Advanced Encryption Standard Algorithm Validation Certificate

The National Institute of
Standards and Technology
of the
United States of America

Certificate No. 109

The Communications Security
Establishment
of the
Government of Canada

The National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) hereby validate the Advanced Encryption Standard (AES) algorithm testing results of the implementation identified as:

SG-DRL3-IP/T-LINK TL250, Version 1.00 (Firmware)

and supplied by:

Digital Security Controls Ltd.

in accordance with the specifications of the *Advanced Encryption Standard (AES)* (FIPS 197) and *Recommendations for Block Cipher Modes of Operation* (SP800-38A 2001 ED) as indicated on the reverse of this certificate. Implementations bearing the same identification and manufactured to the same specifications as the validated implementation may be labeled as complying with FIPS 197 for the modes, states, and key sizes identified in this certificate. No reliability test has been performed and no warranty of the implementation is either expressed or implied.

The validated implementation was tested using the following operating environment (for software implementations, operating environment includes processor and operating system; for firmware implementations, operating environment includes processor only; for hardware implementations, operating environment is not applicable):

MPC855T, a Motorola 32-bit processor

The vendor should be contacted to obtain a list of operating environments that support the validated implementation. Likewise, the vendor should be contacted to obtain a list of products/applications that use the validated implementation.

This certificate must include the following page that details the scope of conformance and includes the validation authorities' signatures.

The NIST document, *"The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)"* describes a series of known answer, multi-block message and Monte Carlo tests for implementations of FIPS 197:*Advanced Encryption Standard* , using modes of operation specified in NIST Special Publication 800-38A 2001 ED,*Recommendation for Block Cipher Modes of Operation* . This implementation has been tested using the Cryptographic Algorithm Validation System (CAVS) Version 1.3. The scope of conformance achieved by the algorithm implementation identified as:

SG-DRL3-IP/T-LINK TL250, Version 1.00 (Firmware)

and tested by the accredited Cryptographic Module Testing laboratory: **EWA-Canada LTD, IT Security Evaluation Facility**
NVLAP Lab Code 200556-0

is as follows. The validated implementation performs AES in the following modes of operation, states, and key sizes:

Mode(s) of Operation	State(s)	Key Size(s)
Electronic Codebook (ECB)	**Encrypt/Decrypt**	**128**

Signed on behalf of the Government of the United States

Signature:

Date: 20 November 2003

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Date: 15 Nov 03

Director, Information Protection Group
Communications Security Establishment

Rev. 07/2002