



Orchestrated Crypto Agility

**A Critical Component
for Today's Post
Quantum Security**

Accenture Quantum Security
Guide Using Tools From QuSecure

By Tom Patterson,
Accenture Global Lead for Quantum Security
with Stephen Harper & Andrew Driscoll of the
Accenture Quantum Security Test Bed Team

Accenture's Experience Implementing Crypto Agility
in a Post-Quantum Security Test Bed with the
QuSecure software suite, QuProtect

Introduction

Leaps in quantum technology, adversarial efforts, and hybrid approaches are shortening the time to Q-Day, the day when adversaries can use quantum computing to break modern cryptography and threaten data safety for all organizations. While we cannot predict exactly when this will happen, experts typically agree that governments and companies should start implementing their post-quantum defenses now. There are proven and affordable solutions to protect sensitive data from this emerging threat, thus mitigating the substantial risk to individuals, organizations, sectors, countries, and the global economy. There are multiple approaches available for a post-quantum defense ranging from rudimentary algorithm substitution to advanced quantum physics-based quantum key distribution. Here we share possibly one of the most effective defensive approaches being deployed today—Orchestrated Crypto Agility.

Key Takeaways

01	Avoid Falling Behind 2024 will usher in the new post-quantum standards for encryption, posing an immediate risk to organizations that delay initiating a QuProtect pilot, as they risk lagging behind competitors who are already adopting solutions. Early adopters, on the other hand, can refine strategies, understand challenges, and secure trust and their market position through proactive security measures.
02	Leverage Competitive Advantages Implementing QuProtect pilots offers leadership opportunities by demonstrating crypto agility to customers, partners, and regulators, thus strengthening an organization's reputation as security-forward. It also boosts customer confidence through a clear commitment to data security, providing peace of mind.
03	Create a Quantum-Ready Strategy Tailored recommendations and resource allocation work hand in hand to identify and mitigate an organization's unique quantum security risks. By setting up a pilot for QuProtect, organizations can assess its value in mitigating risks effectively, while allocating resources towards initiatives that yield tangible security insights for actionable improvements.
04	Unlock New Revenue Streams Infrastructure providers are innovating by integrating QuProtect into their services, like offering post-quantum VPNs as an add-on, which not only caters to millions of clients but also unlocks new business opportunities and revenue streams, enhancing market advantage.

Next Steps

- 1. Start the Pilot Today** Don't wait. Launch a QuProtect pilot now and discover how orchestrated crypto agility can advance your organization.
- 2. Easier Than You Think** Setting up a pilot is straightforward and cost-effective. We help you quickly find effective solutions and tackle quantum threats for your organization and customers.
- 3. Partnering for Success** As your partner, we provide all the necessary tools to unite stakeholders, streamline the process, and highlight your leadership.
- 4. Customized Roadmap for Competitive Edge** We offer a tailored post-quantum and crypto agility migration roadmap aligned with your organization's goals, facilitating discussions with leaders and giving you an advantage over competitors entangled in complex processes.

Future quantum computers will crack today's encryption

Today's hyperconnected worlds of governments, finance, health, transportation, and defense stand on the pillar of trust that digital information is protected and can be exchanged safely around the globe. However, even as cyber-attacks become more sophisticated and the security landscape more difficult to navigate, a new and more foreboding threat has appeared: quantum computers that have the potential to break today's most widely used cryptography. Quantum computers will certainly bring many benefits to society but conversely, also pose a serious threat to today's digital security due to their ability to quickly factor large numbers into their primes, which obviates the underlying math (and therefore effectiveness) used in today's public key encryption.

How immediate is this threat? 2023 alone has seen reports of a group of scientists claiming that RSA encryption (the public-key cryptosystem widely used for secure data transmission) could be broken using a quantum computer with only 372 qubits, a task that experts estimate classical computers would never be able to solve. Separately there were breakthroughs reported in room-temperature superconducting that would have dramatically shortened the time toward large scale quantum computers. After a few days of global tension which left all companies feeling vulnerable and unprotected, both of these claims were disproved by international bodies. Despite the specific flaws, these incidents highlighted both the international race as well as new ways to use early-stage quantum computers for decryption, thereby emphasizing the urgency to get ready.

Ten Board Level Questions

Boards need to ask, and executives need to be prepared to answer.

