



Per poter eseguire telefonate cifrate, assicurarsi che il canale GSM DATI/FAX CSD sia abilitato nella propria scheda SIM (verificare presso il proprio operatore telefonico). Il canale dati è generalmente un servizio gratuito e, spesso, con l'attivazione vengono forniti un ulteriore numero di telefono per i dati e uno per i fax. Alcuni operatori non forniscono il canale CSD DATI/FAX.

1. Inizializzazione telefono Cryptech

Al primo avvio del telefono è richiesto di **impostare la password utente**, richiesta due volte per sicurezza. Prestare molta attenzione alla password prescelta, poiché sarà richiesta ad ogni accensione del telefono e per la modifica delle impostazioni di sicurezza. Annotare la password utente in un luogo sicuro poiché senza di essa non sarà più possibile utilizzare ed accedere ai dati presenti sul telefono. In seguito sarà possibile **cambiare la password** selezionando il menù *Impostazioni (4) > Generale (1) > Sicurezza (1) > Password utente (2)*. Nel presente manuale, quando s'illustreranno le voci di menù da premere per attivare determinate funzioni, si farà seguire al nome del menù il numero corrispondente nella tastiera che permette di selezionare velocemente tale voce senza doversi spostare con le frecce su/giù sul menù. Ad esempio, nella spiegazione relativa al cambio password poche righe più in alto, l'impostazione è raggiungibile premendo il tasto Menù e quindi in successione i numeri 4, 1, 1 e 2 (corrispondenti alle voci di menù "Impostazioni", "Generale", "Sicurezza" e "Password utente").

Una volta inserita la password apparirà la schermata nera con il logo CRYPTTECH, il nome dell'operatore e l'orologio. Per **impostare data e ora** selezionate il menù *Impostazioni (4) > Generale (1) > Data e ora (3)*.

2. Telefonate criptate e in chiaro

Il telefono è configurato, nelle sue impostazioni di fabbrica, per eseguire e ricevere solo telefonate e SMS cifrati. Questa configurazione è consigliata poiché garantisce che tutte le telefonate ricevute e d'effettuate dal telefono siano sicure contro le intercettazioni. In questo modo si evita anche l'errore umano nell'utilizzo, impedendo completamente l'esecuzione di telefonate in chiaro (quindi non protette dalle intercettazioni).

Chi ha necessità di usare lo stesso apparecchio telefonate ed SMS normali (in chiaro, quindi intercettabili come su di un telefono tradizionale), può abilitare la **funzionalità di telefono in chiaro** accedendo al menù *Abilita Chiamata Standard (7)*. Finché non si abilita la chiamata standard non si potrà ne chiamare ne ricevere chiamate in chiaro e stessa cosa anche per gli sms normali.

Abilitando questa funzione si potrà passare dalla funzione di telefono in chiaro a quella di telefono crypto premendo il tasto con la nota, rappresentato qui di fianco. Per fare telefonate cifrate si dovrà digitare il numero o il contatto da chiamare accertandosi di trovarsi nella schermata nera con il logo CRYPTTECH rosso.

Per **fare una telefonata normale** (quindi non criptata e intercettabile) basterà premere il tasto con la nota e si vedrà comparire la schermata bianca con l'operatore e l'orologio in primo piano. Qualunque telefonata effettuata da questa schermata non sarà protetta.

3. Autenticazione

Ogni volta in cui si desidera passare dalla funzione di telefono normale (in chiaro) a quella di telefono criptato verrà richiesta la password utente (questo per impedire che utenti non autorizzati accedano al telefono criptato). Se si desidera, si può modificare tale impostazione per **abolire la richiesta di password** o impostare politiche più restrittive. Per le impostazioni relative alla sicurezza dell'autenticazione, selezionare il menu *Impostazioni (4) > Generale (1) > Sicurezza (1) > Autenticazione (3)*. Qui si potrà decidere se impostare l'autenticazione per accedere ai contatti, al registro chiamate, agli SMS oppure ogni volta che si chiude lo sportellino del

telefono, o ancora se si vuole disabilitare l'autenticazione nel passaggio da funzionalità di telefono in chiaro a quello crypto.

