



(Riferimento offerta n. 274/RUF del 16/07/2008)

Certificazione Tecnologia Software CRYPTTECH

Il sottoscritto, **Giancarlo Ruffo**, Professore Associato in Informatica, afferente al Dipartimento di Informatica dell'Università degli Studi di Torino, in possesso delle necessarie competenze scientifiche e tecniche atte ad esprimere una valutazione sulle caratteristiche di sicurezza di una tecnologia software, per conto del suddetto Dipartimento di Informatica, espone qui di seguito le proprie valutazioni ed i propri rilievi tecnici in ordine alla tecnologia **CRYPTTECH**, ideata, realizzata e mantenuta dalla società **Casper Technology S.r.l.** Tali rilevazioni si riferiscono alla versione della tecnologia CRYPTTECH da me visionata il giorno 22 Luglio 2008 presso la sede operativa della società Casper Technology S.r.l., sita in Via Cardinal Massaia, 83 - Torino.

In riferimento alla tecnologia CRYPTTECH in oggetto, vanno segnalati i seguenti dati identificativi:

1. Titolo brevetto: "Sistema e Metodo per la comunicazione cifrata di voce e/o dati e/o fax e/o video";
2. Brevetto d'invenzione n. 1344047 concesso il 12/02/2008 (già domanda TO2003A000337 depositata il 9/5/2003);
3. Registrazione del marchio n. 1101293 concessa il 13/3/2008 'Criptofonino' (classe 9) (già domanda TO2004C001949 depositata il 21/06/2004);
4. Registrazione del marchio n. 003760139 concessa il 29/7/2005 'Cryptech' (classe 9,38,42) (già domanda 003760139 depositata il 14/04/2004).

Il sottoscritto, a seguito di testimonianza diretta ed in presenza degli sviluppatori della tecnologia di cui all'oggetto

CERTIFICA

che la tecnologia CRYPTTECH possiede le seguenti caratteristiche tecniche:

1. Autenticazione utente all'avvio del Sistema tramite password alfanumerica fino a 32 caratteri;
2. Cifratura simmetrica tramite algoritmo AES 256 bit con implementazione nota in conformità FIPS 197 ed utilizzo chiave a 256 bit;
3. Cifratura a flusso tramite OFB;





UNIVERSITA' DEGLI STUDI DI TORINO
DIPARTIMENTO DI INFORMATICA

4. Hash crittografico tramite algoritmo SHA-256 con implementazione nota in conformità FIPS-180-2;
5. Protocollo di generazione della chiave che fa uso del sistema Diffie-Hellman 4096 bit con implementazione nota;
6. Protocollo di generazione della chiave che adotta l'opzione Diffie-Hellman a curve ellittiche a 571 bit di tipo KOBLITZ con implementazione nota;
7. Protocollo di generazione della chiave che prevede la distruzione della chiave al termine della connessione, sovrascrivendo le aree di memoria principale che sono state utilizzate anche solo temporaneamente;
8. Protocollo di generazione della chiave che prevede il doppio riconoscimento vocale, da parte degli agenti umani coinvolti nella conversazione, dei numeri utili all'autenticazione delle chiavi generate tramite lo schema Diffie-Hellman;
9. Funzione di Zeroize per la cancellazione di tutto il contenuto del sistema cifrante, attivabile anche in modalità remota a seguito di autenticazione tramite parola chiave;
10. Generazione numeri RANDOM con implementazione nota in conformità FIPS 186-2;
11. Firma digitale di ogni componente del sistema atta a prevenire eventuali modifiche non autorizzate.

Inoltre, si precisa che, qualora non vengano operate successive modifiche, alterazioni e cancellazioni alla tecnologia qui certificata, il sistema, nelle parti da me visionate e sopra riportate che seguono puntualmente le specifiche FIPS del NIST, prevede ed implementa i necessari accorgimenti tecnici atti a prevenire la presenza di backdoor maliziose e che le strategie implementate sono allo stato dell'arte e pubblicamente disponibile alla comunità scientifica.

Tanto certifica il sottoscritto ad evasione del mandato ricevuto.

Torino, 22 Luglio 2008



Prof. Giancarlo Ruffo