1. Is quantum computing real?
2. Does quantum computing and security matter to us?
3. When will an adversary have a cryptographically relevant quantum computer (CRQC)?
4. How much will it cost us to be quantum secure?
5. What are the laws and regulations for quantum security?
6. What are our peers doing with quantum security?
7. When should we start?
8. How should we start?
9. What partners should we use?
10. What architecture should we go forward with for quantum security?

Asking these questions is a great way to start the process of defining the protection you want your business to have when Q Day comes (the day that a cryptographically-relevant quantum computer exists) The capabilities that could be needed are referred to as post-quantum security technologies, because they are meant to advance security beyond the threat that quantum computing creates.

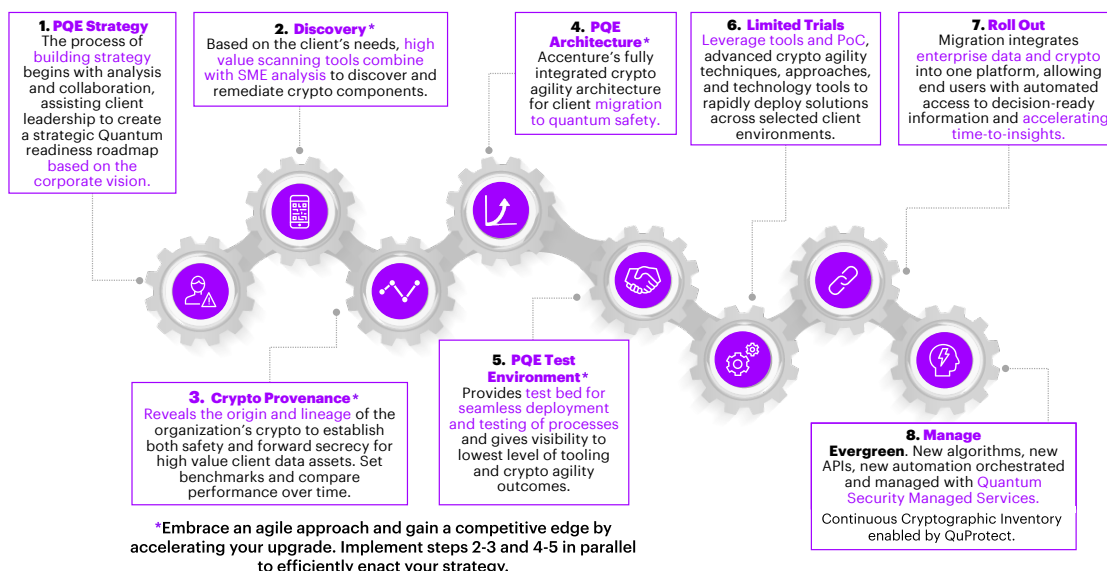
Answering these questions for your specific enterprise will take some time. Generally, it should be appropriate to start with a short workshop that combines your technical and business leadership with experienced post-quantum experts. This provides the opportunity to match business operations with quantum approaches. Answering the first few questions as a leadership team enables the clarity and consensus needed to complete the rest of the questions that may result in a road map for success.

Before we go further, a quick word on the root of the post-quantum security problem—Factoring

1. Quantum computers are built on quantum bits or qubits instead of the digital bits in classical computers, and these qubits have special quantum physics properties, most importantly 'superposition' and 'entanglement', which allow them to be used to process data in a completely different fashion. One of these key differences is the ability to perform 'factoring' on large numbers much more efficiently.
2. Public Key Encryption relies on it being practically impossible for a computer to identify the two large prime numbers that are the 'factors' for an even larger number. For example, Prime1 (ex 3) TIMES Prime2 (ex 5) (a math problem that any computer can do) = Shared Secret (ex 15) used for encryption. Using very large prime numbers instead of 3 and 5, factoring that big Shared Secret is impossible with classical computers, yet will be easy with coming quantum computers.
3. Enter the lattice, a different mathematical approach that does not use factoring, and therefore the introduction of a cryptographically relevant quantum computer would not affect its efficacy. Some of the new post-quantum candidate algorithms from NIST leverage this new lattice mathematical approach.