4. Effettuare una chiamata cifrata

Per fare una chiamata cifrata sarà sufficiente digitare il numero della persona da chiamare dalla schermata nera CRYPTTECH oppure selezionarlo dalla rubrica. Il telefono ricevente (che dovrà aver un telefono Cryptech e possedere una sim abilitata al traffico dati CSD) riceverà la telefonata. In maniera silenziosa, inizierà a scambiare dati di sincronizzazione per generare e concordare una chiave di cifratura in maniera sicura (la barra sullo schermo segnerà l'avanzamento del processo di generazione della chiave). Al termine della fase di sincronizzazione – nel momento in cui la barra di avanzamento avrà completato il suo riempimento – il telefono del ricevente inizierà a squillare. Per rispondere alla telefonata, il ricevente dovrà semplicemente aprire lo sportellino del telefono e premere il tasto verde. Se sul telefono del ricevente è stata impostata l'autenticazione, verrà richiesta la password utente per poter rispondere al telefono premendo il tasto verde

5. Ricevere una chiamata

Quando il telefono riceve una chiamata, automaticamente propone l'interfaccia in chiaro oppure in crypto in modo che chi risponde sappia in anticipo il tipo di telefonata che sta ricevendo. Per rispondere basterà **premere il tasto verde**. Se è attiva l'autenticazione, prima di poter premere il tasto verde per rispondere alla telefonata sarà necessario inserire la propria password utente nell'apposito campo.

6. Creazione delle proprie chiavi crittografiche

Il telefono Cryptech utilizza due sistemi di gestione delle chiavi: chiavi "statiche" inserite e generate dall'utente su ogni telefono e le chiavi "dinamiche" generate e distrutte automaticamente ad ogni telefonata. Per fornire il massimo della sicurezza, i due sistemi possono essere utilizzati contemporaneamente. Per **creare le proprie chiavi** si dovrà selezionare il menu *Impostazioni (4) > Telefono (2) > Chiamata Crypto CSD (1) > Gestione chiavi (3) > Chiavi utente (1)*.

In questa schermata si vedrà la prima chiave di test che è possibile utilizzare fino a che non viene inserita almeno una propria chiave di cifratura. Per **creare una nuova chiave** premere "nuova" nel menù in basso. Inserire il livello di priorità rispetto a tutte le altre chiavi (1 livello più alto) e sotto inserire la chiave di cifratura che si vuole utilizzare; più lunga è la chiave e più è sicura. La chiave appena inserita dovrà essere memorizzata allo stesso modo anche sul telefono dell'altro utente con cui si vuole parlare in cifrato. Una volta inserita la chiave, la si potrà solo veder sotto forma di codice HASH, un codice ricavato dalla chiave ma dal quale non si può risalire alla chiave stessa. La ragione della visualizzazione del codice HASH invece della chiave appena inserita è che per questioni di sicurezza bisogna poter verificare se due telefoni hanno la stessa chiave (quindi hanno lo stesso HASH) in comune senza visualizzare la chiave reale.

Il sistema trasformerà la chiave inserita in una stringa di 256 caratteri che sarà utilizzata dall'algorithm AES256 per cifrare le comunicazioni. Una volta create le proprie chiavi si può eliminare la chiave di TEST. Si possono inserire quante chiavi si desidera, è però essenziale che con ogni persona con cui si intende comunicare in criptato ci sia almeno una chiave in comune. Il telefono all'inizio di ogni telefonata

verificherà automaticamente se è presente una chiave condivisa e se ne è più di una, sceglierà quella con la priorità più alta.

7. Gestione delle modalità di cifratura

Cryptech permette di utilizzare due tipi di chiavi di cifratura: statica (condivisa) e dinamica (basata sul protocollo Diffie-Hellman). A differenza delle chiavi statiche, il protocollo Diffie-Hellman non richiede intervento da parte dell'utente: quando tale funzione è abilitata, ad ogni telefonata una nuova chiave dinamica verrà automaticamente creata e rimossa al termine della telefonata stessa. E' altresì possibile l'utilizzo contemporaneo di chiavi statiche e dinamiche, che garantisce sicurezza massima poiché le telefonate vengono in questo modo criptate con chiavi diverse ad ogni conversazione.

Per verificare che la chiave generata attraverso il protocollo Diffie-Hellman sia totalmente sicura (e che quindi nessun estraneo abbia intercettato i dati scambiati durante la generazione della chiave) l'applicazione visualizza due codici numerici di autenticazione sullo schermo, durante tutta la telefonata. **Nel caso in cui si utilizzi soltanto il protocollo Diffie-Hellman, è raccomandabile comunicare il codice corrispondente alla voce "Leggi" all'interlocutore, affinché egli verifichi la corrispondenza con il codice che egli visualizza in corrispondenza della voce "Senti". Egli dovrà, a sua volta, comunicarvi il suo codice e voi verificare che corrisponda a quanto leggete sullo schermo.** Se i codici numerici corrispondono, si ha la conferma che nessun estraneo si è intromesso nella telefonata. L'utilizzo contemporaneo di chiavi statiche e dinamiche elimina il rischio di intrusione – e quindi la necessità della verifica – intrinseco nell'utilizzo del protocollo Diffie-Hellman. E' altresì possibile selezionare diverse opzioni per fornire massima flessibilità di utilizzo.

