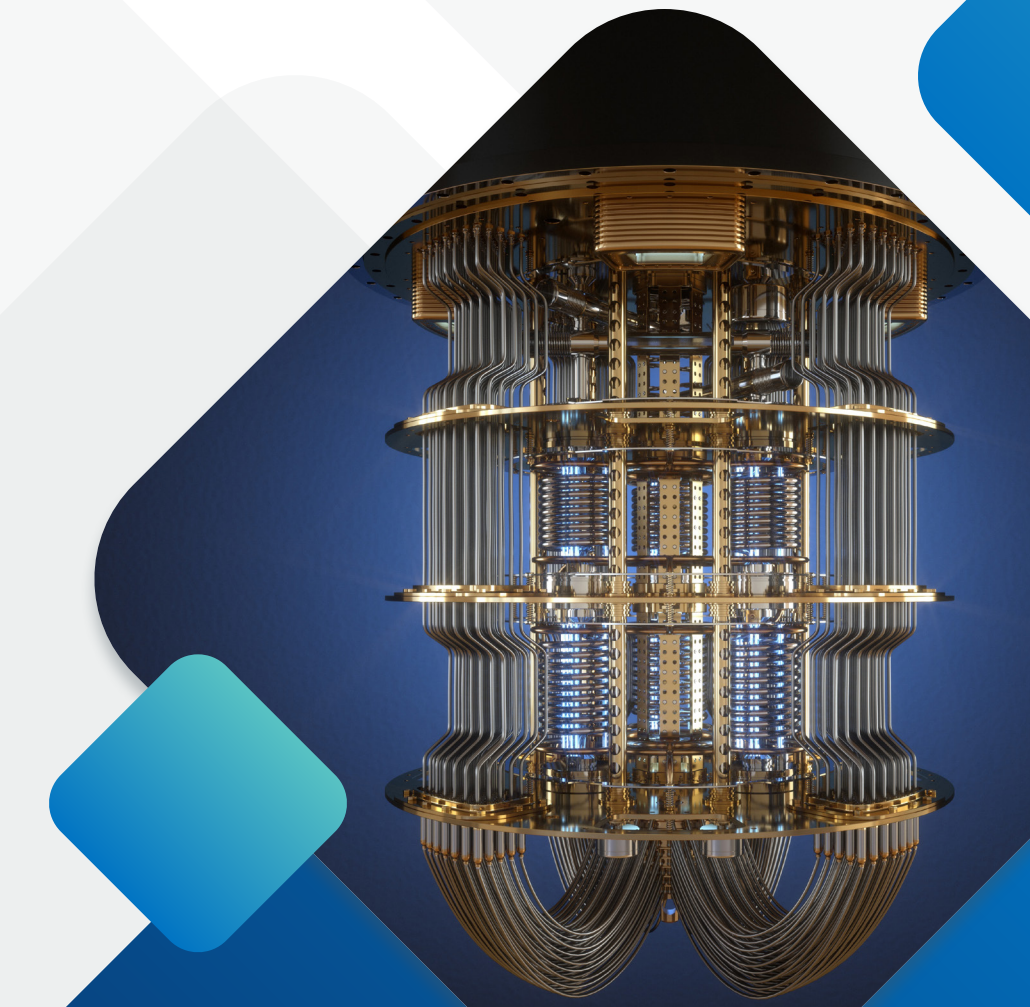
digicert®

Post-Quantum Cryptography (PQC) Maturity Model



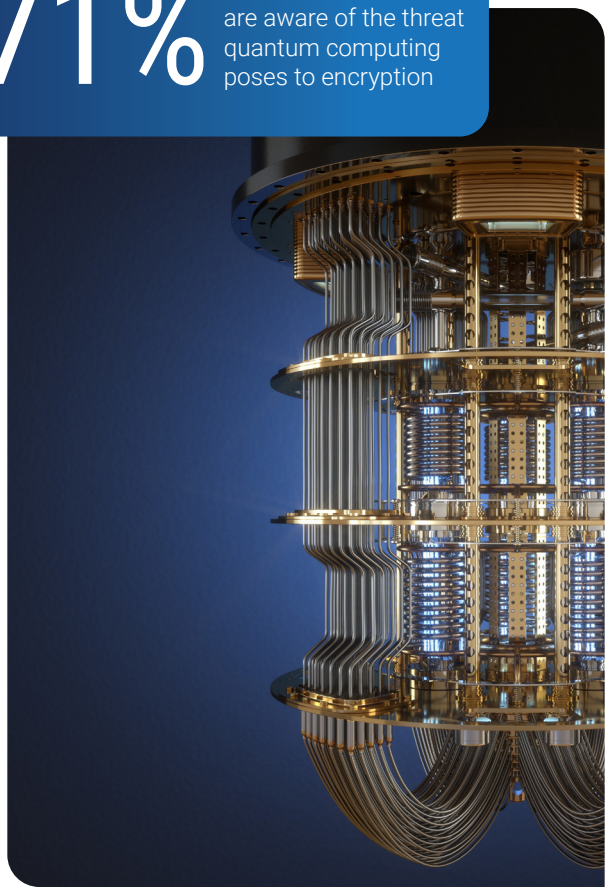
WHITE PAPER

Table of Contents

The Imminent Quantum Computing Threat

Most enterprises are aware of a formidable threat growing as a result of advancements in quantum computing. Existing encryption algorithms may be no more secure against the power of quantum computers than an unlocked door to a burglar. In a recent study[1], DigiCert found that the majority of IT professionals (71 percent) know of the threat quantum computing poses to encryption. Yet, in the same study, DigiCert found wide variation in how well organizations understand this threat, and equally wide variation in the levels of preparation. The Post-Quantum Cryptography Maturity Model is not only a guide for understanding the PQC threat, but also a tool for identifying your current level of preparation, and how you can get ahead of the challenges coming with this computing revolution. By following the model, you'll be able to advance your organization down a pathway to post-quantum security.

71% Most IT Professionals are aware of the threat quantum computing poses to encryption



Quantum vs. Encryption

In order to understand your organization's current position on the pathway to post-quantum security, it's important to understand quantum computing, and how it relates to current encryption tools.

Quantum computing represents the next evolutionary leap in computing. By combining information theory with quantum mechanics, quantum computers process massive amounts of data simultaneously, solving complex problems with endless numbers of possible answers. In essence, quantum computers sidestep linear computing processes to arrive quickly at nonlinear answers.

Our current public key encryption algorithms depend on "trapdoor" mathematical functions that are easily performed in one direction, but nearly impossible to solve in reverse. This start-to-finish mathematical process is trivial work for any computer—multiplying two prime numbers, for example. However, if the result is large enough—more than 2,048 bits—no computer can factor that number back into the two primes.

All that changes with quantum computing. While we once thought it would take a quantum computer with billions of qubits to factor such a large number, recent research shows faster solutions with fewer qubits (8 hours, 20 million qubits[2]).

This news sent shockwaves through the world of cryptography, and forced organizations to pay new attention to the coming security threat.

Maturity levels

