White Paper, sponsored by DigiCert | June 2024

The Evolution of Digital Business Dictates a Modern Crypto Landscape

Jennifer Glenn
Research Director,
Security and Trust Group, IDC

Table of Contents

CLICK ANY HEADING TO NAVIGATE DIRECTLY TO THAT PAGE.

Executive Summary

Digital business is the new reality for most enterprises. In IDC's January 2024 *Future Enterprise Resiliency and Spending Survey*, **47% of respondents identified as either mostly a digital business or digital native.** One of the primary benefits of operating a business digitally is that data can be shared easily with more applications, web properties, devices, departments, and users. This enables organizations to confidently enable remote work, securely communicate across the supply chain, and create digital services and products that make customers happy.

The reality of being a digital business is that it requires a complex environment that combines multiple cloud infrastructures and digital data, as well as legacy hardware and data to keep businesses running optimally. Further, there is just more of everything: more devices talking to one another, more users accessing corporate resources remotely, and more applications running in different clouds or on premises. The volume and value of data assets are increasing exponentially. Maintaining the security and integrity of this complex environment — and protecting all these assets — is essential for business success.

Good Encryption Is Essential for Effective Security; Crypto-Agility Is Essential for Effective Encryption

There are many ways to secure data across the enterprise and its ecosystem. Encryption, in its various forms, is a common security capability for protecting the integrity of the connections and data in each of these environments. For example, encryption keeps data on devices from being viewed by unauthorized users. It protects data on public websites from being compromised. It also protects data as it is being transferred between devices for software updates or communications between the software agent and its hosts.

Organizations may use multiple encryption algorithms to obscure data, especially when the data being protected is considered confidential or sensitive. Encryption is a common and necessary component of security. In IDC's March 2024 *Data Security and Privacy Survey,* nearly 80% of respondents reported using encryption as a means for addressing privacy (see **Figure 1,** next page). The process for encrypting and decrypting information between devices and/or users requires additional technologies to confirm legitimacy and authorization.

These technologies include:

Cryptographic keys:
The generation and management of cryptographic keys, which allows the data to be encrypted and then decrypted by the intended entity (user, device, app, etc.).

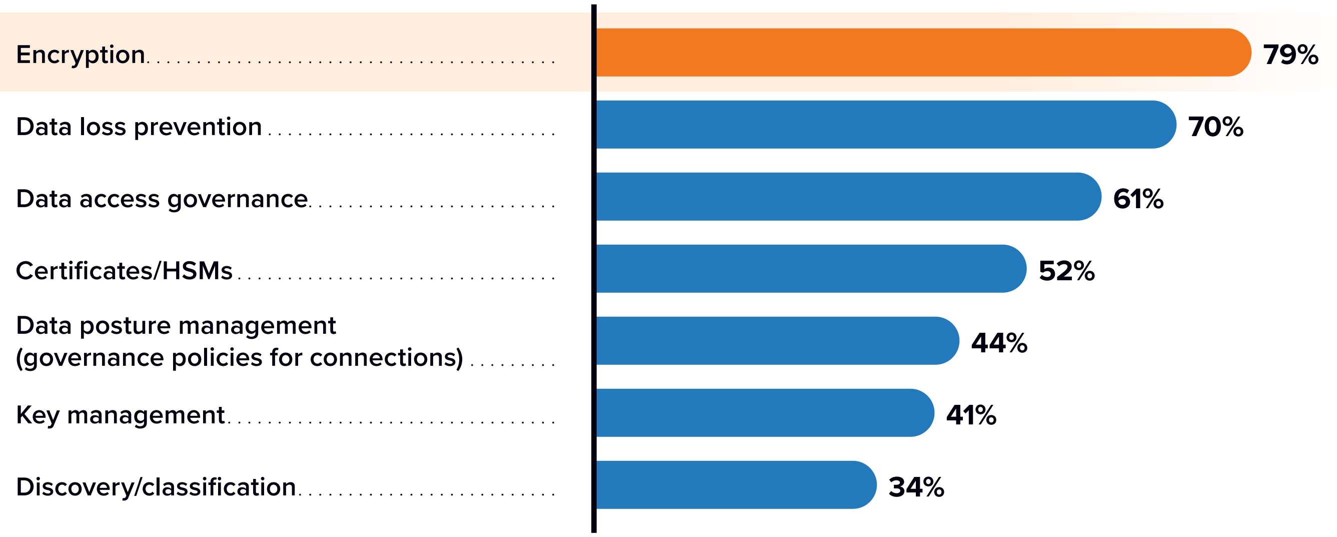
Digital certificates:
The combining of an identity to the cryptographic key to certify that the machine, app, or user is valid and legitimate. (Certificates are issued by a certificate authority [CA], which uses industry standards to validate a user or machine identity. These validations are time sensitive, and they can expire or be revoked if a cryptographic key is compromised or if standards change. A public key infrastructure [PKI] provides the framework for issuing digital certificates.)