Cryptech è pre-impostato nella configurazione di massima sicurezza (utilizzo contemporaneo di chiavi statiche e dinamiche), è comunque possibile modificare la configurazione di sicurezza dal menù *Impostazioni (4) > Telefono (2) > Chiamata crypto CSD (1) > Opzioni di sicurezza (2)*. Sono disponibili le seguenti opzioni:

Chiave condivisa [richiesta/opzionale]

Permette di selezionare se la chiave condivisa è opzionale o richiesta.

Diffie-Hellman [richiesto/opzionale/disabilitato]

Permette di scegliere se il protocollo di generazione automatico delle chiavi di cifratura Diffie-Hellman è opzionale, richiesto oppure disabilitato

ECDH [abilitato/disabilitato]

Abilitato come impostazione di fabbrica, indica che la generazione della chiave Diffie-Hellman (se richiesta) sarà eseguita utilizzando il metodo delle curve ellittiche di Koblitz a 571 bit. Se l'opzione ECDH è disabilitata, la generazione della chiave Diffie-Hellman avverrà attraverso il protocollo standard a 4096 bit, computazionalmente più pesante e ritenuto meno sicuro del protocollo a curve ellittiche ECDH. Nel caso in cui uno dei due interlocutori abbia disabilitato l'opzione ECDH, la generazione della chiave di cifratura avverrà attraverso il protocollo standard DH a 4096 bit.

E' opportuno selezionare le opzioni in base alle impostazioni concordate con il proprio interlocutore. Raccomandiamo, quando possibile, di abilitare tutte e tre le funzionalità per ottenere il massimo livello di sicurezza. Nel caso in cui si desideri comunicare con un dispositivo "Easy Cryptech", è necessario impostare le chiavi statiche come opzionali e verificare che, invece, il protocollo Diffie-Hellman sia abilitato o opzionale.

8. Gestione delle chiavi di cifratura SMS

Cryptech, nella sua configurazione di fabbrica, genera automaticamente le chiavi crittografiche per scambiare SMS criptati. Durante la parte iniziale di ogni telefonata criptata, Cryptech genera una chiave di cifratura da utilizzare per cifrare gli SMS che saranno scambiati in seguito con l'interlocutore. Tale chiave sarà rigenerata ad ogni telefonata, per garantire un livello di sicurezza ancora maggiore. Per verificare che la generazione della chiave SMS per il contatto sia avvenuta, basta osservare la presenza di un'icona a forma di chiave

verde che comparirà, a pochi secondi dall'inizio della telefonata, nella parte bassa dello schermo.

E' possibile decidere di disattivare la creazione automatica delle chiavi di cifratura degli SMS, attraverso il menù *Impostazioni (4) > Telefono (2) > SMS Crypto (2) > Gestione chiavi SMS*.

Nel caso in cui desideriate far sì che tutti gli SMS criptati inviati dal vostro cellulare non possano essere salvati sul telefono dopo che il destinatario ne ha letto il contenuto, potete impostare la modalità Flash come default, attraverso il menu *Impostazioni (4) > Telefono (2) > SMS Crypto (2) > Flash come default*.

Per inviare un SMS criptato è necessario andare nel menù *SMSCrypto (3)* e selezionare il menù "Nuovo sms" oppure, per fare prima, premere la freccia a destra dalla schermata principale dell'applicazione Cryptech. Comparirà una finestra nella quale scrivere il vostro messaggio, selezionare il destinatario dai contatti e inviare l'SMS criptato. Se è selezionata l'opzione chiave automatica, il messaggio verrà criptato utilizzando la chiave di cifratura che è stata generata automaticamente durante una precedente telefonata con il contatto. Se è invece selezionata la chiave manuale, sarà necessario inserire la chiave di cifratura per criptare il messaggio verificando che il destinatario sia a conoscenza della stessa chiave per poter decifrare il messaggio.

9. Rubrica dei contatti criptati

E' possibile memorizzare i propri contatti in una zona sicura criptata, accessibile soltanto attraverso l'inserimento di una password utente. I contatti possono essere inseriti in tale area manualmente oppure importandoli dalla scheda SIM mediante il menù *Contatti > Menù > Importa da SIM*.