Accenture recommends Eight Steps to Quantum Defense

Quantum Security Lifecycle | Strategy Playbook



1. Set your quantum Strategy

- Assess your quantum risks and create roadmap
- Define your approach to Discover and Remediate
- Establish your quantum ecosystem

2. Plan your quantum risk Discovery

- Scanning Tools, Systems, and Strategies
- Perform cryptographic inventory
- Leveraging existing PKI & Key Encapsulation Mechanisms (KEM)

3. Create your quantum Ecosystem

- Internally
- Suppliers
- Partners/Clients

4. Choose your Architecture(s)

- PQE
- Crypto Agility
- Quantum Key Distribution (QKD)

5. Establish a Quantum Test Environment

- Functionality
- Interoperability
- Performance

6. Launch learning Trials

- Choose Applications
- Establish trial guardrails
- Monitor and Measure

7. Phase your Deployment

- Risk based roll outs
- Geographies
- Patch and upgrade coordination

8. Plug into Managed Services

- Orchestrated management
- Integrated with quantum-aware threat management.
- Evergreening for security, technology, and efficiency

Most enterprises would be doing some version of these eight steps internally, or by engaging expert help in this new field. The key is to complete these steps before adversaries have a cryptographically relevant quantum computer and when it could be much less critical in terms of time, expense, and risk. Our project experiences across multiple industries including governments, finance, energy, health, space, and more have taught us that post-quantum cryptographic upgrades require multi-year planning and execution. For each of these eight steps, **Accenture has created ‘post-quantum accelerators’ that may reduce the time, cost, and risk of completion.** We can leverage these post-quantum accelerators, from **strategic templates to vendor databases, testbeds, discovery tools, crypto agility processes, and managed services**, for all of our client engagements around the world.

The fourth of the eight steps is where you determine your post-quantum **defensive architecture**. Accenture can compare and recommend the optimum between the **three most useful approaches—Post-Quantum Encryption (PQE), Crypto Agility, and Quantum Key Distribution (QKD)**. Certain approaches provide protections at different technology layers, hence understanding the overlaps between network, application, and dataflow is critical for coverage and in depth defense.

The most recommended approach today is known as Crypto Agility. At the highest level, Crypto Agility simply **allows enterprises to change encryption algorithms as easily as they rotate encryption keys today.** This is important because of the emerging nature of the quantum threat combined with the relative ‘newness’ of the NIST candidate algorithms that continue to undergo testing, the over 40 existing candidate algorithms for encryption and digital signatures (as of July 2023), and the differences in performance and compatibility of the new algorithms versus the older ones. In the future, it would be necessary to use the most appropriate encryption algorithm for very specific combinations of risk across an enterprise, and once you’ve installed orchestrated Crypto Agility this could become an easy and automatic task going forward. In the eighth (managed service) phase of Accenture’s eight step post-quantum model, it’s even possible to link your threat intelligence feeds directly to your orchestrated Crypto Agility controls, making almost seamless and near real-time adjustments to hazard threats.

Crypto Agility: Architecture and Policy

Understanding Crypto Agility as an Architecture - A More Technical Deep Dive.

Let's start with a definition of Crypto Agility. We can broadly define cryptographic agility as the ability of a cryptographic protocol, application, or service to upgrade or swap out vulnerable cryptography with minimal disruption. Another definition might be the ability to see and change crypto across your ecosystem. But there is yet another way of viewing Crypto Agility. Thinking about it more specifically as is done in Internet RFC 8784, cryptographic agility can be viewed as three distinct types of agility, each corresponding to a different component of the cryptography stack which might be vulnerable:



1. Algorithm agility



2. Protocol agility



3. Implementation agility

Algorithm agility refers to the ability to swap out a vulnerable algorithm within a system with minimal disruption. For example, a system which has algorithmic agility could easily swap out a weak symmetric cipher such as RC4 with AES or an insecure hash function such as MD5 with SHA-2. Protocol agility means the ability to upgrade from a vulnerable protocol version, e.g. migrating from TLS 1.1 to TLS 1.2/3. Lastly, implementation agility means quickly patching vulnerable algorithm implementations.

The **benefits of Crypto Agility** are clear: agility allows future-proofing systems against novel cryptanalysis, evolving adversaries, and implementation errors. In particular, agility implies a shorter deprecation period, which relates to the time between when (1) somebody demonstrates a vulnerability in an algorithm, protocol, or implementation, and when (2) all applications and services which use the vulnerable cryptography are patched or upgraded. While vital for post-quantum security, even beyond security Crypto Agility allows for more efficient algorithms and implementations.

