



UNIVERSITA' DEGLI STUDI
DI TORINO
DIPARTIMENTO
DI INFORMATICA

Riferimento offerta n. 274/RUF, 16/07/2008

CRYPTTECH Software Technology Certification

I the undersigned **Giancarlo Ruffo**, Associate Professor in Computer Science, member of the Computer Science Department of the "Università degli Studi di Torino", in possession of the necessary scientific and technical knowledge suitable to express an evaluation of the security features of any software technology, on behalf of the aforementioned Computer Science Department, hereby exhibit my own evaluations and technical surveys with reference to the CRYPTTECH technology designed, developed and maintained by the "Caspertech Technology S.r.l." company.

Such surveys refer to the version of the CRYPTTECH technology examined in first person on July 22, 2008, at the Operational Office of Casper Technology S.r.l., situated in Via Cardinal Massaia, 83 – Turin.

As for the CRYPTTECH technology referred above, the following identification points can be put remarked:

1. Patent Title: "Sistema e Metodo per la comunicazione cifrata di voce e/o dati e/o fax e/o video";
2. Patent Invention n. 1344047 released on 12/02/2008 (previously patent pending n. TO2003A000337 issued on 9/5/2003);
3. 'Criptofonino' (class 9) Registration Mark n. 1101293 issued on 13/3/2008 (previously patent pending TO2004C001949 issued on 21/06/2004);
4. 'Cryptech' (class 9, 38, 42) Registration Mark n. 003760139 issued on 29/7/2005 (previously patent pending 003760139 issued on 14/04/2004).

I the undersigned, after direct verification in the presence of the aforementioned technology developers

CERTIFY

that the CRYPTTECH technology complies to the following technical features:

1. User authentication during System startup by means of alphanumeric password up to 32 characters length;
2. Symmetric encryption by means of AES 256 bit algorithm with known implementation in compliance with FIPS 197 and 256 bit key;
3. Stream cipher encryption by means of OFB;





UNIVERSITA' DEGLI STUDI DI TORINO
DIPARTIMENTO DI INFORMATICA

4. Cryptographic hash by means of SHA-256 algorithm with known implementation in compliance with FIPS-180-2;
5. Key generation protocol with Diffie-Hellman 4096 bit system with known implementation;
6. Key generation protocol with Elliptic Curves Diffie-Hellman 571 bit of type KOBLITZ with known implementation;
7. Key generation protocol which assures the destruction of the key at the end of the connection, by overwriting the main memory areas employed even for a short time;
8. Key generation protocol which involves double vocal acknowledgement, performed by the human agents who are holding the conversation, of the numbers which can identify the key derived by means of the Diffie-Hellman scheme;
9. Zeroize function for the wiping of the whole encryption system, which can be activated also remotely upon passphrase authentication;
10. RANDOM numbers generation with known algorithm in compliance with FIPS 186-2;
11. Digital signature of each component of the system, aimed at preventing any potential unauthorized modifications.

Furthermore, it's relevant that – provided that no modifications, alterations or deletions be performed to the hereby certified technology – the system, in its aforementioned and personally verified components complying to NIST FIPS specifications, provides and enforces the necessary technical solutions aimed at preventing the presence of malicious backdoors and that the implemented strategies are state-of-the-art and publicly available to the scientific audience.

I the undersigned hereby certify the above, to fulfill the duties deriving from the received assignment.

Turin, July 22, 2008



Prof. Giancarlo Ruffo