PrimeFactors™

— Applied Data Protection —

White Paper

Thinking Beyond Post-Quantum Readiness

Building a Secure Infrastructure for Tomorrow with Crypto-Agility

Table of Contents

Introduction

Advancements in computing technology and a rapidly evolving threat landscape are compelling government and enterprise organizations to rethink their approach to how they optimize their applications to safeguard sensitive data. While much of the recent conversation on the concept of crypto-agility has focused on the ability to smoothly transition to post-quantum (PQ) resistant algorithms, crypto-agility in practice is a much broader approach to application architecture with immediate and longer-term advantages.

As such, crypto-agility as a framework that extends beyond PQ preparedness, enables organizations to address a variety of data protection needs throughout the enterprise. The objective is to deliver comprehensive data security, providing the adaptability to not only prepare the organization to transition to quantum-resistant algorithms, where appropriate, but to also seamlessly adjust the data security posture to meet new threats and vulnerabilities on the fly, without extensive changes to applications, and while addressing operational demands and regulatory requirements.

Essential Security Strategies Beyond Post-Quantum Readiness

What is Crypto-Agility?

According to Gartner®, “crypto-agility is the capability to transparently swap out encryption algorithms and related artifacts in an application, replacing them with newer, different, and presumably, safer algorithms.[1]”

However, if we think of crypto-agility in a broader sense as **data protection agility**, the concept ensures that organizations can effectively respond to evolving threats, which may include threats resulting from advancements in computing technology, as well as virtually any security, regulatory, or business demand that requires a change in how sensitive information is secured or revealed.

Why is Agility Important?

Data protection agility is critically important because change is inevitable. Not only is the threat landscape constantly changing but use cases and business requirements are always evolving. Sensitive

[1] Gartner, Hype Cycle™ for Data Security Technologies, 2025, Andrew Bales, 10 July 2025. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and HYPE CYCLE is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved.

information today is acquired, processed, and shared in ever-evolving ways that require us to rethink how we protect data as a critical business resource.

Not only are algorithms continuing to evolve, but in the wider data security context, many factors must be considered such as the datasets that we should protect and the various techniques that we might use to protect them (such as encryption, tokenization, digital signing, redaction, hashing, etc.). Should all data be revealed in the same way to all users that are authorized to access data? What if there are new reasons to secure the same data in different ways? For example, expanding and more stringent regulations that mandate not only what data needs to be protected, but also how and where data needs to be processed and stored, are driving the need to quickly adapt to change. This requires a proactive approach to cryptography with flexibility at its core. Enterprises implementing data security in their application can forecast with some certainty that change is coming, but if applications are not architected to handle this change seamlessly, things could get messy… and expensive.

Being prepared is only the tip of the iceberg. There are many more benefits beneath the surface as to why an organization would want to implement agile architecture, like operational and regulatory compliance and continuous adherence to updated security standards. Deploying agile architecture enables organizations to navigate these challenges and effectively address:

- Obsolete algorithms that must be replaced to avoid vulnerabilities.
- Operational demands that require the protection of new datasets, records, or fields.
- Changes in industry standards, such as PCI-DSS, or new regulatory pressures demanding compliance with the latest standards.

Data protection agility equips organizations with tools to address these challenges while minimizing the expense and disruption related to evolving or, in some cases, overhauling data security.

Post-Quantum Computing Driving the Need for Change

While there is certainly a myriad of practical drivers for implementing crypto-agile applications, quantum computing may be one of the best and most relevant examples of changing threats that all enterprises will need to address. As advancements in quantum computing heighten the risk of brute-force attacks, existing cryptographic algorithms become vulnerable and will need to be replaced with stronger, more resistant ciphers. In recent years, the concept of crypto-agility has become widely used across the industry in the context of PQ preparedness; however, in the three recently published Federal Information Processing Standards (FIPS) for PQ cryptography[2], crypto-agility is never specifically mentioned. The new FIPS-approved lattice-based key encapsulation, digital signature, and stateless hash-based digital signature standards provide a family of robust new algorithms to address the quantum threat.

[2] National Institute of Standards and Technology, FIPS 203, 204, and 205, Post-Quantum Cryptography Standardization Project, August 13, 2024.

