

Sterling Connect:Direct and FIPS 140-2

Revision number: 2.0

Date: 5/29/2009

Prepared by: Dirk Maney, Product Line Manager (e-mail: dirk_maney@stercomm.com)

Federal Information Processing Standard 140-2 (FIPS 140-2) is a standard published by the U.S. and Canadian governments. The standard defines the security requirements that must be satisfied by a cryptographic module. FIPS 140-2 covers security requirements that must be met by IT products used by the U.S. Federal government for Sensitive, but Unclassified (SBU) use. By law, agencies within the U.S. government are forbidden from purchasing products (hardware or software) that use encryption or other cryptographic security that do not meet FIPS 140-2 requirements.

Sterling Commerce places significant emphasis on ensuring that integration solutions, such as Connect:Direct, meet the highest level of security requirements, including FIPS 140-2. In particular, Connect:Direct Secure+ leverages FIPS 140-2 cryptographic modules to accomplish a number of security related activities for data security and integrity.

The following table summarizes the FIPS 140-2 certified cryptographic modules that are utilized by Connect:Direct on the z/OS, UNIX, and Windows platforms.

Product/Platform	FIPS 140-2 Certified Cryptographic Module and Level Used by Connect:Direct	FIPS Cert. #	Connect:Direct Release Number
Connect:Direct for z/OS	IBM eServer Cryptographic Coprocessor Security Module (when present and operated in FIPS mode) ¹ Level 4	661	All supported releases of Connect:Direct for z/OS
Connect:Direct for UNIX	Sterling Crypto-C Software Version: 1.5 (when operated in FIPS mode) Level 1	921	Connect:Direct for UNIX version 4.0 and higher
Connect:Direct for Windows	Sterling Crypto-C Software Version: 1.5 (when operated in FIPS mode) Level 1	921	Connect:Direct for Windows version 4.4 with Patch 060 and higher

¹ Connect:Direct for z/OS Secure+ relies upon the IBM System SSL libraries for all cryptographic functions. If the IBM eServer Cryptographic Coprocessor is present, System SSL can make use of it through the IBM Integrated Cryptographic Services Facility (ICSF). When the Cryptographic Coprocessor is not available, software encryption is performed by the System SSL libraries. IBM has indicated that System SSL in z/OS V1.11 is planned to provide a mode of operation designed to meet the FIPS 140-2 Level 1 criteria. Refer to http://www-01.ibm.com/common/ssi/rep_ca/9/897/ENUS209-029/ENUS209-029.PDF for additional information.

Additional information can be found on the National Institute of Standards and Technology Computer Security Resource Center at <http://csrc.nist.gov/groups/STM/cmvp/validation.html#03>.