Random Number Generator (RNG) Validation Certificate

Certificate No. 259

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 Random Number Generator (RNG) testing results of the implementation identified as:

CryptoServer CS DRNG, Version 2.0.0.0 (Firmware)

and supplied by:

Utimaco Safeware AG

in accordance with the specifications of Federal Information Processing Standards (FIPS) 186-2 (change notice dated October 5, 2001), ANSI x9.62, and ANSI x9.31 (Appendix A.2.4), 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 the Random Number Generator 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 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 presents the validation authorities' signatures.

The Random Number Generator Validation System (RNGVS) describes a series of tests for implementations of random number generators in the following standards: FIPS 186-2 (Change Notice dated October 5, 2001), ANSI x9.62, and ANSI x9.31 (Appendix A.2.4). The scope of conformance achieved by the algorithm implementation identified as:

CryptoServer CS DRNG, Version 2.0.0.0 (Firmware)

and tested by the accredited Cryptographic Module Testing laboratory: **InfoGard Labs, Inc.** **NVLAP Lab Code 100432-0**

CAVS Version 5.2

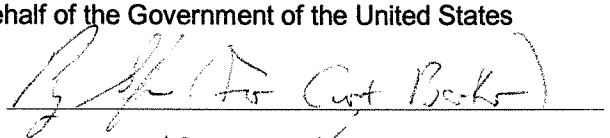
is as follows:

Algorithm Tested: FIPS 186-2 General Purpose RNG Change Notice dated October 5, 2001

Algorithm(s) Tested: x-Original

G-Function(s) Tested: SHA-1

Signed on behalf of the Government of the United States

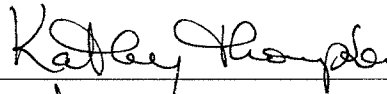
Signature: 

Date: 12-21-06

Chief, Computer Security Division

National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: 

Date: January 11, 2007

Director, Industry Program Group

Communications Security Establishment