Attachmate

CryptoConnect

Encrypting Transport System

Security Policy

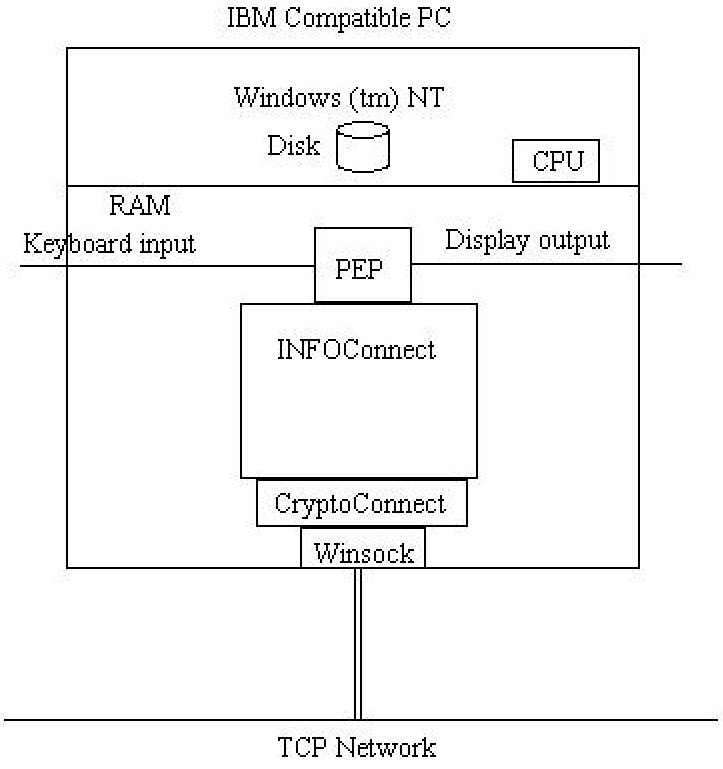
Introduction

The CryptoConnect Encrypted Transport System (CryptoConnect ETS) is a Dynamic Link Library, TCPWIN32.DLL. It serves as an INFOConnect transport module which performs encryption on all of the data sent to and received from the host. When used in place of the standard INFOConnect TCP transport, it connects via TCP to an encryption server (the CryptoConnect Gateway) which handles the encryption tasks at the host end. It supports the FIPS approved SHA-1, DSA, DES, and Triple DES CBC algorithms. It also supports the non-FIPS approved RC2, RC4 and RSA algorithms.

For the purpose of maintaining compatibility with existing communications paths, CryptoConnect ETS can also be configured to run in an unencrypted mode to a non-encrypting host.

When CryptoConnect ETS is first loaded, it runs a test for structural integrity. If the test fails, the module is not permitted to run.

Each time a session is opened, CryptoConnect ETS runs a set of self-tests to verify the validity of the cryptographic suite. If these tests are not successful, the session open request is rejected. CryptoConnect ETS uses the Secure Sockets Layer protocol to negotiate encryption parameters and keys with the encryption server. It uses the negotiated keys and parameters to encrypt all data being sent to the host, and to decrypt all data received from the host.