FIGURE 1

Data Security Technologies Frequently Used for Privacy Adherence

What data security technologies are being used to demonstrate privacy/compliance?

(Percentage of respondents)



Note: Multiple responses were allowed. n = 619; Source: IDC's *Data Security and Privacy Survey*, March 2024

This entire process plays an important role in building digital trust. But, like the infrastructure it is protecting, it must evolve and modernize to keep data and systems safe. Attackers can take advantage of more powerful computing processes to break encryption algorithms. Regulatory standards change. Cryptography will evolve and advance. More than just modernizing, today's digital businesses need crypto-agility.

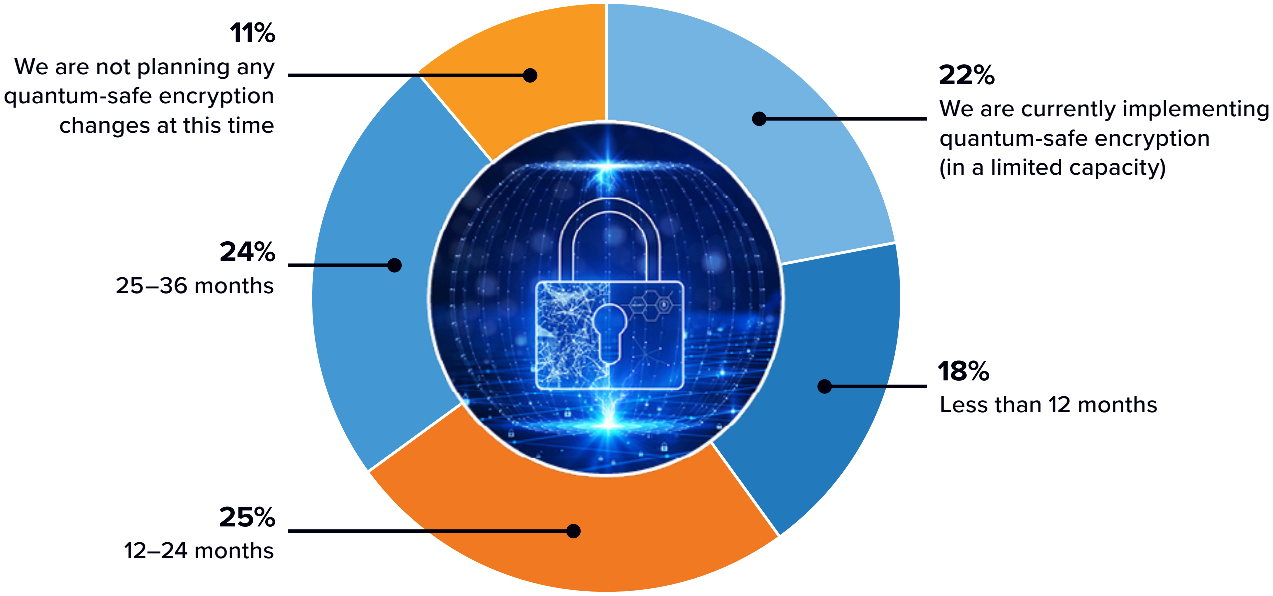
Crypto-agility allows businesses to quickly adapt or switch cryptographic algorithms, parameters, or methods without a major infrastructure overhaul. This will be important as organizations prepare to address vulnerabilities stemming from quantum computing, which promises faster processing power that can break existing encryption in a matter of seconds. Many organizations are already actively implementing quantum-safe encryption to keep these connections and data safe. In the same IDC *Data Security and Privacy Survey,* 22% of respondents indicated that they are currently implementing quantum-safe encryption in a limited capacity. Another 18% of respondents are planning to implement quantum-safe encryption in less than a year (see **Figure 2**).

FIGURE 2

Implementing Quantum-Safe Encryption Is Already in Progress

When do you plan on implementing quantum-safe encryption into your organization?

