Preparing for the Quantum World With Crypto-Agility

Published 2 September 2022 - ID G00743967 - 12 min read

By Analyst(s): Mark Horvath, Brian Lowans, Joerg Fritsch

Initiatives: Security of Applications and Data; Build and Optimize Cybersecurity Programs

Failure to migrate to new quantum-safe cryptographic algorithms can leave application and data security at risk of compromise. Security and risk management leaders must prepare for “harvest now, decrypt later” attacks by merging cryptographic upkeep with DevSecOps.

Additional Perspectives

- Summary Translation: Preparing for the Quantum World With Crypto-Agility (27 September2022)

Overview

Key Findings

- Quantum computing will cause existing asymmetric encryption to weaken over the course of the decade, leading to replacement with quantum-safe cryptography.
- Most IT organizations are not aware of the type of encryption they are using — including which applications are using it, how it is used, or who makes decisions about cryptography.
- Developers are often blind to the details of cryptographic and hash function libraries and sometimes hardware security modules (HSMs) or hard-coded dependencies. This can make patching or incidence response difficult or unpredictable.
- Open-source algorithms are often viewed as safe because of their constant public exposure, but effective security reviews are rare, due to inconsistent security training of reviewers.

Recommendations

To help ensure the security of applications and data, security and risk management leaders should:

- Prepare for changes to cryptographic algorithms by building an inventory of metadata for applications that use cryptography. This will give your organization a way to scope the impact of new cryptography, determine the risk to specific applications, and prioritize incident response plans accordingly.
- Make crypto-agility a DevSecOps process, so that applications can quickly adopt new quantum-safe algorithms as they become vetted over the next decade. Gartner expects that new algorithms with better performance characteristics will appear on a continuous basis over the next few decades.
- Start your quantum crypto assessments today by creating a crypto center of excellence (CCoE) to coordinate cryptographic policy, retain valuable metadata about how algorithms are used, and provide expertise to development teams.

Strategic Planning Assumptions

By 2029, advances in quantum computing will make conventional asymmetric cryptography unsafe to use.

By 2026, advances in quantum and cloud computing will require classic symmetric algorithms to support larger key sizes.

By 2025, postquantum encryption algorithms will see more use for their secondary properties like privacy enhanced computation, than they will as replacements for existing cryptography.

Introduction

The Rivest-Shamir-Adelman (RSA) algorithm has been the software developer's workhorse for over 30 years. It has been used in almost every aspect of security — including X.509 certificates, digital signatures and blockchain-based systems, logging, and identity and access management (IAM). Unlike cryptographic hash functions, which get broken and replaced relatively often, the RSA algorithm has never had a successful core algorithmic compromise. However, key cracking is one of the small set of mathematically approachable problems that cloud computing or the new generation of commercial quantum computers are positioned to solve. Progress in quantum computing has been steady, and Gartner predicts that by 2029, quantum computing will be in a position to weaken existing systems to the point that they are considered unsafe to use cryptographically.

Gartner expects the depreciation of RSA and elliptic curve (EC) cryptography to unfold much in the way that the Secure Hash Algorithm 1 (SHA-1) digital signature algorithm was progressively weakened over time. The first theoretical attacks on SHA-1 occurred in 2005, and by 2010, replacement programs were already well underway, with NIST formally deprecating the algorithm in 2011. It should be noted as a cautionary tale that, according to Venafi, by 2017, 35% of websites still used SHA-1 despite the fact that it had been completely compromised at that point. [1] This is not a mistake we can afford to repeat.