Through research and experience, DigiCert has identified two crucial factors in measuring an organization's quantum maturity level:

- How much your organization knows about and understands the quantum computing threat.
- How much preparation your organization is doing to defend against the threat.

By plotting your knowledge and planning levels on the spectrum, you can identify where you sit in the process of deploying successful PQC measures.

1. 2019 DigiCert Post Quantum Crypto Survey
2. How to Factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits | Craig Godfrey at Google in Santa Barbara and Martin Ekerá at the KTH Royal Institute of Technology in Stockholm, Sweden

Overview of Maturity Levels

PQC Novice

The PQC Novice has little, if any, knowledge of the threat quantum computing poses to their organization. As a consequence, their organization is engaged in little, if any, preparation for combating quantum computing attacks.

PQC Apprentice

The PQC Apprentice understands the need to start preparing for the upcoming quantum computing threat. This professional is aware that encryption across their entire network is the foundation of quantum-safe security practices. More, the Apprentice understands their organization's use of HSMs and the role they play in encryption practices.

PQC Practitioner

The PQC Practitioner has begun work on combating quantum security threats. They understand their organization's level of risk, and they've put in place tools to protect their encryption. They have consolidated their certificates onto a single management platform to optimize visibility and control over all their organization's assets. In addition, the PQC Practitioner has taken the first steps toward creating a comprehensive strategy that not only secures their network against quantum threats today, but in the future, too. It's at this level of knowledge and preparation that we see organizations testing the viability of post-quantum cryptographic certificates.

PQC Master

The PQC Master has thoroughly documented their organization's policies and standards around the use of encryption, understands crypto-agility and how to correctly utilize it, and has a platform in place that employs automation to keep a current inventory of all digital certificates with full visibility and control over their entire encryption infrastructure. The PQC Master actively searches for new ways to test and deploy post-quantum cryptography within their network, so deployment into production doesn't disrupt or damage critical systems and applications. As a result of knowledge and preparation, the PQC Master anticipates security needs, and is also ready to solve problems before they become a threat to security.

