Secure Hash Standard (SHS)
Validation Certificate

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

Certificate No. 8

The Communications Security Establishment of the Government of Canada

The National Institute of Standards and Technology and the Communications Security Establishment hereby validate the Secure Hash Standard testing results of the implementation identified as:

Cryptographic iButton™, v1.01

and supplied by:

Dallas Semiconductor

in accordance with the specifications of the *Secure Hash Standard (SHS)* (FIPS 180-1), 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 180-1 as identified in this certificate. No reliability test has been performed and no warranty of the implementation is either expressed or implied.

The validated implementation, if implemented in software, was tested using the following operating environment:

N/A

The supplier should be contacted to obtain a list of operating environments which support the validated implementation.

This certificate must include the following page that details the scope of conformance and the validation authority signature.

A NIST Special Publication, *Digital Signature Standard (DSS) and Secure Hash Standard (SHS) Validation System: Requirements and Procedures (June 1995 Draft)*, describes a series of tests for implementations of the SHA-1, which is specified in FIPS 180-1. The scope of conformance achieved by the algorithm implementation identified as:

Cryptographic iButton™, v1.01
(Part# DS1954-004; hardware)

and tested by the Cryptographic Module Testing accredited laboratory: **CEAL: A CygnaCom Solutions Laboratory**
NVLAP Lab Code 200002-0

is as follows.

*The implementation was tested and is validated **only** for the correct hashing of **byte-oriented** data, for messages of length ≤ 1024 bits.*

Signed on behalf of the Government of the United States

Signature: Miles E. Smid

Dated: 3 April 1998

Manager, Security Technology Group
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: Barry Madill

Dated: 17 April 1998.

Director, Information Protection Group
The Communications Security Establishment