X9 Launches Effort to Create Post-Quantum Cryptography Assessment Guidelines; Participants Sought

ANNAPOLIS, Md. – June 13, 2023 -- The Accredited Standards Committee X9 Inc. (X9) today announced the development of a new technical report, TR 61 -- Post-Quantum Cryptography (PQC) Assessment Guidelines. The report will provide objectives and assessment criteria. X9 seeks participants for the initiative.

In a post-quantum world, data must be protected against attacks from both quantum and conventional computers. Post-quantum cryptography is the next generation of cryptographic algorithms, designed to protect data against attacks from both quantum and conventional computers. The transition from current cryptography to PQC is a complex process that will require resources, knowledge and planning.

One of the first things a company needs is an understanding of its current cryptography, to identify systems and software that will need to be upgraded or replaced with post-quantum cryptography. The assessment in the technical report will include a set of criteria that will help to identify the areas that will need upgrading to PQC. This assessment will provide initial information needed to identify systems using legacy cryptography, thus allowing the start of project planning activities targeting the work that will need to be performed. The new technical report will build on quantum-related work products already developed by X9.

The cryptographic transition to PQC algorithms will affect not only the financial industry but also X9 standards. Part of the development of the assessment guidelines will be to identify X9 standards that will need to be updated to include PQC. The guidelines will act as a roadmap for the next stages of the PQC transition.

When completed, the X9 guidelines might be used by an organization as a self-assessment tool, as an informal assessment of a third-party service provider or as an independent assessment by a qualified information security professional. An auditor or regulator might refer to these assessment guidelines. The guidelines might also be the foundation for crypto agility standardization.

"As we prepare for the advent of quantum computing and its aftermath, we realize that the entire financial services industry, from financial institutions, regional banks, credit unions and retail merchants, to service providers, cloud providers and mobile operators, will need to transition to PQC algorithms, and possibly to alternative key management methods," said Michael Talley of University Bank, chair of the X9F1 Cryptographic Tools working group, which will carry out the initiative. "It will be important to have PQC assessment guidelines available before transitions are underway, for consistency to make the process as smooth as possible and the outcomes optimal."

Prospective participants can indicate their interest on the X9 website.

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

###