Potete importare tutti i contatti presenti sulla SIM, oppure utilizzare il pulsante centrale per selezionare i contatti che si desidera copiare e premere "Importa".

E' possibile impostare il telefono in modo che memorizzi automaticamente ogni nuovo numero chiamato all'interno della rubrica criptata, selezionando il menù *Impostazioni (4) > Telefono (2) > Chiamata crypto CSD (1) > Salva nuovo contatto (6)* selezionando "abilitato" oppure "disabilitato" a seconda della propria preferenza.

E' importante osservare la presenza di due diverse aree per la memorizzazione dei contatti: una per i contatti che si utilizzano per le chiamate in chiaro (nel caso in cui sia stata abilitata la funzionalità di telefonate non criptate) e una per i contatti che vengono utilizzati per le chiamate criptate, protetta come descritto pocanzi dalla password utente. Nel caso in cui si utilizzi il cellulare anche per eseguire o ricevere telefonate non protette, suggeriamo di importare tutti i contatti dalla scheda SIM nella rubrica dei contatti non criptati e inserire nella rubrica dei contatti criptati soltanto quelli con sui si scambiano abitualmente telefonate criptate.

10. Impostazioni audio

Durante le telefonate criptate è possibile regolare il volume mediante l'utilizzo dei tasti posti nel lato sinistro del telefono. Durante l'impostazione del volume, compariranno sullo schermo i valori del volume che potranno variare da 1 a 7. Di norma, un valore del volume di 3 o 4 è sufficiente per sentire correttamente una telefonata. Si consiglia di non alzare esageratamente il volume per evitare che il proprio interlocutore senta l'eco della sua stessa voce.

Per impostare, invece, il volume della suoneria, potete utilizzare il menù *Impostazioni (4) > Generale (1) > Suoneria (2)*.

Per attivare il silenziatore della suoneria rendendola muta potete utilizzare il pulsante '#' della tastiera, verificandone la corretta impostazione tramite l'icona che compare nella parte alta dello schermo.

11. Luminosità dello schermo

E' possibile regolare la luminosità dello schermo utilizzando il menu *Impostazioni (4) > Generale (1) > Luminosità (5)*. Sugeriamo di non aumentare troppo la luminosità per non ridurre eccessivamente la durata delle batterie.

12. Blocco del dispositivo

E' possibile bloccare rapidamente il telefono premendo e mantenendo premuto il tasto '*' (asterisco) sulla tastier. Per sbloccare il telefono, inserire la password utente.

13. Autenticazione e timeout

Quando si trova nella schermata del telefono criptato, per motivi di sicurezza il telefono si bloccherà automaticamente dopo 5 minuti di inattività. Il periodo di sicurezza al termine del quale il telefono entra automaticamente in stato di 'lock' è definito 'timeout'. E' possibile aumentare o ridurre il timeout accedendo al menù *Impostazioni (4) > Generale (1) > Sicurezza (1) > Timeout (3)*. Trascorso il periodo impostato come timeout, per utilizzare il telefono sarà necessario inserire la password utente. E' possibile, inoltre, disattivare il blocco automatico del dispositivo accedendo al menù *Impostazioni (4) > Generale (1) > Sicurezza (1) > Autenticazione personale (4)* e scegliendo "disabilitato".

Suggeriamo vivamente di mantenere la modalità di blocco di sicurezza abilitata, per fare in modo che soltanto voi possiate fare telefonate criptate e inviare/ricevere SMS cifrati.

14. Utilizzo del codice PIN della SIM

E' possibile decidere se abilitare o meno la richiesta del codice PIN memorizzato nella propria carta SIM. Se il PIN è abilitato, è necessario ricordare di autenticarsi due volte all'accensione del telefono: la prima tramite il PIN della SIM e la seconda tramite la password utente di Cryptech.

15. Risposta automatica

Le impostazioni di fabbrica di Cryptech prevedono che, quando viene avviata una telefonata criptata, i due cellulari comincino la sincronizzazione dei dati di autenticazione e solo al termine di questo processo (che dura solitamente pochi secondi) il telefono del ricevente comincerà a squillare. Il motivo di questa funzione è che in questo modo il ricevente può rispondere immediatamente alla telefonata, non appena sente lo squillo, senza dover aspettare la fine del processo di sincronizzazione.

Per disabilitare questa funzionalità, potete accedere al menù *Impostazioni (4) > Telefono (2) > Chiamata crypto CSD (1) > Risposta automatica (5)*. Se la modalità di risposta automatica viene disabilitata, il telefono del ricevente comincerà a squillare non appena viene lanciata la telefonata criptata, mentre la sincronizzazione di autenticazione avverrà solo dopo che questo avrà risposto al telefono. Questo significa che, dopo aver risposto, il ricevente dovrà attendere il termine della sincronizzazione (solitamente pochi secondi) prima di poter parlare.

