Keyfactor

Prepare for the quantum leap with crypto-agility

Ready or not, the quantum era is coming. Protect your digital assets, applications, and infrastructure with crypto-agility that enables your business to adapt smoothly and stay secure.

New risks surface, algorithms evolve, and with the emergence of quantum computers, IT and security teams must be agile. However, lack of visibility, legacy systems, and skills shortages will leave many organizations vulnerable. To stay ahead of the curve, IT and security leaders must prepare now for the inevitable changes ahead.

Crypto-agility: the key to quantum readiness.

Quantum computers will one day be capable of cracking traditional cryptography, like RSA and ECC, which we rely on to secure data, applications, and virtually every digital asset. But whether quantum computers pose a practical threat tomorrow or in ten years, NIST, ETSI, and other industry leaders say the time to prepare is now.

Think about the transition from gas to electric vehicles. Quantum-resistant algorithms are like a new, better fuel source to protect data. To take advantage, businesses will need to upgrade their "digital vehicles" – servers, devices, applications, and cloud workloads to be compatible.

More importantly, the entire ecosystem that supports modern digital infrastructure must change too. PKI, HSMs, and certificate management systems are the digital equivalent of charging networks, power stations, and production lines. All of it must change to support this new, safer, and more secure fuel source. The reality is that this will take time; the industry simply can't afford to wait for the post-quantum era.

Keyfactor solutions:

Certificate discovery

Becoming crypto-agile starts with knowing what you have. Establish enterprise-wide visibility of all machine identities and certificates to identify unknown and vulnerable assets across your business.

Quantum-ready PKI and signing

New algorithms will introduce new challenges for performance, compatibility, and scale. Start testing today by leveraging the only PKI and signing solutions that offer built-in support to test hybrid and post-quantum certificates out of the box.

Lifecycle automation

As new algorithms become standardized, the race to migrate to production begins. Implement automated processes, such as certificate renewal and provisioning, to ensure your organization is ready for a smooth transition.

4 critical steps to establish crypto-agility

This isn't the world's first shift to new cryptographic standards, and it certainly won't be the last. Many organizations took years to transition from SHA-1 to SHA-2, and the shift to post-quantum algorithms is on an entirely different scale. That's why crypto-agility is so critical.

01 Establish visibility

Most businesses are unaware of the scope of the problem. To start the path to quantum readiness, it's on IT and security teams to build an inventory of all the systems and applications that rely on cryptography, including certificates and algorithms.

02 Identify risks and priorities

The next step is to prioritize systems and applications based on their criticality to start swapping out encryption algorithms. The place to start is with critical data that can be harvested now and later decrypted by a future quantum computer, or digital signatures that are trusted for a long time, such as firmware on long-lived IoT devices, roots of trust, and so on.

03 Upgrade, upskill, and test

NIST selected the first four quantum-resistant algorithms, each with its own unique implementation. As we move toward standardization in 2024, software vendors, hardware providers, and enterprise IT organizations should start exploring how to incorporate these algorithms into their products and systems now, as it will take serious effort, upgrades, and new skills to implement them.

04 Enable automation and migration

Being ready to make swift changes to cryptography is the new norm; the key is to make the transition as smooth as possible. That's where automation can help. By automating processes, such as replacing a certificate with one issued from a PKI that supports quantum-resistant algorithms, it's possible to swap encryption at scale and without disruption. That's crypto-agility.

By 2029, Gartner predicts that advances in quantum computing will render conventional asymmetric cryptography unsafe to use.

The Solution:

Achieving crypto-agility and quantum readiness with Keyfactor

Cryptographic APIs

Implementors of cryptographic libraries and security software must begin integrating new algorithms into their products now. The Bouncy Castle APIs in both Java and C# allow teams to implement PQC algorithms in their products today, with support services and expertise available directly from the developers.

Bouncy Castle with Keyfactor

Learn more ↗

End-to-end visibility and automation

Getting quantum-ready starts with visibility. Establish an enterprise-wide inventory of all certificate authorities (CAs) and machine identities with Keyfactor Command. Easily identify algorithms in use and define policies and automated workflows to prepare for a smooth transition to PQC algorithms in the future.

Keyfactor Command

Learn more ↗

Quantum-ready PKI

The transition to quantum-resistant algorithms is less about certificates, and more about how they interact with your systems and applications. Get a head start on testing and implementation with EJBCA, a modern PKI platform that delivers built-in support for quantum-resistant and hybrid certificates.

Keyfactor EJBCA

Learn more ↗

Secure software updates

Patching software and firmware to make it quantum-resistant will be critical. SignServer enables product and security teams to digitally sign code and artifacts using NIST PQC algorithms. Not to mention, SignServer has the flexibility to support virtually any signing format and use case.

Keyfactor SignServer

Learn more ↗

Key benefits of crypto-agility

- Implement quantum-ready cryptographic libraries in your software and hardware products
- Gain visibility of PKI, certificates, and algorithms in use across your environment
- Migrate to a modern PKI to issue hybrid and quantum-resistant certificates for testing and migration
- Automate processes to ensure a smooth transition to PQC algorithms
- Securely update software with quantum-resistant code signing
- Integrate with a growing ecosystem of quantum-ready partners

Want more information about Keyfactor's approach to scalable crypto-agility solutions?

Learn more ↗

KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed.

For more, visit keyfactor.com or follow @keyfactor.

Contact us

- www.keyfactor.com
- +1 216 785 2946 (North America)
- +46 8 735 61 01 (Europe)