FOR IMMEDIATE RELEASE

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

ASC X9 Issues New Standard for Public Key Cryptography/ECDSA

Standard Focuses on Elliptic Curve Digital Signature Algorithm Use

ANNAPOLIS, Md. – Oct. 6, 2020 -- The Accredited Standards Committee X9 Inc. (X9) today announced that it has published a new standard, *X9.142, The Elliptic Curve Digital Signature Algorithm (ECDSA)*. This standard defines a mechanism to facilitate the secure authentication and non-repudiation of data in financial and other online transactions, using the ECDSA. X9.142 is now available for download.

The replacement of paper-based transactions by electronic ones has reduced costs and improved efficiency, but it can also yield potentially severe risks such as unauthorized accessing, disclosure, forgery or alteration of data, if protection is insufficient. Digital signatures, in combination with other cryptographic techniques, help ensure the integrity and origin of received data, and thus also help to ensure that sent data goes only to an authorized recipient (when encrypting to a public key that has been digitally signed).

Given a message, a digital signature, and the signer's authentic public key, cryptographically verifying the signature assures a verifier that the signer's private key was applied to the message when generating the signature. If the signer's private key is kept secret from attackers, no known forgery attacks work against a properly secured implementation of ECDSA.

X9.142 specifies a digital signature algorithm, the ECDSA. Elliptic curve signatures, such as ECDSA, are the fastest and smallest available secure digital signatures, and they are now used widely, often replacing legacy RSA signatures. Some of the most prominent websites are now secured with the help of ECDSA. The web server generates an ECDSA signature in a secure handshake for each web visitor. Web browsers verify the ECDSA signature, showing this verification to the user by way of a secure lock icon next to the web address. A blockchain financial transaction may also use an ECDSA signature to permanently bind the transaction on a ledger.

The X9.142 ECDSA standard provides methods and criteria for generating the public and private keys that the ECDSA requires, and procedural controls needed for secure use of the algorithm with these keys. The standard also provides methods and criteria for generating the elliptic curve

domain parameters that the ECDSA requires, and procedural controls for secure use of the algorithm with these domain parameters. It replaces X9.62-2005, an earlier specification of the ECDSA.

"The ECDSA has been used for over 20 years to authenticate electronic data. Recently, it has become even more popular, authenticating much of today's internet traffic, including top websites," said Dan Brown, Senior Standards Manager at BlackBerry, and editor of the X9.142 standard. "The financial community has collaborated to develop cryptography standards such as X9.142, leading to strong electronic transaction data security that benefits all stakeholders, from financial institutions and online service providers to financial customers and general internet users."

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; PKI; checks; cloud; data breach notification and more.

X9 acts as the U.S. Technical Advisory Group (TAG) for ISO TC68 (Financial), TC321 (E-Commerce) and TC322 (Sustainable Finance) and performs the secretariat functions for ISO TC68. Please visit our website (www.x9.org) for more information.

Follow ASC X9 on Facebook, LinkedIn and Twitter

###