Public Comments on the Proposal to Approve FFX Schemes

On June 9, 2011, NIST announced a period of public comment, ending July 7, 2011, on a proposal to approve two schemes of the FFX framework for format preserving encryption. The announcement was posted on the News and Events page at NIST's Computer Security Resource Center.

Below are the public comments that NIST received in response to this request.

James Torjussen

Hi,

As a manufacturer of hardware security modules (HSMs) for use in the financial payments sector, Thales e-Security would welcome the publication of a standard in the area of format preserving encryption (FPE). Many of our customers are involved in processing payment card transactions, and wish to improve the level of security they provide, whilst at the same time, minimizing the impact to their existing (legacy) back-end systems. It is our belief that FPE in general, and FFX in particular, will provide our customers with the necessary methods to achieve their goal.

Best Regards,

James Torjussen
HSM Product Manager

Thales
Meadow View House, Long Crendon, Aylesbury, Bucks HP18 9EQ
www.thalesgroup.com/iss

Sarah McCrary

To whom it may concern:
Heartland Payment Systems supports the NIST approval of the FFX framework. Encryption solutions based on FFX have provided useful applications for the protection of credit card account and authorization data. Because the format of the data did not have to be altered to take advantage of the encryption protection the implementation of an FFX framework solution was straightforward and met with low resistance within the Heartland operating environment.

Thank you.

Sarah McCrary
Heartland Payment Systems – Director of Product Delivery

6860 Dallas Parkway
Suite 400
Plano, TX 75024

Timothy Masey

To: NIST Computer Security Division
Re: Comments on the Proposal to Approve Two FFX schemes

I would like to recommend the approval of FFX schemes for Format Preserving Encryption (FPE) methods proposed for two block cipher modes of operation, these were announced on June 9, 2011. Our implementation and use of FFX at AAA The Auto Club Group has allowed our organization to encrypt with no changes to database schemas and few application changes utilizing the Voltage Security Systems encryption software for FPE. Our implementation of these encryption methods have enhanced our security and confidentiality of data throughout the organization on various platforms. Without the support of FPE we would have engaged in a longer project plan attempting to re-write portions of applications and table structures within databases. FPE has provided a framework for us to move forward with encryption services at a rapid rate of deployment, ensuring PCI compliance for our entire organization.

Please consider this recommendation in review of the FFX mode as a recognized NIST standard.

Feel free to contact me of any additional questions or comments.

Thank you,

Tim Masey, CISSP
Director of Enterprise Information Security
AAA - The Auto Club Group

Umesh K. Tiwari

Support for AES FFX mode (Format Preserving Encryption) given its strategic importance to my company.

I am familiar with FPE concept and technology and very excited to learn that NIST is finally considering development of a standard around FPE.

The reason why FPE is so profoundly importance is that while the privacy control value of encryption is very well understood, without a technology that offers FPE, the baggage of long/unformatted encrypted string storage/processing and maintenance in business systems/databases is too burdensome to justify large scale implementation of encryption at database levels. FPE nicely resolves this problem by making the argument of storage capacity and performance completely irrelevant/non-issue by eliminating the format discrepancies between the source and cyphertext data. End-to-end encryption with proper key separation/control also makes the encryption control more business friendly and robust.

Umesh K. Tiwari, CISM, CISSP, PMP
IT Compliance & Risk
US Cellular

Bryan Bailey

To whom it may concern,

I'm writing today to express full support for approving the two FFX schemes currently under consideration by NIST. As a merchant acquiring processor, Vantiv is constantly looking for new ways to protect our merchant customers as well as their patrons. One such way is to protect sensitive cardholder data with encryption while in flight, often called end-to-end encryption. As a fairly new initiative in the industry, retrofitting existing payment platforms poses a significant challenge technically and financially. Format preservation eases the implementation of such protections by providing the ability to encrypt data without impacting existing fields in legacy message formats, databases, and data structures.

NIST approval of the FFX algorithms will also allow for simpler cryptographic architectures for acquiring processors such as Vantiv. Most host security module (HSM) vendors are unlikely to support unaccepted algorithms in their products. Because the industry has such a great need for increased data protection, there is a high probability that acquiring processors will be pressed to implement solutions with supporting vendors. Lack of global support will potentially require cryptographic hardware outside of what is utilized in current processing environments.

While these are the most obvious examples of the benefits of FFX in the merchant space, there are certainly others on both acquiring and issuing sides of a transaction. I ask that NIST strongly consider acceptance of the two FFX schemes for the benefit of the payments industry.

Sincerely,
Bryan Bailey

Bryan Bailey | VP, Online Systems Internals | Vantiv

Marco Mabante

Subject: VAES3 FPE Standard

I've been personally involved with the evolution of this method for over 6 years. It has the most acceptance and footprint in the industry today and my current pipeline of new merchants that plan to support it is enormous. To have this as an additional standard would be greatly appreciated.

Cheers,

Marco Mabante
Elavon
Director, Strategic Product and Security Solutions
Savannah, GA

Scott Sysol

In the IT environments that exist in large enterprises, traditional ways to encrypt sensitive data are difficult and very time consuming. Using AES-CBC encryption, for example, changes both the format of data as well as its length, and it's not at all uncommon for changing either of those to cause problems that are expensive to diagnose and work around. This makes implementing encryption much harder and more expensive that you might expect it to be. This then results in encryption not being used in many cases where it should be used, and this means we leave our sensitive data vulnerable.

