



## **CryptoXpress™ SDK**

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

#### **CryptoXpress SDK Enterprise Focus**

What differentiates CryptoXpress SDK from the competition? CryptoXpress SDK 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.
- Credit card security features - a solution that supports security features unique to the credit card industry.
- Fraud protection features - a solution that supports fraud protection features related to address verification.
- 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 SDK Overview**

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

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

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

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

- MD5
- SHA1
- HMACMD5
- HMACSHA1

##### **Credit Card Security Features:**

- LUHN formula (Mod 10) account number validation.
- Account number masking as per credit card processing industry standards.

##### **USPS Address Information Services:**

- USPS Address Verification APIs
- USPS Zip Code lookup APIs
- USPS City/State lookup APIs

## 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 SDK 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.

## Technical Challenges

Traditionally, encryption and message digest technologies are some of the most difficult technologies that programmers must deploy. Yet, almost all security features are built using these technologies. Their implementation requires considerable thought and absolute concentration to produce valid, repeatable results. One of the major reasons why hackers are so successful at compromising systems is that programmers either avoid using these technologies or deploy them incorrectly.

The core issue is that most cryptography toolkits are extremely complex and difficult to use. Using them correctly can require many weeks of intense effort. Programmers fall victim to too much documentation, too many APIs and not enough examples. Even if the programmer understands precisely what they want to do, they are swamped with decisions:

- Which encryption algorithms to use?
- Which key size to use?
- Will I use a user provided key, a secret key, or a key file?
- Is an initialization vector required and if so, how is it created and deployed?

- Which encryption mode will be used?
- What padding option will be used, if any?
- Which provider will be used?
- How will short keys be handled?

Mathematically speaking, there are thousands of possible combinations that can be applied to the task at hand. Of the thousands of possible combinations, which ones produce valid, repeatable results and provide the level of protection required? CryptoXpress SDK simplifies the selection process by reducing the decision process to 6 "preferred" combinations:

- AES128/PKCS5Padding/ECB
- AES256/PKCS5Padding/ECB
- AES128/PKCS5Padding/CBC
- AES256/PKCS5Padding/CBC
- TripleDES/PKCS5Padding/ECB
- TripleDES/PKCS5Padding/CBC

Each of the above options creates results that have been validated using the test vectors provided by the NIST, or the appropriate standards organization. Typically a user would pick one of these preferred methods and stick with it. It just doesn't get any easier than this!

## Data Confidentiality

CryptoXpress SDK can be used to encrypt and decrypt text, files and fields within a database. CryptoXpress SDK 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 SDK. Although thought to be considerably less secure than even AES 128-bit encryption, it is still commonly used in some industries.

## Data Integrity

CryptoXpress SDK 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 compared 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.

## Credit Card Security Features

The credit card industry requires use of additional security features:

### **LUHN formula (Mod 10) validation:**

The LUHN formula was created in the late 1960s by a group of mathematicians. Shortly thereafter, credit card companies adopted it.

Because the algorithm is in the public domain, it can be used by anyone. The LUHN formula (also known as the Modulus 10 or Mod 10 algorithm) is used to generate, validate and verify the accuracy of credit-card numbers. Almost all institutions that create and require unique account or identification numbers use the Mod 10 algorithm. For example, the LUHN formula is widely used to validate many different forms of account numbers. CryptoXpress SDK provides a function that validates that a value passed to the function passes the Luhn formula test.

### **Account number masking as per credit card processing industry standards:**

The Cardholder Industry Security Standard (CISP) is specific relative limiting what credit card account number data can be displayed. Only the last four digits of the account number can be displayed. CryptoXpress SDK provides a function that masks all but the last four digits of the account number.

## USPS Address Information Service

The service supported by this gateway includes the "Address Information" APIs published by the United States Postal Service. The USPS Address Information APIs support the following:

### **Address Standardization API:**

This API corrects errors in street addresses, including abbreviations and missing information, and supplies Zip Codes and Zip Codes + 4. It supports one lookup per transaction. By eliminating address errors, businesses improve overall package delivery service.

### **ZIP Code Lookup API:**

This Zip Code Lookup API returns Zip Code and Zip Code + 4 corresponding to the given address, city and state.

### **City/State Lookup API:**

This City/State Lookup API returns city and state for the given ZIP Code.

## 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 SDK 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 SDK successfully on the IBM platforms and that the product is backed by IBM marketing and technical support. CryptoXpress SDK has also been tested on several additional platforms including Windows, Linux (Intel) and IBM's iSeries running OS/400.

## CryptoXpress SDK 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 SDK 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 HPUX

## 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).



Al Nickles  
CEO/CTO  
CFXWorks, Inc.

770-441-0952  
anickles@cfxworks.com