(Percentage of respondents)



n = 415; Source: IDC's *Data Security and Privacy Survey,* March 2024

In addition to preparing for quantum computing, adopting crypto-agile processes can make it easier to address some of the other challenges that result from multiple cloud and legacy infrastructures, including:

Increased volume of certificates:
With the growth in hybrid and multicloud infrastructures, the number of connections within an organization's ecosystem has increased. These certificates may have different owners across multiple departments. Expiration dates will vary for each certificate depending on its use. Further, web properties are shrinking the life cycle of their certificate validations in the name of security. At the same time, the desire to demonstrate confidence and trust in those connections has also become a priority for most businesses. Altogether, this has added thousands of certificates and attributes to manage, making it challenging to know the status of each one.

Certificate sprawl:
The move to multicloud and hybrid infrastructures creates more connection points coming from more places. Certificates may be required by product teams as well as IT operations groups for different purposes. Often, these teams are not working together and may use different CAs. Without a unified view, managing the entirety of the organization's cryptographic processes is nearly impossible.

Lack of skilled staff/lack of strategic focus of resources:
Cryptography is a specialized craft that most often sits with IT. For those that took the role with intention, it can be hard to demonstrate its business value (outside of keeping certificates from expiring), leading to additional tasks being delegated to the employee. It is also likely that many practitioners inherited the job through attrition. In either case, the ability to effectively manage the cryptography process is hindered.

Implementing a Modern Digital Trust Infrastructure

Digital trust empowers organizations to demonstrate confidence and integrity in the connections and data they offer to customers. Implementing a crypto-agile infrastructure is a critical element for ensuring digital trust both now and in the future.

Making digital trust a reality will require a multistage approach that combines technology and process, including:

Security hygiene:
The foundation of crypto-agility is simply knowing what cryptographic elements are in circulation. This includes an inventory of certificates across the business, including ownership, life cycles, and relevance. In addition, organizations need to understand the standards governing the issuance of these certificates and what changes are coming to pass. As noted previously, the current business environment can make this challenging.

Defining success:
Armed with the knowledge of what exists to be managed, the next step is determining what success looks like for the organization and putting the right pieces in place to achieve that. This includes:

- **Goal setting:**
  Determine which elements are essential for business operations. For many, this is service availability, meaning no outages due to certificate expiration. For those that have a significant Internet of Things presence, success is making sure that the devices are updated securely. Other areas of focus include ensuring product security and validity and a secure remote workforce.

- **Prioritizing:**
  Identify which systems/outcomes are most at risk. Given the breadth of cryptographic assets that make up the modern enterprise, prioritizing is essential. It can also involve knowing which systems can be updated quickly versus those that will require a significant overhaul.

- **Resource investment:**
  Plan and budget for the products, partners, and staff required to do the job. Skilled staff and budget are always a concern. Prioritizing essential tasks can help.

Centralized visibility and management:
Discovery and planning of these assets are critical — but then creating a continuous process for managing everything is a key part of crypto-agility. Bringing assets from across the organization into a single view offers visibility into what may be missing, as well as the status, owner, and needs of each asset.

Reporting and justification:
An important part of any business process is demonstrating success. This is true for crypto-agility as well. Practitioners should be prepared to share important metrics related to success planning, including the number of outages prevented and what steps were taken to reduce risk in the remote workforce.

Adjustment:
An overlooked area for implementing crypto-agility is adjustment. The point of the crypto-agility process is to be flexible for the business — but the process itself may require some adjustment. Based on the results, where does the organization need to make changes? Are there redundancies? Are there areas to increase efficiency or make things more secure or to demonstrate that security more clearly?

Benefits of PKI Modernization/Crypto-Agility

Crypto-agility prepares organizations for quantum-safe computing while helping meet several other objectives, such as automation. As highlighted previously, there may be hundreds of thousands of digital certificates throughout an enterprise organization, with different owners, uses, standards, and life cycles. Putting crypto-agility processes in place makes it easier to automate the discovery, provisioning, and management of these assets.

Automation over manual processes offers a host of business benefits, including:

Cost savings:
With improved visibility, organizations have a better handle on what certificates and crypto assets they have. This is the first step in eliminating assets that are no longer needed. Further, automation can help organizations do more with fewer employees.

Time savings:
This offers direct time savings benefits, including reducing time spent on the entire process by several weeks. It also offers some indirect time savings benefits by reducing outages that require teams to stop what they are doing to address the expired certificate.