Avoiding the dangers of imbalance

Knowledge without practice, and practice without knowledge can both pose just as much a threat to your encryption as an outside attacker. All IT professionals should avoid falling into either of the following categories.

PQC Academic

The PQC Academic holds deep knowledge of the upcoming quantum computing threat but hasn't yet engaged in any meaningful preparations.

PQC Maverick

The PQC Maverick may have no more knowledge than the Novice, but they've begun preparing and deploying unproven or poorly designed security measures.

Overview of PQC Maturity Levels

PQC Novice

The PQC Novice has little, if any, knowledge of the threat quantum computing poses to their organization. As a consequence, their organization is engaged in little, if any, preparation for combating quantum computing attacks. The apprentice may be working within their organization to begin preparations, but they don't have a plan for the implementation of PQC security measures.

PQC Novice Risks

The coming threat

Being a PQC Novice puts your organization at great risk. In a recent study, DigiCert found that the majority of IT professionals believe quantum computing will become a somewhat large to extremely large threat. Median estimates suggest this threat will manifest as soon as 2022. That leaves little time for the PQC Novice to develop the knowledge and planning necessary for protecting their organization from quantum attacks.

Knowledge is power

Even the move from PQC Novice to Apprentice significantly reduces the security risk to your organization. By learning enough to understand the quantum computing threat, you'll be able to start thinking in new ways about your organization's security infrastructure. You'll have the knowledge you need to move forward with the adoption of a digital certificate management platform with automated features, giving you consistent visibility and control over your entire encryption environment.

PQC Novice Education

The PQC Novice should begin by developing their fundamental knowledge of encryption. Solid encryption across your organization's network is the foundation of quantum-safe security practices. Start here:

Certificates and Cert Management

What is AOSSL, and why does it matter?

Always-on SSL (AOSSL) is the de-facto best practice for applying encryption across all your websites. When correctly deployed, AOSSL ensures all internal and external webpages are encrypted, reducing your exposure to cyberattacks. AOSSL should be applied not only to all internal webpages, but also to any thirdparty integrations for an improved overall security posture.

When deployed through a capable encryption management platform, you'll be able to view and control your entire AOSSL security environment, giving you complete oversight of your organization's threat protection.

How does Always-on SSL work with quantum security?

HTTPS best practices require correctly installed encryption across all webpages (internal and external) and machine-to-machine. With confident AOSSL in place, you'll be positioned to update your encryption for the future of quantum threats.

What's so important about a management platform?

Many PQC Novices don't realize the security measures they've deployed don't cover their entire organization's digital existence. One of the first steps in preparing for the quantum threat is understanding your organization's encryption (digital certificate) practices. A capable encryption management platform gives you full visibility over all your networks, and the adoption of a platform is critical to assessing risks and fixing gaps.

Your encryption management should be able to provide:

Reporting. Comprehensive reporting lets you see what's currently encrypted while ensuring those encryptions are correctly configured (communications protected, code and documents signed, etc.) and updated.

Full visibility. Complete visibility of your organization's network and connected devices is the only way to identify holes in your encryption. You can't fix what you can't see.

Certificate automation. Knowing which certificates are automated and which are not is vital to optimizing your infrastructure. Consistent use can save time and prevent gaps due to outdated or expired certificates.

Hardware Security Modules

Identifying custom key generation implementations

It's important to determine if your organization uses Hardware Security Modules (HSMs) for custom key generation, and how those HSMs are used. You can contact your HSM provider to find out if your organization's HSMs are capable of upgrade to quantum-safe encryption. You'll also want to verify the timeline for those upgrades. Be sure the HSM updates and practices align with your organization's timeline and plans for deployment of quantum security. DigiCert recommends industry leaders Gemalto and Utimaco for the best in quantum-safe HSMs.

PQC Novice Engagement

As your knowledge grows, it's important to engage in certain tasks, in order to move from PQC Novice to PQC Apprentice. This checklist will help you work toward protecting your organization from quantum computing threats.

- Make an effort to understand how encryption across your entire network is the foundation of best practices in security. Get a sense of your entire network, so you can see the scope of your encryption needs as you move to add quantum-safe protection to your security measures.

- Document your organization's encryption (digital certificate) practices, and determine the capabilities of your certificate management platform. Assess risks and gaps. Where are you vulnerable? Make sure your platform can provide these capabilities:

  Reporting: certificate, deployed location, lifecycle, and type.

  Certificate discovery: network-wide scans of all devices and domains for all digital certificates in use, regardless of CA.

  Automation: implementation of certificate automation throughout your network for the prevention of outages and gaps in your encryption.

  Visibility: the ability to view encryption holes (lack of certificates) in your network.

