

## ASC X9 Launches New Security Study Groups on Public Key Infrastructure (PKI) and Transport Layer Security (TLS)

ANNAPOLIS, MD - The Accredited Standards Committee X9 Inc. ([X9](#)) has formed new study groups that aim to improve security and safeguard privacy for the financial services industry in two related areas: one will look into issues regarding Public Key Infrastructure (PKI) Certificate Authorities and the other will research concerns related to use of the Transport Layer Security (TLS) protocol. Participants in both new initiatives are [sought](#).

### PKI Study Group

The purpose of a Public Key Infrastructure (PKI) is to facilitate the secure electronic transfer of information for network activities such as e-commerce, internet banking and confidential email, where simple passwords are inadequate. A PKI functions through a process of registering and issuing certificates via a Certificate Authority (CA).

Existing commercial CAs provide digital certificates for protecting internet traffic, and legacy systems rely on the same certificates for browsers, mobile apps and servers. However, security policies for financial services (including strong authentication for web-based financial transactions) increasingly have different requirements from general internet use. As financial services evolve towards such things as distributed ledger technologies (e.g., blockchain), the Internet of Things and quantum computing, gaps will continue to grow.

This new X9 study group for PKI will seek solutions that protect the financial services industry's interests while maintaining a strong security and privacy posture for its customers. The group will examine issues related to private CA and public third-party CA service providers and investigate the opportunity of an independent, dedicated CA for the financial services industry.

### TLS Study Group

Transport Layer Security is a cryptographic protocol for providing secure communications over a private computer network or the internet; TLS replaces Secure Sockets Layer (SSL), which is obsolete. TLS is widely used to provide privacy and data integrity between two communicating applications, such as between a website server and a computer or mobile browsers, between a web server and a mobile app, or even between two servers. Many virtual private networks that provide privacy over the internet are TLS-based. Like many internet protocols, TLS continues to evolve and software implementations struggle to keep pace. Meanwhile, changes in the most recent TLS version will affect financial institutions and other large organizations.

The new X9 study group for the TLS protocol will research problems encountered in current usage of the protocol, review concerns with the new TLS version, and consider potential future issues. The group will work to determine tactical and strategic solutions for the financial services industry, which might include new standardization efforts, implementation guidelines or other possible activity including alternative protocols.

"These new initiatives will provide important additions to the landscape of financial communications security and privacy," said Steve Stevens, executive director of ASC X9.

"Building on our robust history of creating and maintaining ANSI and ISO standards, X9 members are committed to developing the technical financial standards needed for our industry to act efficiently and competitively in the marketplace. We invite any interested subject matter experts to [participate in these efforts](#)."

**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 national 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](http://www.x9.org).