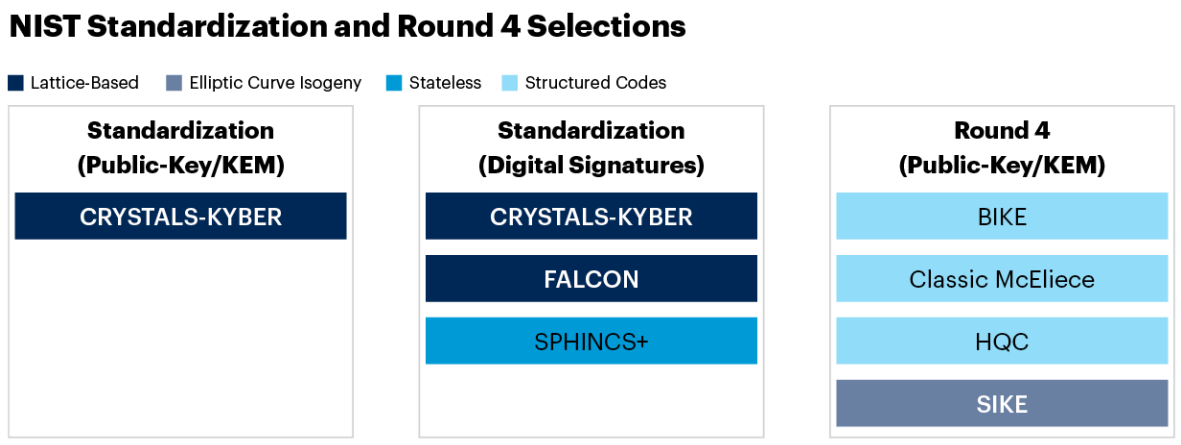
Replacement of existing algorithms has begun and is expected to accelerate in the wake of Round 4 of the NIST PQC contest. [2]

NIST identifies the following acceptable replacements:

- CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications.
- FALCON will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large.
- SPHINCS+ will also be standardized to avoid relying only on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.

Security and risk leaders may ask themselves what they should do at this point. It's too early to begin wholesale replacement, but we do want to be prepared for the changes and, where possible, use the new algorithms for new business opportunities (see Figure 1).

Figure 1: NIST Standardization and Round 4 Selections



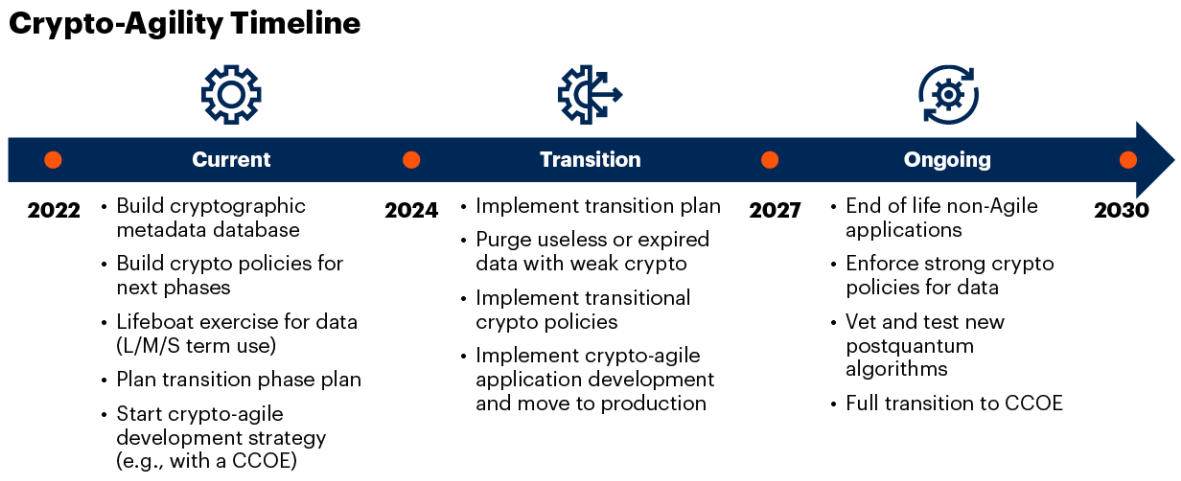
Source: Gartner
Note: the Supersignular Isogeny Key Exchange (SIKE) algorithm was rejected in June 2022.
743967_C

Gartner

Analysis

Gartner predicts that there will be three phases of activity over the next 10 years as quantum computing advances (see Figure 2).

