per la sostituzione/ripristino del software.



Per ragioni di sicurezza, si raccomanda di abilitare il Bluetooth® solo quando strettamente necessario. Evitare inoltre di installare o eseguire applicazioni all'infuori di quelle fornite con il dispositivo.

Per mantenere in funzione il software di cifratura è necessario non eseguire mai l'operazione di hard-reset che riporta il telefono nel suo stato iniziale e rimuove ogni applicazione installata sul dispositivo.

11. Personalizzazione delle chiavi crittografiche

Le chiavi crittografiche statiche vengono condivise da tutti i dispositivi utilizzati per parlare in modalità cifrata tra di loro, e vengono utilizzate per cifrare l'intera conversazione. Sono spesso definite anche chiavi "simmetriche" o "condivise", in quanto devono essere identiche per entrambi gli interlocutori.

Premere "Menu", "Opzioni" e "gestione chiavi". Creare almeno una chiave crittografica, selezionando "nuova", quindi digitando "1" nel "Liv. Priorità" e la password prescelta nello spazio sottostante.

Per immettere una chiave si può scegliere tra Text mode (impostazione di default) e Hex mode. La maggior parte degli utenti può utilizzare semplicemente il Text mode, digitando le chiavi di cifratura utilizzando tutti i caratteri disponibili. La modalità Hex mode è stata inclusa per utenti di una certa esperienza, e richiede che i caratteri inseriti come chiave di cifratura siano quelli facenti parte della codifica esadecimale (0-9, A-F).

Il valore "1" indica "priorità massima", ed è necessario per anteporre le chiavi appena create alle password di "test" di Cryptech.

Una volta create le proprie chiavi, sarà possibile eliminare la password di test: selezionare la chiave, cliccare su "Menu", quindi "Gestione chiave" e infine su "Cancella chiave". E' importante ricordare di inserire le stesse password su tutti i dispositivi con i quali si intende comunicare, o considerare l'utilizzo del protocollo Diffie-Hellman per fare chiamate cifrate *senza condividere chiavi* di cifratura.

Da notare che le chiavi inserite in quest'area sono utilizzate per cifrare le conversazioni, a differenza della password di autenticazione utente inserita in precedenza che serve per accedere a Cryptech e proteggere/gestire le chiavi.

12. Contatti cifrati

Cryptech permette di aver dei contatti cifrati separati rispetto alla normale rubrica del telefono in modo da agevolare la chiamata dei contatti crypto ma soprattutto di proteggere la privacy dei contatti. Per accedere ai contatti è necessario inserire la password di autenticazione. Per creare un contatto cifrato si può sia inserirlo a mano, importarlo dalla rubrica Microsoft del telefono. Il sistema crea automaticamente il contatto cifrato alla ricezione o alla prima chiamata crypto con il contatto stesso. Se non si gradisce inserire la password di autenticazione ai contatti, questa può essere disabilitata da manu>opzioni>modalità autenticazione.

13. Lista chiamate

Cryptech tiene traccia delle chiamate crypto effettuate. L'accesso a tale lista è protetto dalla password, che può essere eventualmente disabilitato. In ogni caso la lista è temporanea ed allo spegnimento del telefono questa lista viene cancellata senza lasciare tracce sul telefono.

14. Gestione delle modalità di cifratura

Cryptech supporta due tipologie di chiavi: statiche (*condivise*) e dinamiche (basate sul protocollo Diffie-Hellman). Diversamente dalle chiavi statiche, il protocollo Diffie-Hellman non richiede intervento da parte dell'utente: abilitando tale opzione, all'avvio della telefonata verrà generata una chiave di cifratura dinamica che verrà poi cancellata in modo sicuro al termine.

Entrambi i tipi di chiavi – statico e dinamico – garantiscono sicurezza assoluta, va però tenuto conto anche del "fattore umano". Le chiavi statiche devono essere condivise da tutti gli interlocutori e, se il loro numero cresce sostanzialmente, si corre il rischio che qualcuno possa compromettere alcune chiavi. Nel protocollo Diffie-Hellman, c'è la possibilità remota che un intruso comprometta la creazione della chiave dinamica durante la sincronizzazione iniziale (questo attacco è chiamato *man-in-the-middle*). Cryptech protegge da questo tipo di attacco generando dei codici numerici di autenticazione che compaiono sul display durante la telefonata. Entrambi gli interlocutori dovrebbero comunicarsi a voce questi codici: se coincidono, significa che la chiamata non è stata compromessa. Poiché gli utenti possono dimenticare tale precauzione, Cryptech può combinare chiavi statiche e dinamiche eliminando così persino il rischio della "negligenza umana". In ogni caso, sono disponibili varie opzioni per fornire la massima flessibilità di utilizzo.

Cryptech è pre-configurato con un alto livello di sicurezza, cioè la combinazione di chiavi statiche e dinamiche. E' però possibile impostare la Sicurezza selezionando "Menu", "Opzioni" e quindi "Sicurezza":

1. Chiave condivisa: può essere opzionale o richiesta. In questo modo si può escludere la comunicazione con dispositivi EasyCryptech che non hanno chiavi condivise oppure altri Cryptech che non abbiano una chiave in comune.
2. Diffie-Hellman: posso decidere se renderlo opzionale, richiesto o disabilitato. In questo modo si può forzare l'uso delle chiavi generate sul momento in abbinamento con le chiavi statiche oppure escludere l'utilizzo del Diffie-Hellman in modo da avere sempre il controllo sulla chiave utilizzata per la cifratura.
3. Il Diffie-Hellman genera le chiavi con calcoli che si basano sulle curve ellittiche a 571 bit (ECDH), se si toglie la spunta a questa funzione, si utilizzerà il Diffie-Hellman che genera chiavi derivandole da numeri primi di 4096 bit. In questo caso la generazione sarà più lenta e meno robusta nella sicurezza.
4. Si può decidere se la generazione delle chiavi per l'sms crypto deve avvenire in modo automatico durante la chiamata criptata con il contatto

15. Selezione lingua

Sotto opzioni>lingua si può selezionare la lingua che si vuole utilizzare per il software. di default è selezionata la stessa lingua del sistema operativo.