Elliptic Curve Digital Signature Algorithm (ECDSA) Validation Certificate

Certificate No. 44

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 Elliptic Curve Digital Signature Algorithm (ECDSA) testing results of the implementation identified as:

CryptoServer CS ECDSA, 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 X9.62-1998, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). 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 Elliptic Curve Digital Signature Algorithm in FIPS 186-2 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 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 Elliptic Curve Digital Signature Standard Validation System (ECDSAVS) describes a series of tests for implementations of the ECDSA, which is specified in FIPS 186-2 (Change Notice dated October 5, 2001). The scope of conformance achieved by the algorithm implementation identified as:

CryptoServer CS ECDSA, 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:

Secure Hash Generation: *Corresponding Secure Hash Standard (SHS) validation cert.# 547*

Random Number Generation: *Corresponding Random Number Generation (RNG) validation cert.# 259*

ECDSA Public Key (Q) Generation

Curves tested : P-192, P-224, P-256, P-384, P-521

ECDSA Public Key Validation

Curves tested : P-192, P-224, P-256, P-384, P-521

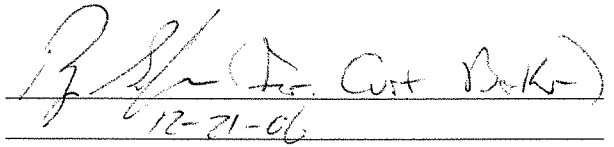
Signature Generation

Curves tested : P-192, P-224, P-256, P-384, P-521

Signature Verification

Curves tested : P-192, P-224, P-256, P-384, P-521

Signed on behalf of the Government of the United States

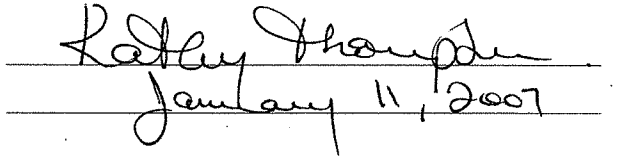
Signature: 

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