Figure 2: Crypto-Agility Timeline



CCOE = crypto center of excellence; L/M/S = long/medium/short
Source: Gartner
743967_C

Gartner

Build an Inventory of the Cryptographic Metadata of Applications That Use Cryptography

Prepare now by:

- Creating and tracking cryptographic metadata.
- Developing or updating data retention and classification plans.
- Writing or updating cryptographic policies.
- Preparing the development organization to use new algorithms and code.
- Creating a transition plan that allows you to protect your IP and data within your resource constraints.

Building this database will help inform your transition plan to postquantum algorithms. It will help to establish policy for data security, and enable decision making around algorithm replacement. Discovering your existing use of cryptography can be a difficult process. However, many vendors in the public key infrastructure (PKI) and cryptography space have put together discovery tools that will identify all your organization's uses of cryptographic algorithms. These tools also identify inventory key lengths and list life cycle information on certificates, and store all this information as a metadata database. Generally, these vendors will also provide consulting and expertise to help you manage the items identified as technical debt. Vendors in this space include:

- Cryptosense
- Cryptomathic
- Capgemini
- DigiCert
- Entrust
- ISARA
- IBM
- InfoSec Global
- IronCore Labs

- Protiviti
- Sandbox AQ
- Senetas
- Thales
- Utimaco
- Venafi

Please note that this list is representative only and Gartner makes no endorsement of any of these vendors.

Create and Centralize Cryptographic Policies

Because cryptography has been so easy to use and reliable, only the largest, most-regulated organizations generally have a centralized policy for its use. For most organizations today, decisions are made on an ad hoc basis, by product owners, IT security, vendors or developers — with little input from experts beyond what might be needed for certain regulatory compliance.

This scattered way of looking at cryptography has allowed many breaches to take place, and facilitated numerous attacks. This has been acceptable until now because there were not any real long-term consequences beyond the occasional patch. However, with new algorithms coming soon, organizations need to put in additional effort to establish metadata around their use of cryptography, so that it can be evaluated and, if necessary, replaced. To be completely clear, one of the working assumptions that most security and risk management leaders hold about replacement cryptography isn't true. Many believe that new algorithms are simply drop-in replacements for existing cryptography, and things can be fixed through simple patching. This does not reflect reality in most cases.

> **Not one of the new postquantum algorithms is a drop-in replacement for existing cryptography.**

All of the new algorithms have completely different properties from the ones they are replacing (for example, key size, key generation, key exchange, and encryption and decryption times). Most lattice-based algorithms take longer to compute, have much larger keys, and output encrypted texts that are approximately two orders of magnitude (that is, 100 times) larger than their RSA/EC ciphertexts for the same plain texts. This means any application dependent on the speed, size or key management properties of RSA/EC algorithms will need to be reassessed for use with the NIST replacement set.

Where Appropriate, Plan to Extend Current Keys and Hashes

Given the rate of progress in quantum computing and the complexity of the move to new algorithms, it's possible (at least for the next few years) to simply extend the keys and hashes of existing applications. This is particularly true for low- or medium-risk apps. Longer key sizes in classical cryptography will offer some protection for asymmetric cryptography and hashes, and will offer good protection going forward for symmetric keys. For example, AES-256 should be robust against quantum computers available over at least the next decade or so. Longer asymmetric keys will help as well, but we expect the benefit will fade over time and could end comparatively abruptly near the end of the decade.

It's also important to keep in mind that symmetric and asymmetric use cases are very different and AES is not an appropriate substitution for almost any RSA or EC application. These principles apply beyond just software and applications. They encompass all uses of cryptography, including HSMs, smart cards, firmware, hardware and more.

