Triple DES Modes of Operation Validation Certificate

Certificate No. 492

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 Triple Data Encryption Algorithm (TDEA) Modes of Operation testing results of the implementation identified as:

CryptoServer CS TDES, Version 2.0.0.0 (Firmware)

and supplied by:

Utimaco Safeware AG

in accordance with the specifications of the *Data Encryption Standard (DES)* (FIPS 46-3), and the *DES Modes of Operation* (FIPS 81), 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 46-3 for the modes, states, and keying options 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 Instuments TMS320C6414

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 Special Publication 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures, October 1999,* and the document *The Multi-block Message Test (MMT),* describe a series of known answer, multi-block message and Monte Carlo tests for implementations of the Triple DES (i.e.,TDEA), which is specified in FIPS 46-3. The scope of conformance achieved by the algorithm implementation identified as:

CryptoServer CS TDES, Version 2.0.0.0 (Firmware)

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

CAVS Version 5.2

is as follows. The validated implementation operates Triple DES in the following modes and states, with the specified keying options:

Mode(s) of Operation	State(s)	Keying Option(s)
TDEA Electronic Codebook (TECB)	**Encrypt/Decrypt**	**1, 2, 3***
TDEA Cipher Block Chaining (TCBC)	**Encrypt/Decrypt**	**1, 2, 3***

**Indicates a mode and keying option combination that is backward compatible with its single DES counterpart.*

Keying Option 1: Three-key Triple DES Keying Option 2: Two-key Triple DES Keying Option 3: Single DES

Signed on behalf of the Government of the United States

Signature: (for Curt Barker)

Date: 12-21-06

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: Kathy Thompson

Date: January 11, 2007

Director, Industry Program Group
Communications Security Establishment

Rev. 04/2006