



## CryptoXpress™ LT

### ***An Affordable, Commercial Grade, "Strong" Encryption Solution***

#### **CryptoXpress LT Enterprise Focus**

What differentiates CryptoXpress LT from the competition? CryptoXpress LT focuses on providing an enterprise level solution for users who require:

- Cross platform support - a solution that can secure Windows, Linux, Unix, OS/400 and zOS users.
- Cross language support - a solution that can be accessed from multiple programming languages.
- Strong encryption - a solution that supports multiple "strong encryption" algorithms as defined by the National Institute of Standards and Technology (NIST).
- Message digest support - a solution that supports multiple message digest algorithms.
- Usability - a solution that eases the burden of correctly implementing cryptography features that produce repeatable results consistent with NIST standards.
- Pricing - an affordable solution.

#### **CryptoXpress LT Overview**

CryptoXpress LT is a cryptography solution that features "strong encryption" capabilities as defined by the National Institute of Standards and Technology. CryptoXpress LT supports multiple security features including:

##### **Strong Encryption:**

- AES 128-bit
- AES 256-bit
- Triple DES

##### **Message Digests:**

- MD5
- SHA1

#### **Why Use Strong Encryption and Message Digests**

As committed as IT professionals are to preventing perpetrators from compromising their systems, one would think that systems and data are well protected. Yet, the FBI reports that most systems can be compromised in minutes by professional criminals using "targeted attacks".

Unless your data is encrypted at the application layer using "strong encryption" successful attacks can result in loss of data, identity theft, data sabotage and eventually loss of customer and investor confidence.

The intent of an increasing number of attacks is to sabotage data by changing its content. Message digests are used to sign data so that unauthorized changes can be discovered.

Security breaches leading to identity fraud have become so common that now most businesses have to comply with industry standards and government regulations that require the use of "application layer security".

CryptoXpress LT addresses the need for an affordable, commercial grade, strong encryption solution that can be deployed at the application layer on nearly any platform within the enterprise.

## Data Confidentiality

CryptoXpress LT can be used to encrypt and decrypt text, files and fields within a database. CryptoXpress LT supports EBCDIC, ASCII and binary data. Although it supports many encryption algorithms, the preferred encryption technology today is AES. AES is a block cipher (symmetric key) encryption algorithm that supports 128-bit, 192-bit and 256-bit key sizes.

May 19, 2005 the National Institute of Standards and Technology (NIST) announced the withdrawal of the (single) Data Encryption Standard (DES) as specified in FIPS 46-3. DES no longer provides the security that is needed to protect Federal government information. Federal government organizations are now encouraged to use FIPS 197, Advanced Encryption Standard (AES), which specifies a faster and stronger algorithm. For some applications, Federal government departments and agencies may use the Triple Data Encryption Algorithm (Triple DES) as specified in NIST Special Publication 800-67. Triple DES is also supported by CryptoXpress LT. Although thought to be considerably less secure than even AES 128-bit encryption, it is still commonly used in some industries.

## Data Integrity

CryptoXpress LT can be used to calculate a message digest for data, files and fields within a database. The act of calculating a message digest is sometimes referred to as "digesting" the information. The result of a message digest is sometimes referred to as a digital signature.

A message digest (also sometimes referred to as a one-way hash function) is a fixed length computationally unique identifier corresponding to a set of data. The result of the algorithm is that each file or data string digested will map to a particular block of information called a message digest. The digest is not random; digesting the same unit of data with the same algorithm will always produce the same message digest.

Most users prefer to use the MD5 message digest algorithm. MD5 belongs to a family of one-way hash functions called message digest algorithms. The MD5 system is defined in RFC 1321. MD5 takes a message of arbitrary length and produces as output a 128-bit message digest. It is conjectured that it is computationally infeasible to produce two different messages having the same message digest, or to produce any message having a given message digest. RFC 1321 also defines a certification suite to validate correct implementation of the algorithm. CFXMD5 is validated against this suite.

Message digests have many uses. In particular they are used to authenticate data. For example, to create a digest for authentication, data can be digested and the digest saved. Later, to validate that the data has not been altered, the data is digested again and the result is compare against the original digest. If they differ, the data has been altered. This is very different from encryption because the actual data is not modified when it is digested. Encryption is intended to protect the confidentiality of data. A message digest is used to assure data integrity.

The HMAC functions support keyed-hashing capabilities that use either MD5 or SHA1. HMAC is commonly used for message authentication. For example some credit card processors require the user to include a HMACMD5 or HMACSHA1 message digest in the transactions sent to their gateways.

## CryptoXpress LT Benefits

- Encryption complexity reduced to 6 best practices deployment scenarios.
- Message digest complexity reduced to 4 best practices deployment scenarios.
- IBM Certified across numerous IBM and non-IBM H/W & S/W platforms.
- Consistency verified across all supported environments.
- Correctness of SDK implementation verified using NIST test vectors.
- Resource & skill level minimized by use of "best practices" scenarios.
- Product priced to be affordable in SMB market.

## Industry Standards and Regulations

The following list identifies some of today's current regulations and legislation requiring the use of strong encryption. In particular, if you are a merchant doing any e-Commerce transaction over the web, make sure you are familiar with the Cardholder Information Security Program (CISP) and Payment Card Industry Data Security Standard (PCI).

