

**White Paper**  
**For**  
**SkyLOCK™ Electronic File Transfer (eFT)**

**PREFACE:**

This white paper has been prepared by Robert A. Stedron, Chief Technology Officer, Shinho Kang, Senior Technologist and John H. Johnson, Vice President of Encryption Solutions, Inc. (ESI) to describe the methods of encryption used in ESI's SkyLOCK™ eFT, electronic file transfer product. This product has been designed to work on wireless and wired infrastructure, across multiple platforms, initially "fitted" for the Linux, Unix and MS Windows environs, capable of handling large files at high speeds with high efficiency and security.

The information furnished in this document is provided for the purpose of informing potential users, partners, contractors and customers of ESI how the technology is designed to work.

**INTRODUCTION:**

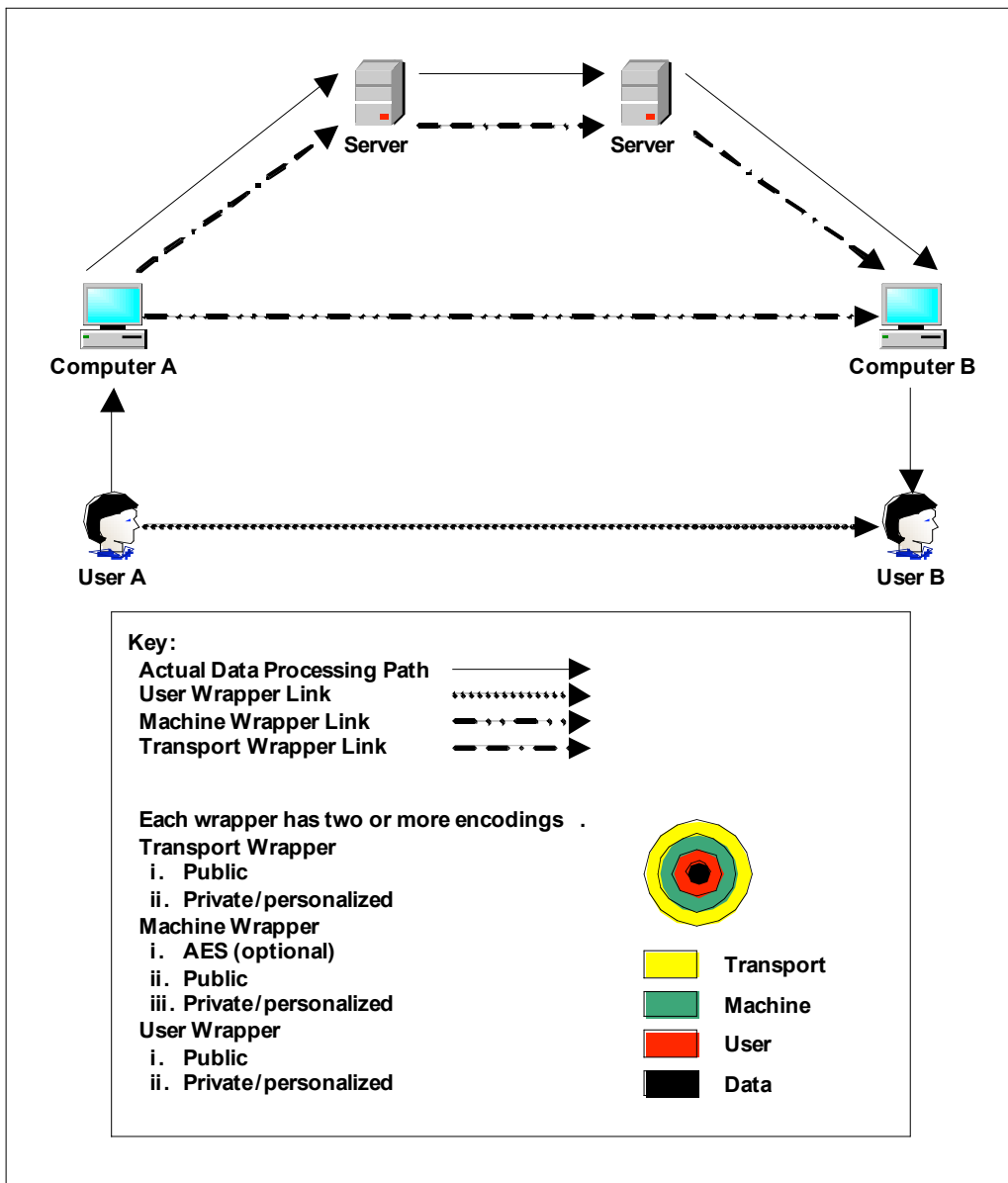
SkyLOCK™ eFT was developed for the purpose of transmitting secure data between a sender and or receiver. The security is such that once a sender transmits a message, only the designated or specified receiver can open or decrypt the data package. The data to be transmitted may exist in many forms, in the form of a file (bit or text) or in the form of messages, graphics, video, voice or data. This is a brief explanation of the eFT product functions.

