

# Advanced Encryption Standard Algorithm Validation Certificate

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

Certificate No. 20

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 Advanced Encryption Standard (AES) algorithm testing results of the implementation identified as:

**stdcrypt.dll Version 1.0**

and supplied by:

**Dekart SRL**

in accordance with the specifications of the *Advanced Encryption Standard (AES)* (FIPS 197) and *Recommendations for Block Cipher Modes of Operation* (SP800-38A 2001 ED) 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 197 for the modes, states, and key sizes 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):

**Pentium 4 w/ Windows 95**

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 document, "The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)" describes a series of known answer, multi-block message and Monte Carlo tests for implementations of FIPS 197: *Advanced Encryption Standard*, using modes of operation specified in NIST Special Publication 800-38A 2001 ED, *Recommendation for Block Cipher Modes of Operation*. This implementation has been tested using the Cryptographic Algorithm Validation System (CAVS) Version 1.0. The scope of conformance achieved by the algorithm implementation identified as:

**stdcrypt.dll Version 1.0**

and tested by the accredited Cryptographic Module Testing laboratory: **EWA-Canada LTD, IT Security Evaluation Facility  
NVLAP Lab Code 200556-0**

is as follows. The validated implementation performs AES in the following modes of operation, states, and key sizes:

<u>Mode(s) of Operation</u>	<u>State(s)</u>	<u>Key Size(s)</u>
Electronic Codebook (ECB)	Encrypt/Decrypt	128,192,256
Cipher Block Chaining (CBC)	Encrypt/Decrypt	128,192,256
8-bit Cipher Feedback (CFB8)	Encrypt/Decrypt	128,192,256
Output Feedback (OFB)	Encrypt/Decrypt	128,192,256

Signed on behalf of the Government of the United States

Signature: [Signature]  
Date: 9 July 2002

Chief, Computer Security Division  
National Institute of Standards and Technology

Rev. 07/2002

Signed on behalf of the Government of Canada

Signature: [Signature]  
Date: 31 July 2002

Director, Information Protection Group  
Communications Security Establishment