Improved compliance with internal and external audits:
The old ways of managing certificates using manual processes and scripts leave organizations vulnerable to outages and security vulnerabilities caused by undiscovered expired certificates. As described in NIST SP 1800–16, automating the management of certificate life cycles — from discovery to renewal or revocation — is essential for minimizing risk and maintaining compliance.

Workplace flexibility:
Automating digital trust operations such as certificate management allows for scalable authentication, which is instrumental for workplace flexibility. With advanced passwordless authentication, organizations can empower their employees to work how and where they need to without being concerned about the integrity and security of their connections.

Considering DigiCert for Digital Trust Modernization

DigiCert, headquartered in Lehi, Utah, is a global provider of digital trust solutions. Its portfolio of offerings is designed to enable enterprise organizations to build a quantum-safe future.

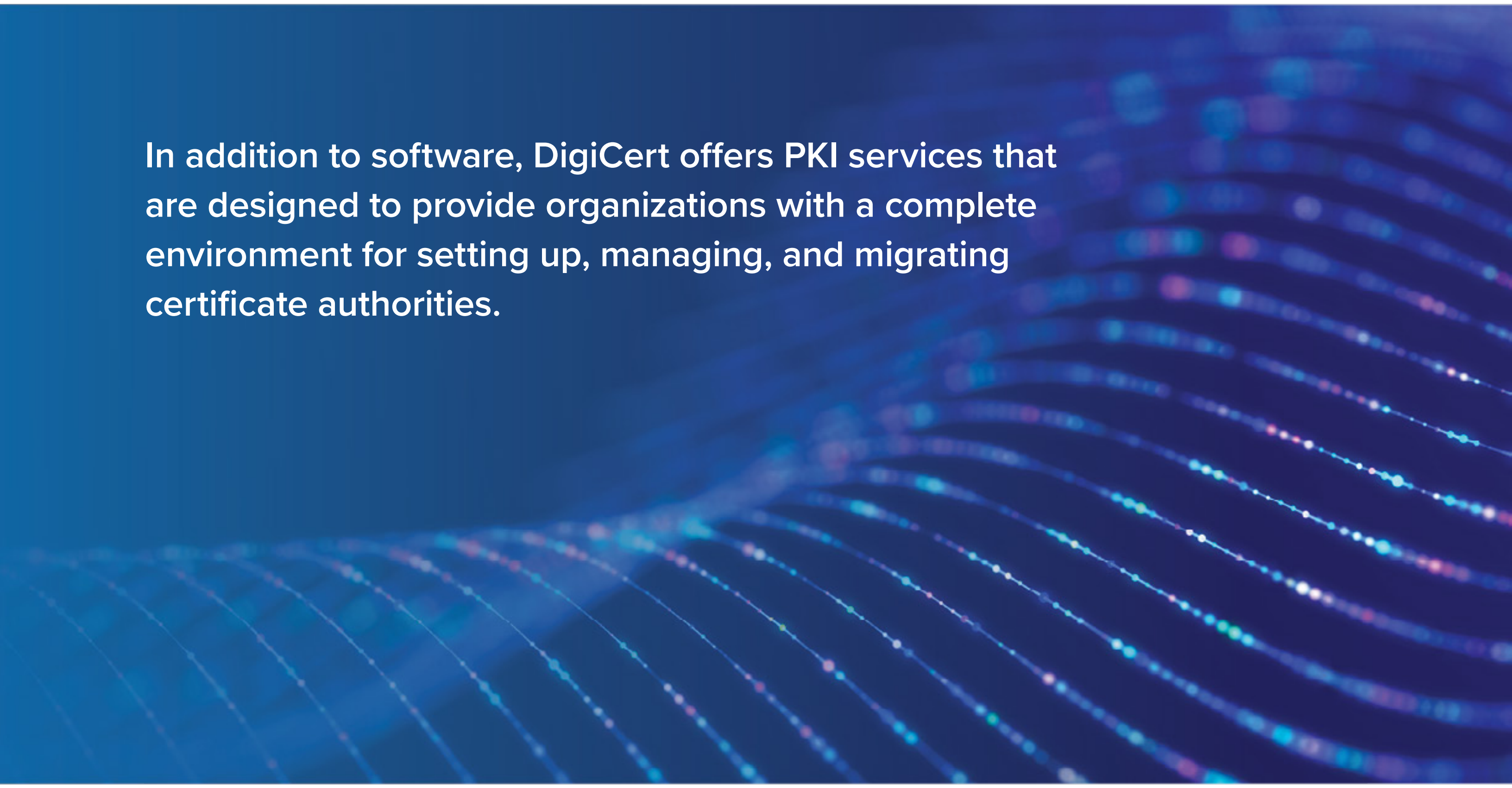
DigiCert Trust Lifecycle Manager (TLM) is designed to address needs at every stage of modernizing the cryptographic process, including:

Discovery:
Crypto-agility starts with having knowledge and control of all your assets. TLM works to provide broad visibility into an organization's cryptographic landscape, regardless of whether they were issued by a public CA or a private CA. This means uncovering, cataloging, and provisioning cryptographic assets such as public and private certificates across the organization. With this information, organizations are in a position to more easily identify vulnerabilities, inefficient practices, and rogue certificates.

Management:
An agile crypto environment is proactive at identifying security or operational issues. DigiCert TLM includes capabilities for managing the life cycle of certificates from a single dashboard and bringing together private and public PKIs. Management capabilities also include essential timeline and authorization criteria, such as knowing when certificates are set to expire and which certificates must be replaced due to changing standards.

Automation:
The increased number of crypto assets in the digital enterprise makes automation necessary for crypto-agility initiatives. DigiCert TLM includes templates and configurations for automating certificate workflows and access privileges. By removing the burden from crypto teams, they are better positioned for scale and agility.

DigiCert Trust Lifecycle Manager is a core part of the DigiCert ONE platform for digital trust. In addition to software, DigiCert offers PKI services that are designed to provide organizations with a complete environment for setting up, managing, and migrating certificate authorities. This environment includes hardware security modules, predefined policies, revocation capabilities, and multiple certificate types.



In addition to software, DigiCert offers PKI services that are designed to provide organizations with a complete environment for setting up, managing, and migrating certificate authorities.

Challenges and Opportunities

Crypto-agility (and cryptography in general) is a highly technical concept for most organizations. While IT and security teams consider certificate management important — particularly when it comes to outages and ownership — they are often investing time and resources on other security initiatives that have more executive visibility, such as keeping sensitive data out of generative AI models and addressing ransomware.

When it comes to quantum computing and quantum-safe cryptography, security and IT teams will likely struggle to justify the expense for these technologies, even with attacks that exfiltrate data with the intent to decrypt it later. Quantum computing is still a few years away from hitting the mainstream, and while there is some movement to get ahead of the threats, a large-scale move to quantum-safe deployments is not likely until a notable attack or compromise occurs. This slow adoption could be a challenge for vendors such as DigiCert as organizations look to invest in other areas.

All the same, crypto-agility is not just about quantum-safe computing. It is about being able to navigate and adjust protections quickly and easily. When discussing risks of long-term projects, crypto-agility — or the need to ensure digital trust — is a valid concern. For teams struggling with justifying the expense for quantum-safe encryption, focusing on approaches and vendors that offer deeper capabilities — such as crypto-agility — can be an opportunity to prepare for a post-quantum world while addressing other business needs.

Conclusion

Digital business has exponentially increased the number of connections and data assets that are protected with cryptographic algorithms.

With an increase in volume comes an increase in risk, not only for compromise but also for key updates being missed in the overload. This problem will only get worse over time as data continues to increase and post-quantum computing comes to fruition. Modernizing cryptographic processes for agility and scale is an important underpinning for strategic businesses. It provides a strong security posture and the ability to adapt to changing standards requirements that protect the cryptographic infrastructure in a post-quantum world.

About the IDC Analyst

Jennifer Glenn

Research Director, Security and Trust Group, IDC

Jennifer Glenn is research director for the IDC Security and Trust Group and is responsible for the information and data security practice. Jennifer's core coverage includes a broad range of technologies including messaging security, sensitive data management, encryption, tokenization, rights management, key management, and certificates. As part of this research, Jennifer will demonstrate the critical role of data security in top enterprise initiatives such as generating customer trust and digital transformation.

More about Jennifer Glenn

Message from the Sponsor

digicert®

DigiCert is a leading global provider of digital trust, enabling individuals and businesses to engage online with the confidence that their footprint in the digital world is secure.

DigiCert ONE, the platform for digital trust, provides organizations with centralized visibility and control over a broad range of public and private trust needs, securing websites, enterprise access and communication, software, identity, content, and devices. DigiCert pairs its award-winning software with its industry leadership in standards, support, and operations and is a top digital trust provider of choice for leading companies around the world.

For more information, visit www.digicert.com

follow @digicert

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

idc.com   in @idc   X @idc

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets.
With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.