- Identify your organization's use of HSMs, and how those HSMs fit into your encryption practices. Determine who provides your HSMs and find out whether they'll offer a quantum security solution in alignment with your deployment timeline.

PQC Apprentice

The PQC Apprentice understands the need to start preparing for the impending quantum computing threat.

This professional is aware that encryption across their organization's entire network is the foundation of quantum-safe security practices. They understand AOSSL, and the importance of a capable management platform. The PQC Apprentice also understands their organization's use of HSMs and the role they play in internal encryption processes.

By replacing outmoded and risky management spreadsheets with a modern certificate management platform, the PQC Apprentice has full visibility and control over certificate issuance, renewal, and revocation. This professional can quickly respond to threats as they arise.

PQC Apprentice Risks

Today's security is tomorrow's threat

The PQC Apprentice has built a solid foundation for today's threats to their organization's security, but they haven't begun assessing what comes next. Even the most secure networks may be vulnerable to quantum computing threats. To move from PQC Apprentice to PQC Practitioner, this professional must develop an understanding of crypto-agility—the readiness for changing out existing cryptography in favor of safer PQC algorithms.

PQC Apprentice Education

What is crypto-agility?

In order to move from PQC Apprentice to Practitioner, this professional must learn crypto-agility. Both what it is, and what it is not.

Crypto-agility focuses on visibility and dynamic movement. It is awareness of every place encryption is used within your organization (like protocols, libraries, algorithms and certificates). It is also an understanding of how these encryption technologies are deployed, and the ability to quickly identify and remediate issues when they arise. True crypto-agility means possessing the capabilities necessary for seamlessly replacing outdated crypto via automation when the time comes. Crypto-agility is not the ability to use different algorithms for critical functions (like hashing, signing, or encrypting). It's also not the ability to choose which algorithm to use for a particular function (like SHA-1 or SHA-256).

Enemies in disguise

In addition to developing crypto-agility, the PQC Apprentice must understand the potential for threats from seemingly friendly sources. No amount of quantum proofing will protect your organization if data and information are shared with companies or entities that are unsecured against quantum attacks.

To move from PQC Apprentice to PQC Practitioner, you'll need to evaluate how vendors, partners and third parties introduce vulnerability to the organization. Make sure you're in communication with your third-party providers and discussing how they plan to test and secure against quantum threats.

PQC Apprentice Engagement

As a PQC Apprentice, you have a solid understanding of the impending quantum threat. Now it's time to deepen your knowledge and develop a plan. This checklist will help you work toward protecting your organization from quantum computing threats.

- Read "How to Improve your Organization's Crypto-Agility" and begin developing a plan based on the recommendations.

  Crypto-agility starts with modern hybrid SSL/TLS (RSA/ECC). The next generation of crypto-agility will be hybrid SSL/TLS (RSA/ECC/PQC). It's important to keep up with advancing information in the industry. Incorporate trusted sources into your plan as new information emerges.

- Build a list of third-party vendors. Document their security: which have fully encrypted networks and which don't.

  Your organization is only as secure as your most vulnerable third-party vendor.

- Know who is creating the next generation of cryptography.
  a) ISARA - https://www.isara.com/crypto-agility-quantum-safe

- b) Microsoft - https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/

PQC Practitioner

The PQC Practitioner understands their organization's level of risk, and they've put in place tools to protect their encryption. They have consolidated their certificates onto a single management platform to optimize visibility and control over all their organization's assets. In addition, the PQC Practitioner has taken the first steps toward creating a comprehensive strategy that not only secures their network against quantum threats today, but in the future, too.

PQC Practitioner Risks

Testing is proof

Developing and launching a testing strategy is just as important as PQC protection itself. Until you know what your system can defend against, your organization is open to risk.

As a PQC Practitioner, you may feel ready to begin testing. With a fair amount of quantum computing knowledge, and a plan in place, the next logical step is pitting your security measures against possible threats. But where should you begin? And what options are available, despite the fact that there's no current PQC standard?

PQC Practitioner Education

Working with hybrid in a testing environment

With your skills in crypto-agility, you already have a sense of the scope and configuration of your organization's systems. The next step in your education is understanding how to incorporate testing technologies into your security practices using hybrid RSA/PQC. Both ISARA and DigiCert offer PQC test kits that include everything you'll need to create and test hybrid TLS certificates.

Hybrid TLS certificates use a post-quantum cryptographic algorithm paired with a classical encryption algorithm, so you'll be able to test the viability of deploying post-quantum hybrid TLS certs while maintaining backwards compatibility. By building and testing in a sandbox environment, you'll gain experience with hybrid certificates before the security of your organization is on the line. In a test environment, you can watch hybrid certs interact with current applications, and seek solutions before you deploy your live PQC security system.