We often hear vendors interchanging post-quantum readiness with crypto-agility. What they often mean is crypto-readiness – meaning that their box or service, which might already be deployed at a given enterprise, has PQ algorithms ready for consumption. However, this often involves complex application re-architecture to make use of these algorithms. True crypto-agile architectures allow for the consumption of new algorithms seamlessly.

> *"Given the increased demands for classical cryptography to achieve operational efficiencies and cost reductions (e.g., agility through policy and automation), and the coming threat of quantum computing, Gartner expects crypto-agility to be a significant differentiator for technology vendors."*
>
> — Gartner Hype Cycle for Data Security Technologies, 2025

Beyond Quantum Preparedness

Beyond a migration to new quantum-resistant algorithms, peripheral capabilities must include the wider set of mechanisms to effectively counter threats to data security. This must be done while ensuring that organizations can continue to meet operational demands within established government and industry regulatory frameworks, to deliver true data protection agility.

Organizations may have a variety of reasons why they need to implement a crypto-agile architecture. These may include performance, as well as the need for interoperability, compatibility, and adaptability of their security posture to quickly change any aspect without having to rearchitect and reintegrate changes into applications. Other reasons why organizations need the capability to change security on demand include:

- Switching over to safer, faster, or more efficient algorithms or techniques to meet performance requirements in high transaction environments.
- Incrementally securing fields as needed, based on threats and operational aspects.
- Changing tokenization techniques or different token lengths to avoid potential token repetition and collisions.
- Ensuring that cryptographic updates do not break compatibility with other systems or protocols.
- Supporting the integration of systems that use different length fields such as account numbers – a scenario typically found with merging organizations.
- Adding digital signing functionality for validation, hashing data for authentication, or changing security techniques to optimize processes and analytic functions.

- Adding security to a field or file that the organization used to be comfortable leaving in the clear given previous threat profile.

Addressing these needs ensures that organizations can achieve and maintain a robust and resilient security posture with minimal disruption in a rapidly evolving threat landscape.

A More Holistic Approach

A more holistic view of crypto-agility would entail implementing architectures, techniques, and solutions that allow for changes to how data is secured and implemented over time with little to no application re-work. Enabling organizations to quickly change any aspect of security, without complex reintegration, allows them to adapt dynamically to new threats and operational needs. By deploying solutions that deliver flexible data-centric cryptography, organizations can take control of evolving security needs and regulatory compliance requirements.

When looking for a solution, organizations should focus on those that:

- Address the security of structured and unstructured data across all applications, on-premises, in the cloud, and in hybrid environments.
- Implement centralized management of the data protection policies to help simplify the work that needs to be done to change security enforcement.
- Enforce data protection in a distributed manner to minimize system load and network dependencies.
- Apply a broad range of security techniques to address safety, performance, and regulatory needs.
- Ensure robust key management to establish the foundation of a data protection strategy.
- Support the ability to implement new security algorithms and deliver architectural approaches and security functionality that enable changes to be made quickly and easily.

> *"Furthermore, with the looming introduction of widespread quantum computing, asymmetric cryptography algorithms are no longer safe. SRM leaders should pay close attention to crypto-agility, postquantum cryptography and quantum key distribution. This includes transitioning to quantum-safe algorithms, as the urgency to replace vulnerable cryptographic algorithms will only intensify as we approach the end of the decade.*
>
> — Gartner Hype Cycle for Data Security Technologies, 2025

Designing for Crypto-Agility: Centralized Control and Decentralized Enforcement

Security Abstraction

Abstracting data security from applications means that the task of securing data is not done individually by each application. Instead, security is implemented at a higher, centralized architectural level – eliminating the need to interweave security into the applications themselves. The approach has significant advantages:

- Reduced cost and complexity
- Broad applicability
- Simplified development
- Future-proofing

By decoupling security from applications, security becomes agnostic. This enables organizations to apply consistent protection policies across their deployments, regardless of platform, technology stack, or programming language, thereby saving months of time that would be otherwise spent architecting applications as security techniques evolve and regulations change. Separation of duties does not just make it easier and faster to apply security with less expertise, but it also controls who knows the keys, algorithms, and security settings for exactly how data is being protected, further enhancing security. This translates to reduced developer burden, enabling them to focus on functionality and user experience, without needing to be experts in cryptography.