Particolare accorgimento va preso se il telefono è registrato sulla rete dell'operatore in roaming (ad esempio quando ci si trova all'estero) poiché, se la sincronizzazione automatica è abilitata, questo comporterà la ricezione della telefonata e il conseguente addebito di parte della telefonata anche se il ricevente non ha premuto il tasto verde di risposta.

16. Notifica del cambio della SIM

E' possibile attivare l'impostazione di notifica del cambio non autorizzato della carta SIM sul cellulare. Questa impostazione è utile nel caso in cui qualcuno rubasse il vostro cellulare o lo ritrovasse in caso di smarrimento e tentasse di rimuovere la vostra carta SIM inserendone un'altra. Se opportunamente configurato, Cryptech è in grado di inviare un SMS al numero di telefono impostato informandovi circa la posizione della cella GSM in cui si trova il telefono e il nuovo numero di telefono inserito nel cellulare. Per visualizzare su mappa geografica la posizione del cellulare, è possibile utilizzare il sistema KMS. Per attivare il rilevamento dell'inserimento di nuove SIM non autorizzate sul cellulare, potete accedere al menù *Impostazioni (4) > Generale (1) > Sicurezza (1) > Notifica cambio SIM (5)* selezionando "abilitato" nella finestra di impostazione. Nel momento in cui si conferma la scelta di abilitare la notifica, verrà chiesto il numero di telefono al quale notificare il cambio non autorizzato della carta SIM.

17. Impostazioni della lingua

E' possibile modificare le impostazioni della lingua del telefono accedendo al menù *Impostazioni (4) > Generale (1) > Lingua (4)*.

18. Tasti di avvio veloce

Per poter eseguire più velocemente alcune operazioni di uso frequente, senza dover cercare le voci di menu corrispondenti, sono state predisposte alcune combinazioni di avvio veloce tramite tastiera:

- Premendo la freccia a destra del tasto di navigazione, viene avviata la procedura di **scrittura nuovo messaggio**
- Premendo la freccia in alto del tasto di navigazione veloce, si ottiene immediato **accesso alla Inbox**
- Premendo e tenendo premuto il tasto '*' (asterisco) della tastiera, si attiva il **blocco del telefono**
- Premendo e tenendo premuto il tasto '#' (cancellito) della tastiera si attiva il **silenziatore della suoneria**

19. Impostazioni di rete

Per accedere alla finestra di impostazione dei parametri di rete è necessario utilizzare la voce di menù *Impostazioni (4) > Telefono (2) > Chiamata crypto CSD (1) > Rete (1)*. Sono disponibili cinque opzioni: "v.110 – Transparent", "v.110 – Non transparent", "v.32 – Transparent", "v.32 – Non Transparent" e "Custom". E' sconsigliato l'utilizzo della quinta opzione, "Custom", poiché è riservato a personale esperto.

L'impostazione di fabbrica di Cryptech prevede l'utilizzo del protocollo di rete "v.110" insieme alla modalità "Transparent", ideale nella maggior parte delle situazioni. In alcuni casi, come ad esempio quando la rete GSM non supporta il roaming o il protocollo v.110, è consigliabile selezionare il protocollo v.32.



Qui di seguito riportiamo alcuni utili accorgimenti e precauzioni.

Normalmente le reti supportano pienamente il protocollo v.110. In alcune situazioni, come ad esempio durante i viaggi all'estero in cui il telefono si registra sulla rete nella modalità detta di "roaming", può essere necessario impostare la modalità v.32 per poter eseguire telefonate criptate. In rari casi e in alcuni paesi può essere necessario digitare il numero dati del ricevente invece del normale numero di telefono. Per conoscere il proprio numero dati è sufficiente contattare il centro assistenza del proprio operatore che, in genere, lo fornirà gratuitamente.



La modalità "Non Transparent" permette in genere di fare chiamate criptate anche in condizioni di rete ridotte (mancanza di campo, etc...) ma durante la conversazione criptata genera dei ritardi evidenti, particolarmente in caso di disturbi sulla linea. In alcune reti GSM si è obbligati a selezionare la modalità "Non Transparent" per poter eseguire telefonate criptate.



Nel caso in cui si sia impostato il protocollo v.32, ricordarsi di reimpostare il protocollo v.110 al ritorno nel proprio paese.