- The Sarbanes-Oxley Act (SOX)
- The Gramm-Leach-Bliley Act, the Safeguards Rule (GLBS)
- Health Insurance Portability and Accountability Act (HIPAA)
- California Assembly Bill 1950 (AB 1950)
- Title 21 of the Federal Regulations Part 11 (21 CFR Part 11)
- California Information Practice Act or Senate Bill 1386
- North American Electric Reliability Council (NERC)
- Federal Information Security Management Act (FISMA)
- USA PATRIOT Act
- Cardholder Information Security Program (CISP)
- Payment Card Industry Data Security Standard (PCI)
- Federal Information Processing Standards (FIPS)
- National Association of Securities Dealers Rule 2711
- SEC 17a-4

## IBM Certification

CryptoXpress LT has been tested and received the "IBM Server Proven", "IBM Ready for Linux", and "IBM Ready for WebSphere" marks from IBM. These marks show that CFXWorks has tested CryptoXpress LT successfully on the IBM platforms and that the product is backed by IBM marketing and technical support. CryptoXpress LT has also been tested on several additional platforms including Windows, Linux (Intel) and IBM's iSeries running OS/400.

## CryptoXpress LT Supported Platforms

Enterprise users must have the ability to transport encrypted data and message digests from one platform to another. Data encrypted on one platform frequently will require decryption on another. CryptoXpress LT will execute on the following platforms:

- Any Java 1.3, 1.4, or 1.5 enabled platform
- IBM's xSeries running Windows or Linux
- IBM's pSeries running Linux or AIX
- IBM's zSeries running Linux or zOS
- IBM's iSeries (AS/400) running OS/400 or Linux
- Any Intel platform running Windows or Linux
- Solaris and HP-UX

## Company Description

CFXWorks was founded as a Georgia corporation in 1993 by Al Nickles. Al was the inventor of IBM's MQSeries in the mid 1980s and managed the startup of IBM's MQSeries laboratory. We specialize in developing cryptography and secure messaging solutions.

Our customers tend to be organizations processing sensitive information that cannot be compromised for financial, political, safety or regulatory reasons. They represent many industry sectors including:

- Federal, state and local government
- Financial institutions
- Insurance
- Retail
- Cross industry ... credit card, fraud protection and web services

We have delivered products to over 500 customers in the US, Europe and South America. Our customers include several ISVs, U.S. Courts, U.S. Intelligent Agencies, State of Michigan Department of Corrections, IBM, Sun Microsystems, Equifax, Bell South, Bell Atlantic, Northside Hospital, Fidelity National Bank, Xerox Connect, Boeing, Reuters, Time Warner, EDS Canada, South Carolina Retirement Systems, South Carolina Employee Insurance Programs, New York City Police Department, Bank of Canada, NASA, the United Nations, and the National Institute of Standards and Technology (NIST).

## CryptoXpress LT Reseller

**Curbstone Corporation** is a reseller for the CryptoXpress LT program. Curbstone offers sales and installation support for this offering.

## CryptoXpress LT Ready to Run Programs

The following programs are included in CryptoXpress LT:

Program:	Description:
CFXCMD	<p>This program can be used to read command line arguments and pipe them to programs that read data from the standard input device (sysin).</p> <p>CFXCMD reads command line arguments and writes them to the standard output device (sysout). Note that this program outputs data exactly as it is interpreted by the operating system's command line parser. Depending on the operating system, it is impossible to pass some characters within command line arguments. Some characters are likely to be ignored and some are interpreted differently than you might expect. Therefore test your input carefully if you intend to use this program.</p>
CFX103FF	A Java program that can be used to encrypt or decrypt a file using 128-bit AES/PKCS5Padding/CBC and writes the output to a file.
CFX103TF (1)	A Java program reads data from the standard input device (sysin) encrypts it using 128-bit AES/PKCS5Padding/CBC and writes the output to an encrypted file.
CFX104FF	A Java program that can be used to encrypt or decrypt a file using 256-bit AES/PKCS5Padding/CBC and writes the output to a file.
CFX104TF (1)	A Java program reads data from the standard input device (sysin) encrypts it using 256-bit AES/PKCS5Padding/CBC and writes the output to an encrypted file.
CFX112FF	A Java program that can be used to encrypt or decrypt a file using 3DES and writes the output to a file.
CFX112TF (1)	A Java program reads data from the standard input device (sysin) encrypts it using 3DES and writes the output to an encrypted file.
CFX401F	A Java program that reads an input file, digests it using MD5, and writes the output to the standard output device (sysout).
CFX401T (1)	A Java program reads data from the standard input device (sysin), digests it using MD5, and writes the output to the standard output device (sysout).
CFX402F	A Java program that reads an input file, digests it using SHA1, and writes the output to the standard output device (sysout).
CFX402T (1)	A Java program reads data from the standard input device (sysin) digests it using SHA1 and writes the output to the standard output device (sysout).
CFXF2D	A Java program that reads a file and displays it in HEX to the standard output device (sysout).
CFXT2F (1)	A Java program reads data from the standard input device (sysin) and writes the output to the standard output device (sysout).
CFXDisplayLicense	Displays the CryptoXpress license information to the standard output device (sysout).
CFXConvert	Converts a file from ASCII to EBCDIC or from EBCDIC to ASCII.



Al Nickles  
CEO/CTO  
CFXWorks, Inc.

770-441-0952  
anickles@cfxworks.com



**Learn more about CryptoXpress LT, call today and schedule a Webex conference:  
770-441-0952**



[www.cfxworks-enterprise.com](http://www.cfxworks-enterprise.com)