FOR IMMEDIATE RELEASE

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

ASC X9 Releases New Standard for Ensuring Security of Symmetric Key Management in Retail Financial Transactions, Using AES DUKPT Algorithm

ANNAPOLIS, Md. – Nov. 28, 2017 -- Today the Accredited Standards Committee X9 Inc. (X9) announced the release of a new standard enhancing the security of symmetric key management used in retail financial services transactions and communications.

ANSI X9.24-3-2017, Retail Financial Services Symmetric Key Management -- Part 3: Derived Unique Key Per Transaction (DUKPT) allows financial institutions to use the Advanced Encryption Standard (AES) algorithm in a secure and interoperable way to provide confidentiality through encryption of PINs and cardholder data, transaction authentication and much more. The standard is now available for purchase from the ANSI Store.

Merchants use symmetric key encryption inside the payment terminal to protect consumer debit PIN and cardholder data. Symmetric key encryption uses a single secret key to protect the contents of a message; the sending and receiving parties must use the same key to successfully transmit information in the message. But using the same key multiple times can put the key, and the data being protected, at greater risk in the event of an attack. To mitigate the damage of a single key being compromised, a DUKPT algorithm is used by the sending and receiving parties to independently derive a new but identical secret key for each new message. Therefore, if one key is compromised, messages sent using other keys are still protected.

The AES DUKPT algorithm, which uses the U.S. government approved Advanced Encryption Standard, is intended to replace a nearly 40-year-old standard based on DES technology. AES DUKPT is a major improvement over the previously used algorithm because, among other benefits, it provides a much larger set of unique secret keys. The new algorithm can generate 2.5 billion unique keys versus about 1 million for the prior version. The keys generated by the DUKPT algorithm can be used for a variety of functions, such as encryption of card PINs, card and financial data or other keys, for derivation of other keys, for message authentication, etc.

"There is a real push in the financial industry to move to AES and AES DUKPT, as the future of financial transactions: we can now progress to using the best security that cryptography has to offer," said Joachim Vance, Chief Security Architect, Verifone, and editor of the X9.24-3

standard. "AES DUKPT supports up to 256-bit AES keys, which are immune to all known methods of brute force attacks, even quantum computing attacks."

Additional information from Vance about the value of the AES DUKPT algorithm is provided in an article on the Verifone website, "The Master of Keys."

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

###