FOR IMMEDIATE RELEASE

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

X9 Issues New Update to Cryptographic Key Management Standard, Adding Protection Against Quantum Computing Attacks

ANNAPOLIS, Md. – July 25, 2023 -- The Accredited Standards Committee X9 Inc. (X9) today announced the publication of an update to its X9.69 standard, *Framework For Key Management Extensions*. This standard defines methods for the generation and control of keys used in symmetric cryptographic algorithms, and the new version includes methods for quantum computing protection, a framework supporting an algorithm at any key length, and provisions to support compliance with HIPAA, Europe's GDPR and other privacy regulations. It is available for purchase through the ANSI website.

The X9.69 standard is an important one, concerned with key systems for message encryption in which the encrypting and decrypting keys are identical. It defines a constructive method for the creation of symmetric keys, by combining two or more secret key components. It also defines a method for attaching a key usage vector to each generated key that prevents abuses and attacks against the key. The two defined methods can be used separately or in combination.

Additionally, the security and reliability of any process based on a symmetric cryptographic algorithm is directly dependent on the protection afforded to the secret quantity, the key. Thus, no matter how strong the algorithm, the system is only as secure as its key management method. With the expected advent of quantum computing, secure key management becomes even more important, as a large-scale quantum computer could easily break the most widely used encryption schemes. This standard provides an immediate and complete solution to quantum computer attacks using Shor's Algorithm.

The standard also offers a framework supporting an algorithm at any key length. For adopters of the standard, this makes it future-proof, deployable now and accommodating of any new algorithms in the future. The new X9.69 can be applied immediately to multiple data representations, such as those of ISO 20022 and QR code payments, as well as any structured and unstructured data. The updated version provides protection of data at the object level, independent of the transmission layer or storage choice, and a persistent protection solution to data security that supports any enterprise configuration, including cloud, hybrid cloud or multi-cloud.

"This new version of X9.69 can be seen as offering an immediate solution to the threat of quantum, as well as an answer to the differential access to content necessary to support various laws and regulations around privacy in the United States and elsewhere," said Jay Wack, CEO of Tecsec, who served as editor for the standard. "X9 is delivering a vital tool for establishing and maintaining the security and privacy of encrypted messaging."

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 and maintain national and – through ISO -- international standards for the financial services industry. The subjects of X9's standards include: retail, mobile and business payments; corporate treasury functions; block chain technology; processing of electronic legal orders issued to financial institutions; tracking of financial transactions and instruments; financial transaction messaging (ISO 8583 and 20022); quantum computing; AI, PKI; checks; cloud; data breach notification and more.

X9 acts as the U.S. Technical Advisory Group (TAG) for ISO TC68 (Financial) and TC321 (E-Commerce) and performs the secretariat functions for ISO TC68. Please visit our website (www.x9.org) for more information.

Follow ASC X9 on Facebook, LinkedIn, Twitter and YouTube

###