Evaluate Your Data Retention Policies With the Cryptography Life Cycle in Mind

This is why a database of your cryptography metadata is a key requirement going forward. You'll need to create and manage policies around algorithm substitution, data retention and — from a development point of view — how you're going to swap out or modify your existing use of cryptography.

Given the inflation in the sizes of ciphertexts, Gartner also recommends conducting a review of your data retention and encryption policies. In most cases, it's not as simple as reencrypting everything with a new algorithm. You'll need to take the lifetime of the data into account and plan for key lengths and algorithms that match the data lifetime against the expected progress of quantum computing (see Table 1).

Table 1: Simple Table

Data Life Expectancy	Action	Long-Term Plan
Data will no longer be used by 2025	Leave as is.	End of life or reevaluate in 2025.
Data will be used in 2025, but will no longer be used by 2027	Move to larger classical keys or hashes for the transition.	Reevaluate in 2027.
Data will be used in 2027, but will no longer be used by 2030	Evaluate postquantum encryption (PQE).	Reencrypt or end of life.
Data will be used beyond 2031	Plan for PQE migration.	Complete migration before 2029.

Source: Gartner (September 2022)

Also consider perfect forward secrecy (PFS), a key agreement technique that allows the safe use of keys even after the long-term secrets are compromised.

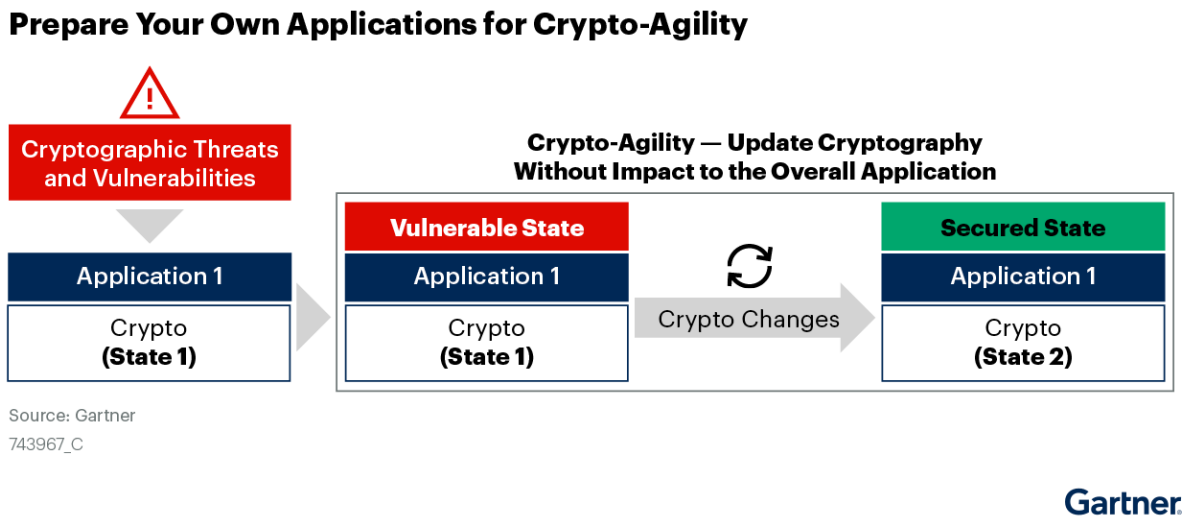
Obviously, this will vary according to your specific needs, regulatory and compliance framework and existing data-retention and privacy policies. This activity can go hand-in-hand with establishing a cryptographic center of excellence for creating and administering policies for data life cycle and cryptography.

Make Crypto-Agility a DevSecOps Process

As the industry moves into the transition phase — where current cryptography is still useful, but expiring — most organizations will want to experiment with new algorithms before full replacement. We also expect that, because the new postquantum candidates are not drop-in replacements for existing ones, quite a bit of development work will be in order. Gartner expects several new postquantum algorithm contests over the next decade or two.