Crypto Agility Policy

A cryptographic policy can be defined as any organizational policy related to the use of cryptography. Such a policy might specify permissible algorithms, libraries, protocols, key sizes, key rotation strategies, key storage options, entropy sources, or random number generators for any given application of cryptography. A cryptographic policy is usually specified by the CIO, CTO and/or CISO in a document and then implemented by an IT team.

An organization's cryptographic policy (if one exists) may be governed at larger companies by a cryptography board, and is typically informed by relevant regulations and compliance frameworks. Examples include Federal Information Processing Standards (FIPS) 140-2/140-3, NIST Special Publication 800-53, the General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and System and Organization Controls (SOC). Each of these examples includes guidelines for protecting data-in-transit, with varying levels of specificity. For example, PCI DSS requires "strong cryptography," which it defines in terms of algorithms and key sizes, and refers to the NIST standards for specific guidance. The most comprehensive standard is FIPS 140-2/3, which specifies compliant algorithms and parameters for symmetric encryption, asymmetric encryption, key exchange, hash functions, random number generators, and entropy sources.

Regulations, standards and laws are likely to lag Crypto Agility implementations, and thus it is advisable to drive specific implementation policies based on best practices across peer groups as well as available technical capabilities. **Orchestration, integration, and linkages** to evolving standards and eco-system products and roadmaps are key considerations in building a Crypto Agility policy.

Policy During the Post Quantum Cryptography (PQC) Migration

The ongoing **NIST PQC Standardization Process** also underscores a critical need for algorithmic and implementation agility. As a study by the European Union Agency for Cybersecurity (ENISA) report summarizes, “almost all of the post- quantum cryptosystems submitted to NIST have lower security against the best attacks known today than against the best attacks that were known in 2017”. New cryptanalysis, side channel attacks, and software bugs have prompted sub-mission teams to respond with algorithm tweaks, larger key sizes, and software patches. In several dramatic cases, researchers completely compromised a candidate algorithm.

In the third round of the NIST process, researchers found a catastrophic key recovery attack against the GeMSS digital signature scheme. In the fourth round, a research team found a catastrophic key recovery attack against the KEM candidate SIKE which required only a consumer laptop to execute. To react to this shifting landscape, any PQC policy should allow for the rapid restoration of secure communications by supporting the ability to swap out a vulnerable algorithm, increase key sizes, or patch vulnerable implementations.

The migration to PQC, however, is not the first time we’ve had to upgrade vulnerable cryptography. Indeed, upgrades from MD5 to SHA-1, SHA-1 to SHA-2, and DES to AES are examples from past years and it’s not likely to be the last time. At a minimum, algorithms naturally become weaker over time as computing capabilities improve. Further, it is unlikely that Grover’s and Shor’s are the only cryptographically-relevant quantum algorithms. Experts may also develop more efficient post-quantum algorithms over time, just as was the case when elliptic curve cryptography overtook RSA as the dominant (pre-quantum) asymmetric primitive. Though we might not be able to anticipate what future changes will look like, we can be sure that cryptography will similarly change over time. **Therefore, we should build cryptographic systems which could adapt and evolve accordingly. In short, they must be agile.**

Policy in Practice

Despite the benefits, agility is difficult to attain. A fundamental obstacle is the decentralized, fragmented deployment model of cryptography in practice. For example, eliminating all SHA-1 TLS certificates concretely means tracking down all SHA-1 certificates on every single endpoint within your network, either manually or with one-off scripts or discovery tools. Furthermore, cryptographic algorithms are usually embedded into end applications that are hard to update edge computing devices with limited processing power. While there can be systems in place for changing cryptographic keys, implementing systems for changing cryptographic algorithms is not standard practice because of the impact changing algorithms can have on application or device performance. The result of having many current crypto polities for many devices and systems is decreased agility. Policy change processes mean longer deprecation periods during which data-in-transit is potentially vulnerable to compromise. As one conference report noted, “Algorithm elimination is a particularly notable failure in the industry as long-deprecated standards (e.g., RC4, MD5, DES) continue to be in use”. In the case of TLS, the deprecation period for vulnerable algorithms and protocol versions has historically been on the order of years.

Another obstacle to agility is that cryptography is often baked directly into secure channel protocols by means of a negotiation phase. For example, both TLS and IPsec—or, more precisely, the Internet Key Exchange (IKE), which is a component of IPsec—include a cipher suite negotiation phase.