Data sensitivity

One of the most challenging threats to organizations today is the theft of secure information that's vulnerable to quantum attacks. Criminals are stealing and hoarding data, even though it's currently encrypted, in anticipation of future hacking solutions with quantum technology.

It's important, as you develop your PQC knowledge and planning, to decide what organization is the most sensitive or of the highest value. This information needs to be guarded with PQC security measures, so that it's safe not only by today's encryption standards, but by tomorrow's, too. Combating this future threat is no easy task. It requires conversations with your chief information security officer, your chief technology officer, and other key players within your organization.

As you consider which of your organization's assets to protect first, think about key proprietary collections like personal client records and intellectual property. Personal client records represent a huge risk to organizations in terms of finances and damage to reputation. Intellectual property has been amongst the most attractive targets from conventional hackers over the past two decades, especially from criminals inside China and Russia, where harvesting foreign intellectual property has become an important part of national economic and security strategies.

PQC Practitioner Engagement

As a PQC Practitioner, you're ready to begin testing the security system you plan to deploy. Now it's time to test.

This checklist will help you work toward protecting your organization from quantum computing threats.

- Meet with key people inside your organization to identify which assets and information need to be protected first. Focus on protecting personal client records and intellectual property, along with recommendations from your CIO, CTO, and other knowledgeable members of your org's team. Set a goal to secure these assets in your first round of PQC deployment.
- Select a PQC test kit and learn about testing options and processes. Make a plan for building and testing a hybrid RSA/PQC digital certificate.
- Run a test of your hybrid certificates. Identify and log vulnerabilities and incompatibilities. Prepare a plan for fixing any gaps before you deploy live.

Data Breaches on average cost

$3.86 million

Likelihood of a breach recurring

Identifying a breach takes more than half a year on average

Encryption saves an average of $13 per lost/stolen record in a breach[3]

For detailed information on the cost of data breaches, look at the latest Ponemon Institute study: https://securityintelligence.com/ponemon-cost-of-a-databreach-2018/

3. Robert Hackett, Data Breaches Now Cost $4 Million on Average, https://fortune.com/2016/06/15/data-breach-cost-study-ibm/

PQC Master

The PQC Master has completed setup of all documented standards for use of encryption within their organization. This professional understands and currently incorporates crypto-agility into their practices.

They have full visibility over their entire organization's encryption, and they control all security measures with a capable platform. At this point, your knowledge and preparation makes you ready to test and deploy post-quantum cryptography across your organization's network. With testing and careful monitoring, you're able to ensure the introduction of PQC into your production networks doesn't break critical systems or applications. A true master is an eternal student and knows they must be ready to adapt, learn and knows when to return to places that can help them gain the knowledge they seek.

PQC Master Risks

The changing landscape

The only risk to the PQC Master is the unknown. Quantum computing is still in the development phase, but it's coming soon. Continual testing and monitoring will safeguard you against threats while this new technology evolves.

PQC Master Education

As a PQC Master, you need only remain agile and aware, responding to the changing landscape of quantum computing as the technology develops. These resources will help you along the way.

Conclusion

In conclusion, waiting until the late minute to start planning the transition to quantum-safe algorithms, unnecessarily puts your organization's data at risk. Taking the steps outlined in the maturity model will help make sure your organization is correctly positioned for the coming transition and ready to take advantage of the latest technologies and methods available. DigiCert is dedicated to helping our customers with each step in the journey to becoming quantum secure.

References

NIST
For the latest developments in stateful hash-based signatures
https://csrc.nist.gov/Projects/ StatefulHash-Based-Signatures

IETF
For the latest on Signature Scheme
https://datatracker.ietf.org/doc/ rfc8391/
Quantum Internet Proposed Research Group (QIRG) session

CA/B
https://cabforum.org/2018/03/08/finalminutes-for-ca-browser-forum-f2f-meetingherndon-va-7-8-march-2018/

ANSI
https://webstore.ansi.org/Standards/ASCX9/ASCX9TR502019

Risk Calculator
https://quantum.bpi.com/

ISARA
https://www.isara.com/

Microsoft Research
Post-Quantum Cryptography Project
https://www.microsoft.com/en-us/research/project/post-quantumcryptography/

For more information on Post-Quantum Encryption, please visit our ongoing blog series, or if you have a specific question on how to bring quantum-safe security practices to your organization today, reach out to Tim Hollebeek at tim.hollebeek@digicert.com