One of the most effective ways to prepare for the long term, frequent change of change of cryptographic algorithms is to practice crypto-agility in your applications. Crypto-Agility is the practice of making calls to cryptography as modular as possible (see Figure 3). This allows application teams to switch quickly and efficiently between algorithms without having to massively recode the application.

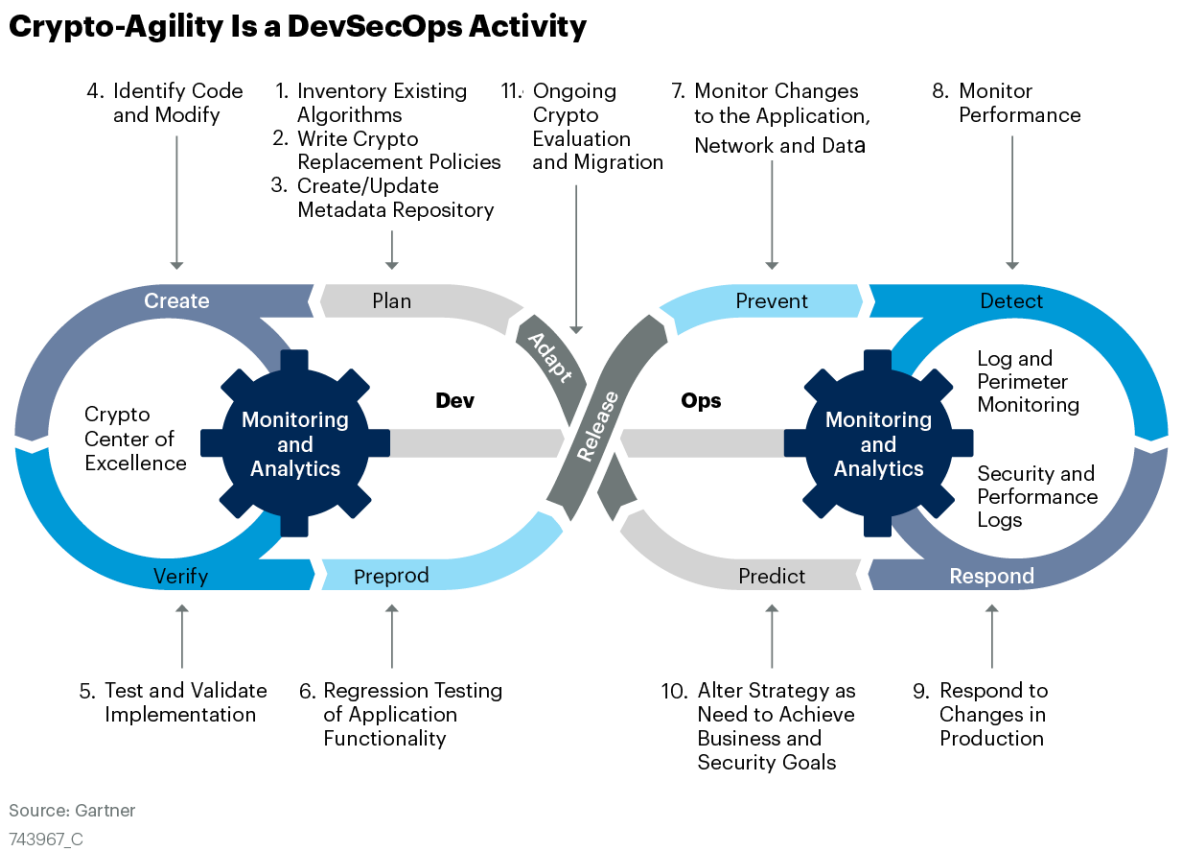
Figure 3: Prepare Your Own Applications for Crypto-Agility



Build Crypto-Agility Into Your Existing Software Development or DevSecOps Pipeline

Cryptographic changes will need to be agile for the next few decades as new algorithms, protocols and date needs change. It makes sense to begin making crypto-agility a fully fledged part of all development projects going forward.

