RSA Validation Certificate

Certificate No. 196

The National Institute of Standards and Technology of the United States

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 RSA testing results of the implementation identified as:

CryptoServer CS SMOS RSA, Version 2.0.0.0 (Firmware)

and supplied by:

Utimaco Safeware AG

in accordance with the specifications of Federal Information Processing Standard (FIPS) 186-2 (Change Notice dated October 5, 2001), Digital Signature Standard (DSS) and specified in ANSI X9.31-1998, Digital Signature using Reversible Public Key Cryptography for the Financial Services Industry (rDSA) and/or as approved in PKCS#1 v2.1: RSA Cryptography Standard, RSA Laboratories, June 2002. The specifications of the implementation are 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 RSA algorithm in FIPS 186-2 and/or PKCS#1 v2.1 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 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 RSA Validation System (RSAVS) describes a series of tests for implementations of the RSA, which is approved in FIPS 186-2 and/or PKCS#1 V2.1. The scope of conformance achieved by the algorithm implementation identified as:

CryptoServer CS SMOS RSA, Version 2.0.0.0 (Firmware)

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

CAVS Version 5.2

PKCS#1 V2.1: RSASSA-PKCS1_V1_5	***Validation Test performed:***	*Signature Verification*
	Modulus sizes tested (bits):	*1024, 1536, 2048*
	SHA algorithm(s) used in validation:	*SHA-1(#547)*

Signed on behalf of the Government of the United States

Signature: [signature]

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: [signature]

Date: January 11, 2007

Director, Industry Program Group
Communications Security Establishment