

Secure Hash Standard (SHS) Validation Certificate

Certificate No. **547**

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

**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 Secure Hash Standard (SHS) testing results of the implementation identified as:

CryptoServer CS SHA, Version 2.0.0.0 (Firmware)

and supplied by:

Utimaco Safeware AG

in accordance with the specifications of Federal Information Processing Standard (FIPS) 180-2, Secure Hash Standard, 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 180-2 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 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):

Texas Instruments TMS320C6414

The vendor should be contacted to obtain a list of operating environments which 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 presents the validation authorities' signatures.

A NIST testing specification, Secure Hash Standard Validation System (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512), describes a series of tests for implementations of SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512, which is specified in FIPS 180-2 (with Change Notice dated February 25, 2004). The scope of conformance achieved by the algorithm implementation identified as:

CryptoServer CS SHA, Version 2.0.0.0 (Firmware)

and tested by the accredited Cryptographic Module Testing laboratory: **InfoGard Labs, Inc.**
CAVS Version 5.2

NVLAP Lab Code 100432-0

is as follows:

Scope of Validation

- SHA-1: Tested and validated only for the correct hashing of BYTE-oriented data.
- SHA-224: Tested and validated only for the correct hashing of BYTE-oriented data.
- SHA-256: Tested and validated only for the correct hashing of BYTE-oriented data.
- SHA-384: Tested and validated only for the correct hashing of BYTE-oriented data.
- SHA-512: Tested and validated only for the correct hashing of BYTE-oriented data.

Signed on behalf of the Government of the United States

Signature: _____

[Handwritten Signature]
(For Curt Barker)
Date: 12-21-06

Chief, Computer Security Division
National Institute of Standards and Technology

Rev. 10/2004

Signed on behalf of the Government of Canada

Signature: _____

[Handwritten Signature]
Date: January 17, 2007

Director, Industry Program Group
Communications Security Establishment