Figure 4: Crypto-Agility is a DevSecOps Activity



Using a framework similar to the one outlined in Integrating Security Into the DevSecOps Toolchain, we can see how crypto-agility activities fit into various parts of software development. While "DevSecOps" has a specific meaning, these goals apply to any style of development — for example, waterfall or agile.

The goal is to empower developers to make changes without adding the undue burden of mastering unfamiliar cryptography and data security, while also retaining their autonomy to own their code. Most of the phases are identical to current software development best practices, but changes include:

- **Planning:** Create the metadata inventory described above, including information regarding policies, ownerships of apps and data, architectures and the overall replacement strategy. Feed this information into the existing development motion as a series of libraries, best practices and examples. This will be an ongoing activity as new cryptography evolves over the next decade, new applications and services are added, and crypto and privacy policies evolve.

- **Creation and verification:** Include new libraries and test the performance and profile of the changes. Have developers experiment with new libraries, but also watch their impact on the existing application work. Not every change will work or meet performance and storage expectations. Here, a CCoE can be extraordinarily helpful in recommending policy and providing best practices and architectures for developers to use. Usability is also critical and must be a high priority.
- **Preproduction:** Test not only the performance and stability in a near-production environment, but also the backward compatibility with existing crypto needs. Classical algorithms will continue to be in play for the foreseeable future, and remaining compatible while simultaneously pushing forward is critical.
- **Production, detection and response:** Performance, performance, performance! A/B testing is also recommended here as the changes start to go into the applications, but may not be activated for some time.
- **Predicting and adapting:** Things will not always work out and making changes to improve the application will be a critical, ongoing activity.
- **Consolidation and Control:** We see CCoEs as central points to manage policy not only for cryptography, but also for IAM, entitlements, zero-trust networks, blockchain, data security and many other policy and technical functions (see Infographic: Why You Need A Crypto Center of Excellence Now). For discussion of the IAM and machine identity issues that crypto-agility will affect, see Market Guide for Identity Governance and Administration.

Modern development organizations have become proficient at adding and adjusting to the kinds of changes that crypto-agility demands. Adapting crypto-agility and applying it within your teams should be (relatively) straightforward.

Establish a Cryptographic Center of Excellence

The most effective way to manage and control the use of cryptography is through establishing a single team that has the expertise needed to make effective policy for the organization. The CCoE can serve as a way to avoid lots of individual point decisions about security technology. While decisions like this are familiar territory for security and risk management leaders, there can be expensive, unexpected consequences if these decisions are mismanaged.

Evidence

[1] SHA-1 Deprecation, Venafi.

[2] PQC Standardization Process: Announcing Four Candidates to Be Standardized, Plus Fourth Round Candidates, NIST.

An Efficient Key Recovery Attack on SIDH (Preliminary Version) (PDF), The Cryptology ePrint Archive.

Mironov, I. and Zhang, L., Applications of SAT Solvers to Cryptanalysis of Hash Functions, ACM Digital Library.

Top 1 Million Analysis — June 2022, Scott Helme.

Document Revision History

Better Safe Than Sorry: Preparing for Crypto-Agility - 30 March 2017

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Top Strategic Technology Trends for 2022: Privacy-Enhancing Computation

Cool Vendors in Quantum Computing

Top Trends in Building a Digital Future: Next-Gen Computing

Table 1: Simple Table

Data Life Expectancy	Action	Long-Term Plan
Data will no longer be used by 2025	Leave as is.	End of life or reevaluate in 2025.
Data will be used in 2025, but will no longer be used by 2027	Move to larger classical keys or hashes for the transition.	Reevaluate in 2027.
Data will be used in 2027, but will no longer be used by 2030	Evaluate postquantum encryption (PQE).	Reencrypt or end of life.
Data will be used beyond 2031	Plan for PQE migration.	Complete migration before 2029.

Source: Gartner (September 2022)