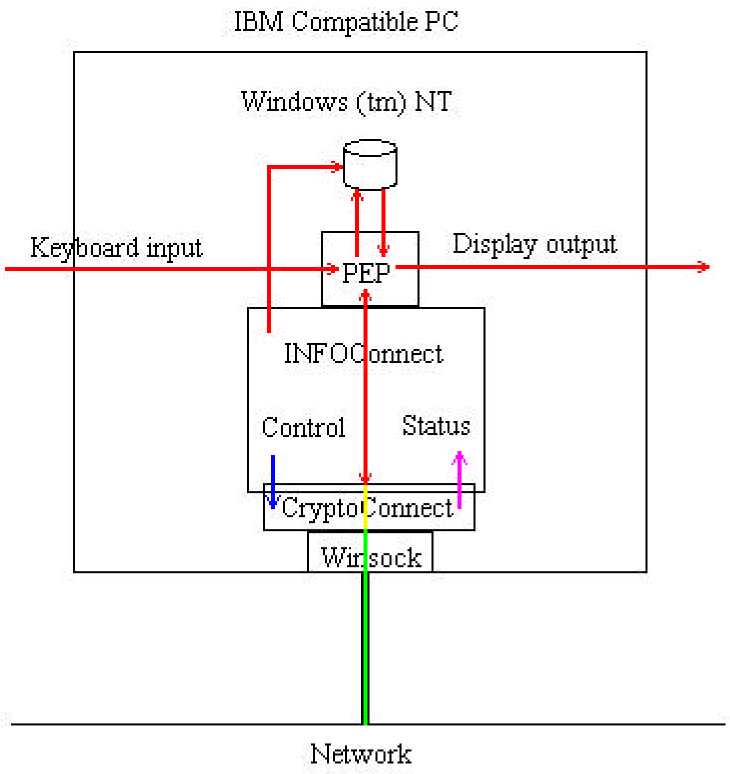
Overview

For FIPS 140-1 classification purposes, the Attachmate CryptoConnect Encrypted Transport System is intended to meet FIPS 140-1 level one requirements and is considered to be a "multi-chip standalone module." The "Secure Cryptographic Boundary" encompasses an IBM compatible PC with one or more network connections (supplied by the user), running the Attachmate INFOConnect software package with the CryptoConnect ETS module, under either Windows^{tm} 95, Windows^{tm} 98, or Windows NT^{tm} (version 4.0, service pack 3 or higher) running in single user mode. All cryptographic functions are performed within the CryptoConnect ETS module by the FIPS 140-1 certified version 4.11 of the RSA^{tm} BSAFE® Crypto-C toolkit.

No keys are stored within the cryptographic boundary. The SSL (Secure Sockets Layer) protocol is used to agree on keys with the server at the other end of the communications link. The server encrypts random key generation material with its private key and sends it to CryptoConnect ETS along with the public key needed to decrypt it. CryptoConnect ETS generates further random key material, encrypts it with the public key, and returns it to the server. Both sides then derive matching DES keys and vectors from the shared key material and use them to encrypt and decrypt their communications. These keys and vectors are never output, and the memory containing them is zeroized after use.

The methods employed in deriving the keys and vectors deviates from the SSL standard, which specifies the use of MD5 and SHA-1 to produce a “master secret” and then to derive the keys and vectors. Since the use of MD-5 in key generation is not FIPS approved, CryptoConnect ETS uses only SHA-1 in generating the master secret and the keys and vectors.

Plaintext data, whether entered by the user or by other software, is presented by INFOConnect to CryptoConnect ETS through the input data API. The data is encrypted and the encrypted data is passed out via TCP through the network output data interface. Cyphertext data is received via TCP through the network input data interface. The data is decrypted and passed to INFOConnect via the output data API.



Roles and Services

The CryptoConnect Encrypted Transport System supports a User role and a Crypto-Officer role. No Maintenance role is supported. The CryptoConnect ETS module does not support user identification or authentication for these roles.

A User is any entity that can operate an INFOConnect Tool that uses the CryptoConnect ETS module to encrypt its communications. When a User is active, the CryptoConnect ETS module is in the User State. A User has no access to any of the cryptographic parameters or keys.

A user can request the CryptoConnect ETS module to (1) open a TCP connection to a designated host, (2) supply the current encryption status of the connection, (3) send data (encrypted) to the host, (4) decrypt data received from the host and (5) close the TCP connection. The following functions are available to a program operating in the User role:

IcLibCloseSession
IcLibEvent
IcLibGetString
IcLibIdentifySession
IcLibInstall
IcLibLcl
IcLibRcv
IcLibOpenSession
IcLibGetSessionInfo
IcLibSetResult
IcLibTerminate
IcLibXmt
IcLibOpenChannel
IcLibCloseChannel

Descriptions of each of these, including its functionality, input, output and status parameters, may be found in the INFOConnect Advanced Developers Kit documentation.

INFOConnect can be configured to create several communication sessions which access the CryptoConnect ETS module simultaneously. The state information for each is maintained independently and one session cannot access any of the data or state information of any other.

A Crypto Officer is any entity that can operate the INFOConnect Configuration Utility to configure the INFOConnect sessions which use the CryptoConnect ETS module. When a Crypto Officer is performing configuration, the CryptoConnect ETS module is in the Crypto Officer State. A Crypto Officer has no access to any of the cryptographic parameters or keys.

A Crypto Officer can request the CryptoConnect ETS module to display and update an INFOConnect configuration record describing a host with which a User can subsequently establish a connection. The following functions may be called by a program operating in the Crypto Officer role:

IcLibUpdateConfig
IcLibVerifyConfig
IcLibPrintConfig

Descriptions of each of these, including its functionality, input, output and status parameters, may be found in the INFOConnect Advanced Developers Kit documentation.

A Crypto Officer may access the Configuration Utility while a User is active. The configuration utility runs as a separate process under the operating system. Information for each is maintained independently and neither has any access to the data or state information of the other.