The story for protocol agility is similar; the two parties typically settle on a mutually supported protocol version within the same negotiation phase. Problems tend to surface with this existing approach to agility. For one, negotiation usually translates to additional round trips, adding latency and band-width issues to each handshake. Second, negotiation adds complexity to a protocol. Complexity, in turn, makes security harder to reason and can introduce vulnerabilities, especially when we consider a network adversary that can freely drop, inject, or modify protocol messages. Indeed, the class of downgrade attacks refers to an active network adversary (also known as a man-in-the-middle (MITM)) attacking a protocol negotiation phase in a way which results in the subsequent secure channel or key exchange using weakened or no encryption.

Parallels with Software Defined Networking (SDN)

It is useful to draw comparisons between the current cryptography ecosystem with the computer networking ecosystem before the development of software-defined networking (SDN). Managing a traditional IP network is a complex, time-intensive, error-prone process that involves manually configuring switches, routers, and middleboxes using vendor-specific command-line or network interfaces. As one data point, consider that the migration from IPv4 to IPv6 has been in progress for over a decade.

The same concepts apply to managing cryptography with organization. Cryptography-related tasks such as setting up and managing an enterprise PKI or configuring IPsec peers are similarly complex, time-intensive, and error-prone and involve learning library- or application- specific configurations to properly deploy. This highly decentralized deployment makes the migration to PQC similar in many respects to the migration to IPv6, and points to the advantages of PQC orchestration just as we've gained advantages from SDN.

The insight of SDN is to decouple various layers of the networking stack: An important consequence of the software-defined networking principles is the separation of concerns introduced between the definition of network policies, their implementation in switching hardware, and the routing of traffic. These three layers map to an application plane, a control plane, and a data plane, respectively. The data plane consists of network devices (physical or virtualized) such as switches and routers which are responsible for the actual forwarding of data packets through a network. On the other hand, the control plane consists of a (logically) centralized SDN controller and application programming interfaces (APIs) to control the behavior of the data plane elements. Network applications in the application plane such as load balancers can then make use of the interface exposed by the SDN controller to define the routing policy without any knowledge of the underlying hardware devices or any vendor-specific management tool. In other words, network applications can work at the level of network policy.

In this same light as SDN, Accenture uses a technology solution from QuSecure which decouples the definition of cryptographic policy, the implementation of that policy, and the actual encryption of traffic. These three layers correspond to the management plane, control plane, and data plane. Just as an SDN controller presents an abstracted view of the network, QuSecure's QuOrchestrator (Quark) product allows us to present an abstracted view of the cryptography which secures a network. An administrative dashboard in the management plane interfaces with Quark to provide a single pane-of-glass to view and manage cryptography deployment. In particular, the dashboard works at the level of cryptographic policy. Under the hood, the control plane ensures this policy is executed by configuring applications in the data plane which encrypt data and execute secure channel protocols.

Cryptographic Orchestration in the Accenture Quantum Security Lab, with QuSecure

Accenture has installed QuSecure's full suite of Crypto Agility software in our Quantum Test Lab, which allows us to both demonstrate orchestrated Crypto Agility in practice, as well as quickly simulate client environments to develop specific implementation plans with reduced risks, costs, and elapsed times. Since many existing enterprise cryptography ecosystems today are highly decentralized and fragmented, we are able to simulate algorithms, attacks, regulations, and policy implementations at scale. The lessons that are learnable in a proven post quantum test environment prior to designing or making changes on individual environments has demonstrated critical to successful and efficient cryptographic orchestration.

Establishing a Management Plane

The management plane level should be a user-facing dashboard. Within the dashboard, administrators can register new endpoints and manage the algorithms used by those endpoints. It is important that the dashboard support total algorithmic agility. For example, if new cryptanalysis degrades the security of Kyber512 to an unacceptable level, then an administrator should be able to upgrade all channels currently using Kyber512 to Kyber768 or Kyber1024 with the click of a button. Similarly, in the unlikely event that Kyber is shown totally broken, then administrators should be able to immediately switch all channels using Kyber to BIKE, HQC, or Classic-McEliece. In short, we can potentially reduce the deprecation period for vulnerable algorithms from months or years to minutes.

In our test lab, Accenture uses QuSecure's dashboard called QuManage to provide this control and visibility into the cryptography used to secure each communication channel. This visibility also simplifies auditing and compliance tasks for IT teams. Furthermore, failed connections are detected and pinpointed, providing in-sight for IT and security teams.

