Post Quantum Cryptography and CACI's Archon CSfC

FAQ Guide

Q: What is "quantum-resistant" (QR) or "post-quantum" (PQ) cryptography?

A: Cryptographic algorithms designed to withstand attacks from both classical and quantum computers are referred to as "quantum-resistant," "quantum-safe," or "post-quantum" cryptography. These algorithms can be implemented on current computer systems.

Q: What is the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)?

A: The CNSA 2.0 suite includes quantum-resistant algorithms approved for future use in National Security Systems. Among these, Archon is implementing the Advanced Encryption Standard (AES) with 256-bit keys as a symmetric block cipher.

Q: What policies should I follow to meet NSS algorithm requirements?

A: High-grade equipment must comply with CJCSN 65104 and CNSSAM 01-07-NSM5 guidelines. As per NSM-10 and CNSSP-11, quantum-resistant algorithms in NSS mission systems should be implemented using NIAP-validated products or following specific guidance. This typically requires modules validated by NIST's Cryptographic Module Validation Program.

Q: Why does NSA care about quantum computing today? Isn't quantum computing a long way off?

A: The timeline for developing a cryptographically relevant quantum computer (CRQC) is uncertain, but its potential to undermine current public-key algorithms poses a significant threat. Given the long lifecycles of National Security Systems (NSS), NSA must proactively establish requirements for future-proof systems. In response to advancing quantum computing research, NSA is implementing CNSA 2.0 requirements to safeguard NSS.

Q: What distinguishes Archon's PQ approach from other vendor solutions?

A: Archon's "Commercial Solutions for Classified (CSfC) gateway in a box" offers a turnkey solution that enhances mission capabilities and provides unique functions. As part of this solution, Archon Manager efficiently manages devices across environments, ensuring compliance and minimizing disruption for large enterprises. Archon's PQC key generation solution automates symmetric key and PKI certificate processes, including OTA re-keying, streamlining RFC 8784 implementation.

Q: What is the Symmetric Key Annex and RFC 8784?

A: For CSfC NSS customers protecting long-life classified information, pre-shared symmetric keys must wrap standard IPSec asymmetric keys for quantum resistance. This follows RFC 8784, which extends IKEv2 for quantum resistance using peer-shared symmetric keys. PSKs are required on both tunnels for MSC-CP, inner tunnel for MA-CP, and both tunnels for multiple red networks, using RFC 8784-compliant IKEv2.

Q: When should this be implemented?

A: NSM 10 mandates "VPN symmetric key solutions" for all National Security Systems by December 31, 2023, expanding beyond long-life data protection. For CSfC NSS, the Pre-Shared Symmetric Key Annex is the sole approved compliance method. Many NSS solution owners are currently behind schedule.

Q: Does the addition of Symmetric Keys to CSfC make it as complex as HAIPE and Type 1 devices, given COMSEC key handling rules like CNSSI 4005?

A: Archon's PQC key generation solution enhances Archon Manager's automated certificate and patch capabilities with quantum-resistant symmetric keys, maintaining Two-person Integrity Role-Based Controls. It offers quantum protection and compliance without administrative complexity. Upgrading existing Archon Manager installations requires only an update, a key generation server, and an isolated subnet for server protection.

Visit our website **www.caci.com/archon** or contact us via e-mail at **Archon_Sales@caci.com** to schedule a discussion for your post quantum strategy and learn how CACI can help your journey.

CACI
EVER VIGILANT

EXPERTISE and **TECHNOLOGY**
for National Security

At CACI International Inc (NYSE: CACI), our 25,000 talented and dynamic employees are ever vigilant in delivering distinctive expertise and differentiated technology to meet our customers' greatest challenges in national security. We are a company of good character, relentless innovation, and long-standing excellence. Our culture drives our success and earns us recognition as a *Fortune* World's Most Admired Company. CACI is a member of the *Fortune* 1000 Largest Companies, the Russell 1000 Index, and the S&P MidCap 400 Index. For more information, visit us at www.caci.com.

Worldwide Headquarters
12021 Sunset Hills Road, Reston, VA 20190
703-841-7800

Visit our website at:
caci.com

Find Career Opportunities at:
careers.caci.com

Connect with us through social media: