



New Italy

di ANDREA DI STEFANO

Criptofonino per proteggere dati e telefonate

Proteggere i dati. Ma anche le conversazioni. Utilizzando la tecnologia e le opportunità offerte dai nuovi sistemi operativi, come Windows Mobile 5. Il tutto grazie alla collaborazione tra il Politecnico di Torino e alcuni ingegneri esperti in crittaggio. Così nel 2003 è nata a Torino la Caspertext, che ha lanciato e brevettato il concetto di "Criptofonino". Il criptofonino rappresenta una soluzione portatile sofisticata e affidabile per comunicare in modo sicuro. Il sistema utilizza una classica cifratura con chiave simmetrica sia delle chiamate voce che di sessioni di chat.

Il criptofonino registra, codifica, cifra ed invia in tempo reale il flusso dei dati attraverso il canale dati della rete GSM. Il ricevente allo stesso modo gestisce automaticamente la chiamata cifrata, la decifra, la decodifica e la riproduce in voce. E così avanti per tutta la chiamata. In questo modo tutti i dati inviati dal telefono, viaggiano cifrati su tutte le reti di telecomunicazioni finché non vengono decifrati dal ricevente. Tutto il processo avviene in modo semplice e soprattutto automatico per l'utente. Il sistema è stato sviluppato su piattaforma Windows Mobile 2003 sia in versione

Pocket Pc
c h e

Prodotti da un'azienda italiana, la Caspertext. Il sistema sotto Windows

Pocket Pc e Smartphone. Attualmente i telefonini criptati possono essere acquistati direttamente da Caspertext.

Oltre a fare telefonate non intercettabili, permette l'utilizzo di molte applicazioni tipiche di un notebook come word, excel, outlook, explorer. Tutte queste operazioni possono essere eseguite con la massima sicurezza e garanzia che se il Criptofonino viene smarrito o rubato, tutti i documenti cifrati all'interno di esso non potranno essere decifrati da nessuno senza la password (di esclusiva conoscenza dell'utente). Ogni Criptofonino è unico e viene configurato con un software compilato in modo esclusivo per quel dispositivo. La sicurezza delle comunicazioni viene garantita dalla cifratura con gli algoritmi più robusti (AES 256) e le tecniche più avanzate oggi conosciute che vengono tenute costantemente aggiornate grazie proprio alla collaborazione con il Politecnico e l'Università di Torino. Le chiavi di cifratura simmetriche vengono immesse direttamente dall'utente, che è quindi l'unico a conoscerle. Si può gestire un numero infinito di chiavi diverse, usando così chiavi per gruppo di interlocutori o chiavi dedicate a singole comunicazioni. La cifratura è fatta in modo tale che lo stesso dato cifrato con la stessa password risulterà diversa ogni volta che viene effettuata.

L'enorme vantaggio del sistema Crypthec è la possibilità di disporre della massima mobilità, potendo utilizzare tutte le reti Gsm in Italia e nel Mondo.