Because security policies are implemented independently of the application's codebase, this also reduces complexity and costs. Abstracting security enables organizations to quickly adopt modern technologies or replace legacy systems without having to re-engineer security measures, allowing policies to remain consistent. As a foundational approach, security abstraction, when paired with centralized policy management and decentralized enforcement, enables a strong and agile security architecture.

Design for Agility

Policy and enforcement are essential components of a sound security strategy. Policy establishes the necessary backbone to ensure that the organization's data security practices remain strong and adaptable to current and future needs. Enforcement, on the other hand, makes certain that the policies are implemented in a consistent and effective manner, without disrupting operations. Policy and enforcement are critical to:

- Define governance
- Centralize control
- Decentralize execution
- Support adaptability
- Ensure compliance

Policies establish the rules and standards for how cryptography (i.e., techniques, algorithms, key management, and access controls) are implemented across the organization. The rules ensure consistent application of security practices, reducing vulnerabilities caused by ad hoc or inconsistent implementations. For example, the policy may dictate the cryptographic technique to use if format preservation is required, the approved algorithms to use, along with their required minimum key lengths, and procedures for handling compromised keys.

Defining security governance by centrally controlling policy establishes a framework that provides a "single source of truth," enabling agile responses to changes in the threat landscape and regulatory requirements. Coupling centralized policy with a decentralized execution scheme allows granular enforcement across different use cases, while supporting consistency, scalability, and regional compliance. For example, if a vulnerability is discovered in an algorithm, policy and enforcement tools can quickly enable a transition to a safer, more robust alternative cipher across the enterprise.

Policy and enforcement are critical to achieving crypto-agility because they provide the structure and operational capability to adapt to evolving environments. Effective policy and enforcement enable organizations to deploy cryptographic changes swiftly and with minimal disruption. As data protection regulations evolve, policies define how cryptographic practices align with mandates such as PCI-DSS, GDPR, HIPAA, CCPA, DORA, or NIS2. And enforcement ensures compliance, avoiding costly penalties or reputational damage.

Centralized Policy Control

Centralized policy control refers to the framework that defines how sensitive data is protected, and how access to the data is controlled across the organization. Unlike the function being conducted independently at each application, centralization provides significant benefits:

- Unified security posture – A single repository for security policies ensures consistency across the organization. Whether it's encryption, tokenization, access controls, or monitoring, centralized policy management guarantees that all systems adhere to the same rules.
- Simplified compliance – Regulatory compliance becomes easier when policies are centrally defined and enforced. Auditors can simply review and validate the organization's adherence to regulations, reducing the risk of non-compliance and associated fines.
- Streamlined updates – In the face of evolving threats and stricter compliance requirements, centralized policy management allows for rapid updates to security protocols. Changes to security procedures can be quickly propagated across the organization, minimizing delays, and ensuring continuous protection.
- Enhanced visibility – Centralized policy control provides a singular view of the organization's security posture, enabling better monitoring, auditing, and threat analysis.

Decentralized Enforcement

While policy management offers significant advantages when centrally deployed, enforcement is most effective when decentralized. A distributed enforcement model implements security measures closer to where critical data is stored, moved, or used.

Advantages of this approach include:

- Reduced Latency – By enforcing security policies locally, organizations reduce the latency associated with sending data to a central hub for encryption or other protection mechanism. This is especially critical in real-time operations such as financial transactions.
- Scalability – A decentralized enforcement model scales naturally as the organization grows. As each endpoint enforces and executes security policies independently, this avoids bottlenecks and ensures seamless operation even in large, distributed systems.
- Resilience – Decentralized enforcement also creates redundancy. Even if the centralized policy system is offline, local enforcement mechanisms continue to protect data.

Designing an architecture that abstracts data security from the applications, with centralized security policy management and decentralized enforcement represents a paradigm shift in data protection. The approach embodies true crypto-agility, delivering a highly secure and flexible solution that not only addresses current threats but also adapts to future challenges.

