

FOR IMMEDIATE RELEASE

For further information:

Judith Vanderkay

[jvanderkay@gmail.com](mailto:jvanderkay@gmail.com)

+1 (781) 883-3793

## **ASC X9 Publishes New Standard for Preserving Formatting in Symmetric Key Cryptography, X9.124-2**

**ANNAPOLIS, Md.** – May 8, 2018 -- Today the Accredited Standards Committee X9 Inc. ([X9](#)) announced the publication of a new standard that defines requirements for using a particular method of preserving formatting in the encryption of financial services data. The standard, *X9.124-2 Symmetric Key Cryptography For the Financial Services Industry -- Format Preserving Encryption - Part 2: Key Stream with Counter Mode*, is now [available for purchase](#) from the ANSI Store.

The X9.124 standard defines a collection of format-preserving encryption methods for financial services. Format-preserving encryption (FPE) is useful in situations where fixed-format data, such as primary account numbers or Social Security numbers, must be encrypted, but there is a requirement to limit changes to existing communication protocols, database schemata or application code.

Encryption has historically been an expensive technique to deploy in real-world systems because of the need to alter the operation of existing systems and applications. The benefit of FPE techniques is that encryption can be added to existing systems in such a way that system modifications are kept to a minimum. Often, substantial savings can be realized because database schemas and financial applications can run with encrypted data without needing modification or replacement.

X9.124-2 defines requirements for using a particular approach – Key Stream with Counter Mode -- to specify a set of algorithms that securely encrypts formatted data and retains that format in the resulting ciphertext. Format-preserving encryption Counter Mode is a particularly simple and efficient mechanism for maintaining data format while also safeguarding its security. IT equipment vendors, banks, and retailers are some of the sectors that will benefit from X9.124-2.

"This new standard describes a straightforward method of preserving the format of important data while ensuring its security, leading to cost efficiencies in systems and processing throughout the industry," said ASC X9 Executive Director Steve Stevens.

"The new format-preserving encryption standard offers an additional encryption method to security professionals in search of a solution to efficiently protect data and privacy in a digital world," said Eric Le Saint, distinguished engineer, Visa, and chairman, X9F1 Working Group. "The development of the new standard is the result of hard work by many dedicated contributors from the X9F1 working group, to whom we are grateful."

**About the Accredited Standards Committee X9 Inc.**

The Accredited Standards Committee X9 Inc. is a non-profit organization accredited by the American National Standards Institute (ANSI) to develop both domestic and international standards for the financial services industry. X9 has over 100 member companies and over 400 company representatives that work to develop and maintain approximately 100 domestic standards and 58 international standards.

The subjects of X9's standards include: retail and mobile payments; printing, imaging and processing of checks; corporate treasury functions; distributive ledger technology; processing of legal orders issued to financial institutions; tracking of financial transactions and instruments; tokenization of data; protection of financial data at rest and in motion; data breaches; electronic contracts; and remittance data in business payments. X9 also performs the secretariat function and provides the committee chair for ISO TC 68, which produces international standards for the global financial services industry. For more information about X9 and its work, visit [www.x9.org](http://www.x9.org).

*Follow ASC X9 on [Facebook](#), [LinkedIn](#) and [Twitter](#)*

###