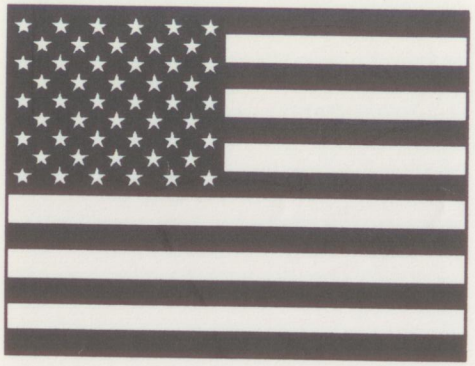

FIPS 140-1
Validation Certificate

Certificate No. 3

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, as the United States FIPS 140-1 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-1 Cryptographic Module Validation Authority; hereby validate the FIPS 140-1 testing results of the Cryptographic Module identified as:

ENTRUST CRYPTOGRAPHIC KERNEL *v* 2.4
(when operated in the FIPS *mode)*

In accordance with the Derived Test Requirements for FIPS PUB 140-1, *Security Requirements for Cryptographic Modules.* FIPS-140-1 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive But Unclassified Information* (United States) or *Designated Information* (Canada) within computer and communications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS-140-1 so long as the product, throughout it's life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate must include the following page that details the scope of conformance and validation authority signatures.

FIPS 140-1 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

Northern Telecom Secure Network Entrust

and tested by the Cryptographic Module Testing accredited laboratory: **DOMUS Software Limited IT Security Laboratory** **NVLAP Lab Code 200017-0** is as follows:

Cryptographic Module Design:	Level 1	*Module Interfaces:*	Level 1
Roles and Services:	Level 1	*Finite State Machine Model:*	Level 1
Physical Security:	Level 1	*Software Security:*	Level 1
EMI / EMC:	Level 1	*Self Tests:*	Level 1
Key Management:	Level 1		

Operating System Security Level 1 is met when used in the following configuration: **PC MS-DOS 6.2 MS Windows 3.1**

The following FIPS approved *Cryptographic Algorithms* are used: **DES (cert.#1); DSA and SHA-1 by written affirmation, pending testing**

The Cryptographic module also contains the following non-FIPS approved algorithms: **MD5, MD2, RSA, CAST, CAST3**

End user queries concerning the non-FIPS approved algorithms may be directed to their respective Cryptographic Module Validation Authority.

Overall Level Achieved: 1

Signed on behalf of the Government of the United States

Signature: Miles E. Smid

Dated: September 17, 1996

Manager, Security Technology Group
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: R A English

Dated: September 11, 1996

Director ITS Services
The Communications Security Establishment