**OPERATION:**

SkyLOCK™ eFT creates a secure "virtual private network", a link, or "pipeline" for transmission between a sender and a receiver. ESI technologists have designed into this product the capability for having the

network architecture be defined by a systems administrator who can be responsible for the overall performance of the company network. Therefore the Administrator can be responsible for determining who may send and receive messages within that network, and their authentication via passwords and pin management.

Since the architecture is developed around the sender and receiver, the technologists have developed a series of levels (layers) to enhance the security of the transmission thereby increasing the protection for data or media. These levels or layers are referred to as “wrappers”, single wrap for the user, DoublWrap™ for the user and the user’s machine, and TriplWrap™ for the transport level or layer. Each wrapper has a minimum of two encodings, public and private/personalized for the user; public and private/personalized for the user’s machine, with an option for the use of an AES algorithm or encoding if desired under the license; and a public and private/personalized encoding for the transport layer. The processes are described and shown on the diagram provided below.



When a message is sent to a receiver through a server, the server “peels back” the transport wrapper, looks at the address, re-wraps the transport layer and sends the message on to either the next server or the intended receiver. The message file or media aren't revealed, only the address. There is no delay or latency experienced in this process.

the package has arrived at the correct destination and the intended receiver “opens” or decrypts the package the sequential number is automatically sent back to the sender’s file for audit purposes. If for example a number does not appear in the sender’s log, then one of three events may have happened: one, the package never arrived and is lost in the “virtual world”; or, it has been stolen; or, the receiver has not yet opened or decrypted the file. In the event that the package was stolen and the thief tries to decrypt the file, that person cannot open-decrypt the file because it cannot be decrypted on a machine that was not intended to receive the package in the first place. This is because there is a specific code or designation specific to a device- machine that is associated with a particular user.

In addition to this protection, the thief would require all six encodings, excluding the 256 bit AES encoding, to decrypt the file, plus the pin and password of the receiver to crack the file.

It should be noted that the SkyLOCK™ eFT product is complete and in testing. InfoGard, one of the two nationally designated laboratories, is accredited by NIST to test and analyze new commercially available products. InfoGard has both a domestic and international reputation in this unique field of encryption testing.

InfoGard completed its review of the ESI security module, SkyLOCK™ and the module passed. InfoGard submitted its report to NIST on Oct. 13, 2006 recommending to NIST that SkyLOCK™ meets the FIPS 140-2, level 2 standard. NIST awarded ESI FIPS 140-2, level 2 certification on March 9, 2007 and this certification has been posted on the NIST site.

The following algorithms used by SkyLOCK™ have been certified by InfoGard to meet the requirements for FIPS-140-2 standards. After each algorithm is the certification number and a link to the NIST website to view the certification:

- SkyLOCK™ AES – #413 <http://csrc.nist.gov/cryptval/aes/aesval.html>
- SkyLOCK™ SHA-1 - #482 <http://csrc.nist.gov/cryptval/shs/shaval.html>
- SkyLOCK™ SHA-1 HMAC-#187  
<http://csrc.nist.gov/cryptval/mac/hmacval.html>

#### SUMMARY:

The key features and benefits are listed below:

- Secure end-to-end transmission, wireless or wired
- Multi level-multi layer protection
- User/Group/Machine specific encryption
- Bandwidth Frugal
- Minimal latency
- The data package is encrypted at rest until it is decrypted or opened by the intended receiver.
- Speed is limited only by the speed of a device's RAM
- SkyLOCK™ is compact with a small footprint
- Data is compressed first then encrypted, "loss-less" compression
- No repeat signature or pattern
- Hardware and platform independent
- Interoperable with MS Windows, Linux, Unix
- Security module has been tested, passed and posted to NIST Site.
- Data tracking and audit capability to meet compliance regulations