Establishing a Control Plane

Given a cryptographic policy from the management layer, it is the responsibility of the control plane to ensure that policy is enforced. Or, viewed from the other direction, the control plane exposes an interface to the management plane to manage the cryptography used to secure communications between endpoints. Accenture is able to demonstrate the viability of a PQC control plane with these requisite capabilities with QuSecure's product called Quark.

In the case of algorithmic agility, we are able to use QuSecure's Quark to configure algorithms and key sizes for the data plane elements which actually encrypt data and execute the secure channel protocols. We use a configuration protocol over an independent post-quantum secure channel. If this configuration channel is compromised, a malicious reconfiguration is an auditable event that can be detected and investigated. The control plane should then be able to automatically push updates to data plane elements for implementation agility, implementing key rotation and management policies, and setting the source of entropy for keys.

Establishing a Cryptographic Data Plane

Recall that in SDN the data plane elements are network devices such as switches and routers which are responsible for the actual forwarding of packets. In other words, the data plane is the "dumbest" layer. Applying the analogy to cryptography, we consider the data plane components as the secure channel protocols and the entities executing those protocols. Within a Quantum-Secure Layer (QSL) we have a number of data plane elements, which we detail next.

Using PQNoise Protocol Framework

To upgrade a network to post-quantum, you should develop or leverage a post-quantum secure channel protocol. To this end, we are able to leverage a PQNoise Protocol Framework as the basis for creating post-quantum secure channels. PQNoise is a post-quantum adaptation of the Noise Protocol Framework, a framework which has seen use in popular applications such as WhatsApp end-to-end encrypted messaging and the WireGuard VPN protocol. Whereas Noise uses Diffie-Hellman key exchanges as the only asymmetric primitive, PQNoise uses post-quantum key encapsulation mechanisms (KEMs).

Just as in the Noise framework, PQNoise omits any in-band negotiation of cipher suite or protocol version within a QSL protocol hand-shake. Instead, each party executes the protocol with respect to a control-plane-configured cipher suite consisting of a static KEM algorithm, an ephemeral KEM algorithm, an authenticated encryption with associated data (AEAD) (symmetric encryption) algorithm, and a cryptographic hash function. At a high-level, the static KEM is a longer-term key pair for purposes of authentication. **The use of a KEM for authentication has practical advantages** over a post-quantum digital signature scheme. On the other hand, the ephemeral KEM provides forward secrecy to connections. This property means that a future compromise of the static KEM private key may not have implications on the security of past communications.

Executing the protocol with respect to a fixed configuration avoids negotiation overhead and means security is easy to reason about: message formats are unambiguous, message sizes are deterministic, and the protocol state machine is a straight line.

Note that the PQNoise specification permits the use of two different KEMs to fill the role of static KEM and ephemeral KEM. Importantly, we can exploit this fact by using two KEMs which depend on substantially different security assumptions. This configuration provides redundancy in the case that future cryptanalysis breaks or weakens one of the two security assumptions.

Cryptographic Command and Control

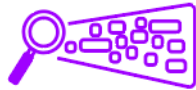
In the Accenture Quantum Test Labs, we have deployed the high-availability and scalable QuProtect crypto-agility platform from QuSecure. This all-in-one system takes organizations through every step of their crypto-agility journey in a low-risk, easy to use solution that integrates seamlessly with their current infrastructure.

1. QuProtect

QuProtect is an comprehensive software solution designed to offer classical and quantum protection for critical data, safeguarding it no matter where it's transmitted. This innovative platform secures valuable data assets against modern threats, including "store now, decrypt later" attacks, while providing enhanced control over cryptography. It lays the groundwork for protecting networks with quantum-resilient capabilities, aiming to minimize future cryptographic upgrade impacts. QuProtect offers easy cryptographic management through modular configuration, eliminating the need for system replacements or new hardware. It allows businesses to ensure quantum-resilient data transit and manage cryptographic controls, such as NIST-recommended asymmetric and symmetric key algorithms.

QuProtect provides a single platform for post-quantum cryptography PQC and ongoing cryptographic management, securing long-term data without disrupting existing systems. QuProtect revolutionizes security by implementing a service mesh architecture that off-loads security tasks from end applications and services. This innovative approach allows application developers and network administrators to concentrate on what they do best creating applications without the added burden of implementing encryption, configuring certificates, or key management. Designed for scalability, QuProtect effortlessly supports a vast range of services, from hundreds to thousands, whether they are cloud-native, micro-services-based, or traditional legacy and monolithic applications, all without any need for modifications or complete overhauls.