Implementing Crypto-Agility: Deploying a Flexible Architecture Across Your Existing Environment

Challenges of Implementing Crypto-Agility in Existing Applications

Before diving into deployment strategies, it is important to first recognize challenges associated with implementing crypto-agility in existing applications and environments. Typical issues that need to be addressed involve:

- Legacy dependencies
- Infrastructure diversity
- Jurisdictional adaptability

Legacy dependencies often arise from systems built on outdated technologies that may depend on obsolete algorithms that cannot be quickly replaced or updated without significant disruption to operations. For example, a banking application written in COBOL built in a 32-bit operating environment might not incorporate sensitive data protection or may leverage legacy crypto-libraries interwoven into the fabric of the application to protect sensitive data. Diverse infrastructures, including legacy on-premises environments operating alongside cloud-based deployments in hybrid configurations, demand varying degrees of security capabilities. Add to this equation varying jurisdictional requirements on how and where data can be processed and stored or revealed, and the complexity associated with deploying a crypto-agile architecture becomes clear.

Best Practices

The design of a crypto-agile architecture involves adhering to core principles. When deploying a crypto-agile architecture across the enterprise, organizations should follow these best practices:

1. **Security abstraction:** Decoupling data protection functionality from applications ensures seamless updates to algorithms and data protection techniques without having to rearchitect systems. Hardcoding algorithms should be avoided; instead, applications should allow for easy upgrades to stronger, more efficient cryptographic methods. Instead of interweaving data protection functionality, which often involves integrating a crypto-library, abstracted security can be provided as a policy-driven service to applications.
2. **Centralized policy management:** By centralizing control over data protection policies, enterprises can simplify the development and upkeep of data security. Centralized policies can enforce uniform security across various applications, platforms, and datasets. This ensures compatibility, mitigates risks from operational silos, and facilitates rapid threat responses, as

centralized policies can be updated more quickly than a fractured ad-hoc approach to data protection, which is deeply prone to inconsistencies.

3. **Decentralized enforcement:** Though central policy control is important, security enforcement must be able to proliferate across the enterprise in order to maximize scalability. Enterprises cannot afford to have performance choke points that throttle overall performance. Tailored updates at the endpoint level, combined with granular access controls and monitoring, reduce insider threats, and enhance the overall security posture.

A true crypto-agile architecture enables organizations to secure sensitive data, adapt to a changing threat landscape, and remain compliant with regulatory requirements while maximizing performance and minimizing the cost and complexity of meeting these demands.

Development Roadmap

To deploy a crypto-agile architecture effectively, organizations must contemplate how both current and future security, business, and regulatory needs might require changes to how data is handled and who and what may have access during use, transit, and storage. Critical steps required to develop and execute this strategy include:

1. Asses the existing environment:

- Identify all data security mechanisms, including encryption, tokenization, hashing, redaction, digital signing, static or dynamic masking, and key management.
- Document the algorithms, key lengths, and protocols in use.
- Evaluate dependencies on specific libraries or hardware.

2. Abstract cryptographic operations:

- Implement an abstraction layer, accessible via APIs or standard program interfaces, to avoid interweaving cryptographic details within application code.
- Look for abstraction layers that incorporate not only a broad set of security functionalities, but also those that can simplify integration into third-party hardware security, if needed.

3. Adopt centralized key management:

- Keys underpin the security of cryptographic systems; integrated key management minimizes misconfigurations and ensures uniform implementation across the organization.
- Leverage automated key management for consistent robust key generation, storage, rotation, and complete lifecycle maintenance, including the ability to suspend (temporarily or permanently) cryptographic keys.
- Generate unique keys for specific operations, applications, or datasets, as may be appropriate to minimize the impact of potentially compromised keys, and regularly audit and revoke outdated keys.

4. Enable algorithm flexibility:

- Leverage security solutions that enable changes to algorithms without having to rearchitect the application code base.
- Support multiple cryptographic algorithms, protocols, and security techniques, such as redaction, random-number generation, or encryption with varying degrees of key lengths and strength to fulfill different applications and security, performance, and transitional requirements.

