



CryptoXpress™ CF

A Commercial Grade, "Strong" Encryption Solution for ColdFusion

CryptoXpress CF Enterprise Focus

What differentiates CryptoXpress CF from the competition? CryptoXpress CF 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.

CryptoXpress CF Overview

CryptoXpress CF is a ColdFusion Custom tag that features "strong encryption" capabilities as defined by the National Institute of Standards and Technology. CryptoXpress CF supports message digests:

Strong Encryption:

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

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 CF 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 CF simplifies the

selection process by reducing the decision process to 6 "preferred" combinations:

- AES128/PKCS5Padding/CBC
- AES256/PKCS5Padding/CBC
- 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.

Compatibility Modes:

CFXWorks has sold for many years C++ implementations of encryption and message digest solutions for ColdFusion. We offer a CFX_ENCRYPT_AES128 (128-bit), CFX_ENCRYPT_AES256 (256-bit), and a CFX_MD5 tag. CryptoXpress CF supports most of the modes of operation supported by the original encryption tags including AES128/ECB, AES256/ECD, AES128/CBC and AES256/CBC. The digest results of this new tag are compatible with the original CFX_MD5 tag.

Data Confidentiality

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

Data Integrity

CryptoXpress CF 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.

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

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 CF Requirements

CryptoXpress CF requires ColdFusion 6.0 or greater .



Al Nickles
CEO/CTO
CFXWorks, Inc.

V: 770-441-0952

sales@cfxworks.com



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



www.cfxworks-enterprise.com