2. QuProtect Discovery



QuProtect Discovery enables organizations to automatically build a standardized cryptographic inventory (CBOM) from real-time network traffic, aligning with the CycloneDX SBOM/CBOM specification. Using data from existing or net-new sensors deployed at strategic network points, QuProtect Discovery captures cryptographic metadata including certificates, protocols, and algorithms with traceable evidence for audit and remediation. Organizations can then use this inventory to prioritize their assets for remediation with custom policy enforcement (e.g., approved certificate authorities) and enable interoperability with other CBOM tools.

3. QuProtect Web App Security



QuProtect Web App Security seamlessly enhances communication between web servers and applications on any device - moving to post-quantum security without impacting user experience or requiring browser modifications. Administrators can select from the latest NIST standards, as well as ensuring web application security with the option to fallback to legacy TLS ciphers if needed. QuProtect logs each session, enabling real-time tracking of the cryptography in use via the QuProtect Administrative console. This feature provides a detailed view of sessions and the browsers utilized by end users, ensuring a thorough and secure web application landscape.

4. QuProtect Network Security



QuProtect Network Security enhances the security of communication between back-end applications, with minimal impact to bandwidth and latency. This feature allows network administrators to securely transmit sensitive data across services or endpoints via the advanced quantum channels provided by QuProtect. Groups of connections can be easily edited in batch and individual connections can be granularly secured down to the port:IP level. QuProtect network enables full flexibility to manage certificates and ciphers to establish highly secure and agile mTLS connections.

5. QuProtect Core Security

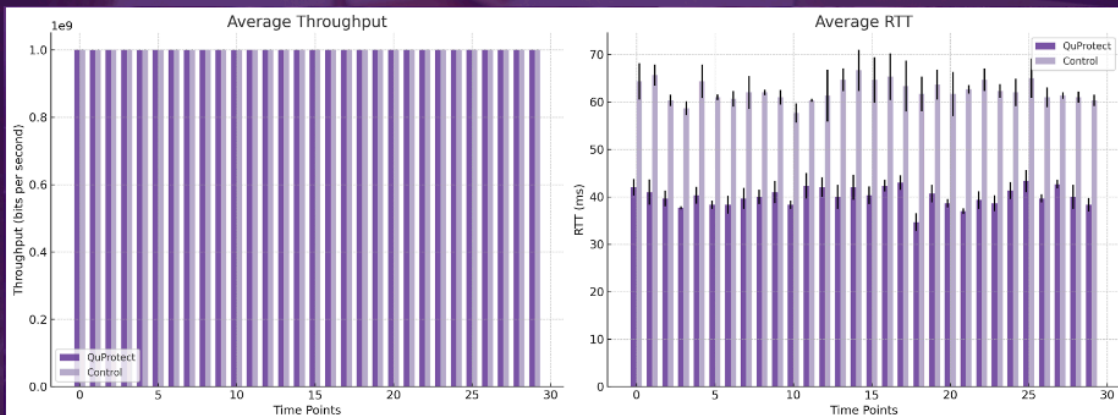


QuProtect Core Security boosts router-to-router communication security without needing hardware upgrades. Developed in partnership with Cisco, this solution secures networks' critical communications backbone with easy implementation. It combines Cisco's reliable routers and QuProtect's quantum-resistant encryption for efficient network protection.

Using Cisco's SKIP protocol for secure key distribution, QuProtect uses quantum-resistant keys based on NIST-standardized algorithms. The solution includes a Key Distribution Center and leverages the PQNoise framework end-to-end encryption framework for key transmission - enabling agile secure key exchanges for future-proof security and streamlines key management, reducing risk.

Benefit from QuProtect Without Impacting Your Network Performance Comparative Analysis of Average Throughput and Round-Trip Time (RTT)

Graph shows bars illustrating side-by-side comparison of average throughput and RTT for QuProtect and Control groups across triplicate measurements of 30 sequential time points. Measurements were made on two c6a.xl AWS instances running RHEL 8.6. Throughput is measured in bits per second, and RTT in milliseconds, with each time point reflecting the mean value derived from three independent measurements. Error bars represent the standard error of the mean (SEM), illustrating variability within the data. The dark purple bars (QuProtect) and light purple bars (Control) highlight performance differences, underscoring the minimal impact of QuProtect on network efficiency and latency.