5. Addressing interoperability:

- Ensure backward compatibility during transitions, supporting both legacy and modern algorithms, including where appropriate new quantum-resistant ciphers following the National Institute of Standards and Technology (NIST) guidance or other updated industry standards.
- Monitor advancements in quantum-resistant algorithms and experiment with hybrid models that combine classical and quantum-resistant ciphers.
- Plan phased migrations to post-quantum solutions, starting with high-risk assets such as "long-lived" data that will remain sensitive for many years and could be collected now by an adversary in protected form and revealed in the future using PQ techniques.
- Adopt a hybrid model that allows the organizations to gradually migrate to quantum-resistant algorithms while maintaining compatibility with existing systems.

The Unique Challenge of Securing Data in Legacy Applications

The concept of implementing data protection functionality into legacy applications can be incredibly daunting, as traditional approaches tend to rely on interweaving cryptographic libraries and general data protection functionality into applications. This approach adds tremendous amounts of cost and complexity to legacy applications that were often architected with little regard to data security. Implementing solutions for protecting data in legacy applications have also traditionally required developers that were familiar with (or even experts in) cryptography and key management. Because of these challenges, many enterprises have simply opted to ignore application-level data security and implement data protection solely in storage environments. However, evolutions in industry standards, such as PCI-DSS 4.0, now require that data itself be secured, independent of its storage location, pointing s to application-level data protection.

The good news is that the very same approaches we have described here for maximizing crypto-agility can also drastically simplify securing data in applications. Instead of interweaving cryptography, applications can simply present a piece of data to a security service for transformation into its secure state. Optimally, these security services (or security services platforms) include a broad spectrum of security techniques that can leverage centralized policies to secure and reveal data at the right time for the right users to meet business objectives. When policies are updated, the application may be able to take advantage of security updates without every changing the way it requests security.

Platforms that support a multitude of interfaces, such as native APIs, command lines, batch scripts, or RESTful APIs, allow for data protection to be implemented with minimum disruption.

The Way Forward

In an era of rapid technological evolution, deploying a crypto-agile architecture has become essential for addressing today's cybersecurity challenges while preparing for the future. Deploying a crypto-agile architecture across legacy systems can be challenging and requires detailed planning and design. By carefully abstracting security functionality, adopting centralized policy management, and enforcing a decentralized execution and enforcement model, organizations can create a resilient and adaptable security foundation that goes beyond simple PQ readiness. Organizations that prioritize crypto-agility today will be better positioned to meet the demands of tomorrow. By ensuring algorithm flexibility, organizations can enhance security, reduce operational risk, and remain compliant with evolving standards.

When evaluating application-level data protection solutions of this nature, look for solution providers that include a broad range of data protection functionality that can adapt to the current and future needs of your enterprise. Look also for those that implement all their security functionality in a single code base, instead of separate system patched together. Identify solutions that can span across multiple environments, including a broad range of operating systems deployed on-premises, in the cloud, and in hybrid deployment environments, instead of those that only support specific deployment models, such as cloud-only, or SAAS only deployments, to ensure that all of your applications can address the need for crypto-agile, modern data protection and privacy. And, above all else, ask for a proof-of-concept (POC). This is where enterprises should be able to easily segregate the solutions that can simplify crypto-agile data protection from those who just have good marketing departments. The proof is in the POC.

About Prime Factors
EncryptRIGHT Data Security Platform

Prime Factors' EncryptRIGHT data protection service as a platform delivers robust, comprehensive, and adaptable data-centric cryptography allowing organizations to run their own security services for complete control over their most sensitive data. Designed with a flexible architecture, EncryptRIGHT enables organizations to secure any data (structured or unstructured), in any application, in any environment, as defined by centralized data protection policies and decentralized enforcement mechanisms.

EncryptRIGHT features include:

- Centralized data protection policy management that leverages a broad array of security techniques including encryption, tokenization, masking, hashing, digital signing, and access controls to ensure sensitive data is accessible only to authorized users.
- Algorithm diversity to enable adaptability to changing threat scenarios and regulatory requirements.
- Decentralized enforcement through the deployment of EncryptRIGHT Instances at the individual application level that synchronize and execute on the established centralized security policies.
- Robust key management to safeguard critical cryptographic keys throughout their lifecycle.
- Traceability and reporting to facilitate auditing and regulatory compliance.

Prime Factors built EncryptRIGHT to empower enterprises with the flexibility they need to stay ahead of evolving data protection and privacy challenges. To experience the benefits of EncryptRIGHT firsthand, visit Prime Factors and request your free trial.