Despite NIST's guidance that FIPS 140-2 is only for government use, the reality is that it's the *de facto* standard for encryption that most of the world looks to. FFX has proven useful for protecting sensitive information, but the fact that it is not yet an approved mode is slowing its adoption, and that means that sensitive data is still available to a hacker that doesn’t need to be. By moving ahead with its proposed approval of FFX, NIST will make it easier for businesses to protect sensitive information in a way that doesn't require the expensive changes to networks and applications that other approaches require. This will ultimately keep sensitive information out of the hands of hackers, so CUNA Mutual fully supports NIST moving forward with the approval of FFX.

Thank you,

Scott A. Sysol, CISM
VP & CISO

Dave Faoro

To: NIST Encryption Modes <EncryptionModes@nist.gov>

Subject: Comments on NIST's proposal to create a format-preserving encryption standard

VeriFone is pleased to hear that NIST has proposed to specify and approve two block cipher modes that are compliant with the FFX framework.

Unlike many other format-preserving encryption schemes, FFX is backed by a solid security proof and is the result of research by multiple cryptographers and a paper that was accepted at the Selected Areas in Cryptography 2009 conference. The pedigree of both encryption schemes proposed for standardization, VAES3 and FFX[radix], is outstanding.

Hundreds of millions of transactions have already been encrypted using these schemes. And while the cryptographic community has determined that encryption schemes based on FFX are strong cryptographically, the lack of a standard has limited broader adoption in applications and markets that have a great need for encryption but are unable to change their message structure. These markets including the financial industry such as credit card authorization and legacy applications and databases with sensitive information have a great need for format-preserving encryption. A standard format-preserving encryption mode would go a long way to supporting the protection of sensitive user information and support the reduction of identity theft.

VeriFone wholeheartedly supports the NIST proposal to create a standard around these two modes compliant with the FFX framework and encourage NIST to move forward with the creation of a Special Publication around these two modes.

Dave Faoro

VP, Chief Security Officer

VeriFone, Inc.

1400 West Stanford Ranch Road Suite 200 Rocklin, CA 95765

Matthieu Bontrond

Dear Mr. Dworkin,

Here are our comments regarding the submission for format preserving encryption mode.

We noticed that our proposal BPS was not included into the NIST approved schemes, however BPS provides a feature that FFX lacks: an efficient and convenient way to cipher long strings of data (the CBC-like operating mode). Indeed, to cipher long strings of data using FFX mode requires performing operations on huge numbers. Moreover, compared to BPS we denote twice more calls to the underlying block cipher. Thus the FFX mode will be more resources-consuming in constraint devices than BPS since the processor will have to perform more operations (hence more time-consuming). Another negative point to us is the need to wait for the complete input before starting the ciphering process. FFX is not streamable hence memory-consuming, which is not suitable to constraint devices.

In opposite, the BPS CBC-like mode is simple and can directly cipher each incoming block of data and maintains the same efficiency. Of course, the drawback is that the security can not be ensured up to the full input size, but only up to a single block size. Note that this is not an issue since one block size will already provide very high security. Moreover, the internal cipher of BPS is actually very close to the two FFX approved modes. It would be easy to get a generic description encompassing both FFX and BPS. Note that this is currently being done in another standardization effort (ANSI X9.124).

Including both BPS and FFX into a single description seems easy to do; this would ensure a large covering of the format-preserving algorithms that will be eventually used in the banking industry. Therefore, we believe the standard would benefit from a broader description that encompasses both FFX and BPS and from the inclusion of the CBC-like operating mode.

Best Regards,

Matthieu Bontrond

Matthieu Bontrond
Cryptography Expert

Todd Arnold

I would like to make some additional comments about the Format Preserving Encryption proposals.

1. It is impractical to have the standards defined so that the algorithms are so broadly defined via parameters. There are nearly an infinite variety of "algorithms" based on the values of the many algorithm-defining parameters that are in these specifications. I think it is essential that NIST limit these to a small list of "recommended" or "preferred" sets of parameters, to limit what vendors have to implement in their products. This would be analogous to the set of preferred ECC curves NIST defined - you do not make vendors support every mathematically possible curve, but instead you narrow it to a small set so that vendors know what to do and can design practical products.

2. The documents are written more as vague, academic papers than like precise, clear technical specifications and standard. They need to undergo major rewriting to make them suitable for the purpose of standards that implementers can use to design and test products. In addition to clearer, more precise, and more consistent language, they also desperately need concrete examples throughout, everywhere they introduce or discuss concepts.

3. The NIST standards MUST be completely interoperable with the ANSI standards on FPE (X9.124). Since they are being developed separately, it is essential the two groups work together to guarantee compatibility. One aspect of this is that X9.124 currently includes BPS while NIST does not. (Note that I was quite disturbed recently when NIST published their AES key wrap proposal and diverged from the existing ANSI X9.102. IBM implemented products to X9.102 and we are very unhappy that NIST published something that would make our products non-compliant with the NIST standards. It's unacceptable for you to define NIST standards for something that has already been done in another standards body, but make yours incompatible so that you "break" existing products.

Todd W. Arnold
Senior Technical Staff Member (STSM)
IBM Cryptographic Coprocessor Development