Quantum Security can be deployed today

Even though quantum computing requires the use of highly advanced principles of quantum physics and quantum mechanics, the primary defenses against these new risks do not. PQC activities are based on existing classical computing and math principles, and fully available today. That said, there are several practical considerations for quantum security.



Budgets

- Build budget within your existing five-year plan
- Leverage existing upgrades and cloud transitions



Personnel

- Train, attract, and retain talent with specific technical experiences
- Important keywords include PKI, KEM, Encryption, Key Management, TLS



Ecosystems

- Joining ecosystems is time and labor saving, and risk-reducing
- Ecosystems forming around business sectors and geographies



Architecture

- Choosing the right post-quantum architecture for your enterprise is a critical choice, and should be carefully considered
- Following the first four steps (strategy, discovery, ecosystem, and architecture) are the recommended steps



Operations

- Changing encryption algorithms throughout your enterprise requires changes to operational cadence and tempo
- Integrating existing threat intelligence (and using one that is quantum risk aware) could make Crypto Agility operations highly efficient



Critical Infrastructure and National Security

- Many organizations are part – either directly or through a supply chain—of critical infrastructure, and therefore may be at greater risk to quantum attacks.
- Understanding your organizations role in your national Critical Infrastructure Program (CIP) with respect to quantum risk may save time and money and lower overall risk for your company, and your industry.

Conclusion: Start Now

Even as fully-published PQC standards are still being tested and hardened, companies should not wait until then to start on their quantum defense. Now that initial candidates have been released, there are established practices for businesses to follow, purchasing decisions to be made, and expertise to be developed to try to avoid future pain.

What to do then? First, build a well-considered strategy that appreciates the specifics of your enterprise, risks and stakeholders. Second, pragmatically and efficiently discover each instance of vulnerable encryption to be updated both in your enterprise and all the related ecosystems and supply chains it interacts with. Third, decide on a new crypto architecture. Fourth, begin the multi-year process of testing, implementing, and promulgating new quantum-resistant security throughout the extended enterprise.

A strong and well-thought out strategy helps businesses find the delicate balance that's needed between moving ahead and taking care to avoid introducing new risks. When deployed correctly, Crypto Agility architectures have been shown to lower risks, costs, and deployment times, and therefore are leading candidates for consideration in many organizations. Crypto Agility is available now, affordable, and it works. Setting a course for Crypto Agility allows businesses to change the encryption method as easily as they change keys today, which protects against the coming quantum threat as well as future-proofing enterprise encryption.

The time to start is now.

Glossary

API

application programming interface

CA

certificate authority

CRQC

cryptographically-relevant quantum computer

FIPS

Federal Information Processing Standards

IKE

Internet Key Exchange

IoT

Internet of Things

IPsec

Internet Protocol Security

KDC

key distribution center

KEM

key encapsulation mechanism

MITM

man-in-the-middle

NIST

National Institute of Standards and Technology

PKI

public-key infrastructure

PQC

post-quantum cryptography

PSK

pre-shared key

QRNG

quantum random number generator

QSL

Quantum-Secure Layer

SDN

software-defined networking

SSH

Secure Shell

TLS

Transport Layer Security

VPN

virtual private network

Authors

Tom Patterson

Accenture Global
Lead for Quantum
Security

tom.patterson@accenture.com

with

Stephen Harper & Andrew Driscoll

Accenture Quantum Security Test Bed

Special thanks to reviewers:

Carl Dukatz

Kellyn Beeck

Tiffini Smith

Joey Lupo

Updates on this subject can be found at

www.accenture.com/quantum

About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth and enhance citizen services creating tangible value at speed and scale. We are a talent and innovation led company with 738,000 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology with unmatched industry experience, functional expertise and global delivery capability. We are uniquely able to deliver tangible outcomes because of our broad range of services, solutions and assets across Strategy Consulting, Technology, operations, Industry X and Accenture Song. These capabilities, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients succeed and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners and communities. Visit us at www.accenture.com.

This document makes descriptive reference to trademarks that may be owned by others.

The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.

Copyright © 2023 Accenture
All rights reserved.

Accenture, its logo, and
High Performance. Delivered.
are trademarks of Accenture.