

FOR IMMEDIATE RELEASE

For further information:
Judith Vanderkay
jvanderkay@gmail.com
+1 (781) 883-3793

ASC X9 Completes Update of ANSI X9.24-1, Detailing Requirements for Managing Symmetric Keys in Secure Retail Financial Transactions

Covers Keys Used in POS and ATM Transactions

ANNAPOLIS, Md. – August 1, 2017 -- Today the Accredited Standards Committee X9 Inc. ([X9](#)) announced the completion of an updated edition of ANSI X9.24-1, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques. X9.24-1 is one of the most important standards relevant to PIN-based financial transactions. This standard provides requirements and guidelines for secure management of symmetric keying material used in retail financial services transactions and communications.

Symmetric key encryption uses one secret key to both encode and decode the contents of a message; the sending and receiving parties must use the same key to make sense of the message. The original version of X9.24-1, published in 2009, is now obsolete. The new standard is now [available for purchase](#) from the ANSI Store.

"In order to depend upon the PIN (Personal Identification Number) to demonstrate that the user of a credit or debit card is authorized to do so, that PIN must be known only to the cardholder, and therefore must be kept secret throughout the transaction," said Scott Spiker, Sr. Security Engineer and founder of Cipherithm LLC, Chair of X9's Cardholder Authentication and ICCs (integrated chip cards) Working Group. "This standard addresses the management of the cryptographic keys used to protect the PIN whenever it is outside the hardware that is specifically designed and certified to protect against PIN disclosure. Our working group redesigned the document to include advancements within the industry and provide additional depth related to safeguarding the keys."

Updated items in X9.24-1-2017 include additions to the minimum key management security requirements, the inclusion of AES (Advanced Encryption Standard) algorithm and new technology in hardware devices used to protect cryptographic keys, as well as significant modifications in the standard's structure.

X9.24-1-2017 specifies the minimum requirements for the management of keying material used for financial services such as point-of-sale (POS) transactions (both debit and credit), automated teller machine (ATM) transactions, messages among terminals and financial institutions, and interchange messages among acquirers, switches and card issuers. The requirements cover the full key life cycle. An institution's key management process cannot be implemented or controlled in a manner that has less security, protection or control than X9.24-1-2017 describes.

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 and processing of checks; corporate treasury functions; block chain 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; 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.

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

###