CSA Financial Standards Article

Standards for Quantum-Safe Security and the Financial Industry
Written by Denis Mandich, Quantum-Safe Security Working Group Member and CTO for Qrypt

The financial community relies on several standards organizations to provide consensus guidance on protecting data and information exchanges, primarily for payments and securities transactions. These standards ensure interoperability and a common understanding of the issues facing this community, to include emerging technologies like quantum and Artificial Intelligence (AI). The Accredited Standards Committee (ANSI) X9 organization produces informational and technical reports compiled from within their own working groups to educate industry experts. This is a consortium of large enterprise and industry volunteers from various sectors to align on priority business requirements. These include the transition to Post-Quantum Cryptography (PQC).

New encryption protocols affecting the X9 community will be issued by the National Institute of Standards (NIST) and finalized in 2024, with a timetable for implementation dependent on the specific application. Several United States Government (USG) National Security Memos (NSM-8, NSM-10), Executive Orders (EO 14073, EO 14028), and pieces of legislation (HR 7535, “Quantum Computing Cybersecurity Preparedness Act”), as well as the National Quantum Initiative (NQI) make the requirements explicit. The USG largely relies on the private sector for both software and hardware solutions, which must comply with these mandates to do business with the USG.

The financial industry is particularly at risk from the threat posed by quantum computers and will need a long time to migrate to PQC and educate their workforce. The time frame is roughly 10-15 years. However, this migration has never been attempted before on the current scale of data networks. To address the multitude of issues and related technologies, groups like X9 produced informative studies to align the larger industry. One example is X9’s “Quantum Computing Risks to the Financial Services Industry” informative study, which attempts to demystify the problem for a broader readership. It serves as a central reference for financial companies to get a scientifically validated understanding of the core concerns without vendor and media hype related to quantum computing and quantum technologies.

These living documents typically require annual updates to reflect scientific developments and input from other standards bodies such as the International Telecommunication Union – Telecoms Standardization Sector (ITU-T). Quantum is a fast-moving field and the expected advent of cryptographically relevant quantum computers (CRQC) impacting cybersecurity has continuously drifted closer to the near horizon, which means revising original estimates. The convergence of many previously separate industries necessitates the harmonization of standards between telecoms, IT providers, app developers, and many more. These include divergent opinions across global regions. For example, Quantum Key Distribution (QKD) has been dismissed by

the National Security Agency (NSA) for use on federal systems, while it has been deployed in several countries. China has built a nationwide QKD backbone. QKD networks are at various stages of implementation in Korea, Singapore, and the European Union. The ITU-T has standards for Quantum Random Number Generators (QRNG) while NIST does not. These standards will need to be reconciled for all international transaction authorities which affect multiple standards bodies and countries.

The financial industry is not unique in the complexity of standards affecting its business processes, but it has emerged as a key contributor to specific solutions. ANSI X9 has been in a position of leadership for international banking and payments, but many of its standards are derived from bodies like NIST. Harmonizing the various international organizations across countries and industries will be challenging and has never been attempted on this scale before. The last major cryptographic transition was more than two decades ago when the internet was much smaller and the global digital economy was just emerging as the primary driver of business. The added complication of cryptocurrency and blockchains further compounds the fast approaching difficulties of implementation. International collaborations and a strong drive towards education, such as the one carried out by the CSA Quantum-Safe Security Working Group, are paramount.

References:

Quantum Computing Risks to the Financial Services Industry
https://x9.org/quantum-computing/

Executive Order 14073 National Quantum Initiative Advisory Committee (4 May 2022)
Enhancing the National Quantum Initiative Advisory Committee

NSM-10 NATIONAL SECURITY MEMORANDUM (4 May 2022)
National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems | The White House

NSM-8 NATIONAL SECURITY MEMORANDUM (19 January 2022)
Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems

HR 7535 Quantum Computing Cybersecurity Preparedness Act (18 April 2022)
Text - H.R.7535 - 117th Congress (2021-2022): Quantum Computing Cybersecurity Preparedness Act | Congress.gov | Library of Congress

Executive Order 14028 (12 May 2021) Improving the Nation's Cybersecurity
Executive Order on Improving the Nation's Cybersecurity | The White House
Executive Order 14028: Improving the Nation's Cybersecurity | GSA

National Quantum Initiative (NQI) (21 December 2018)
About the National Quantum Initiative - National Quantum Initiative

National Cybersecurity Strategy Implementation Plan (July 2023)
White House NCSIP - Strategic Objective 4 prepare for a Post Quantum future