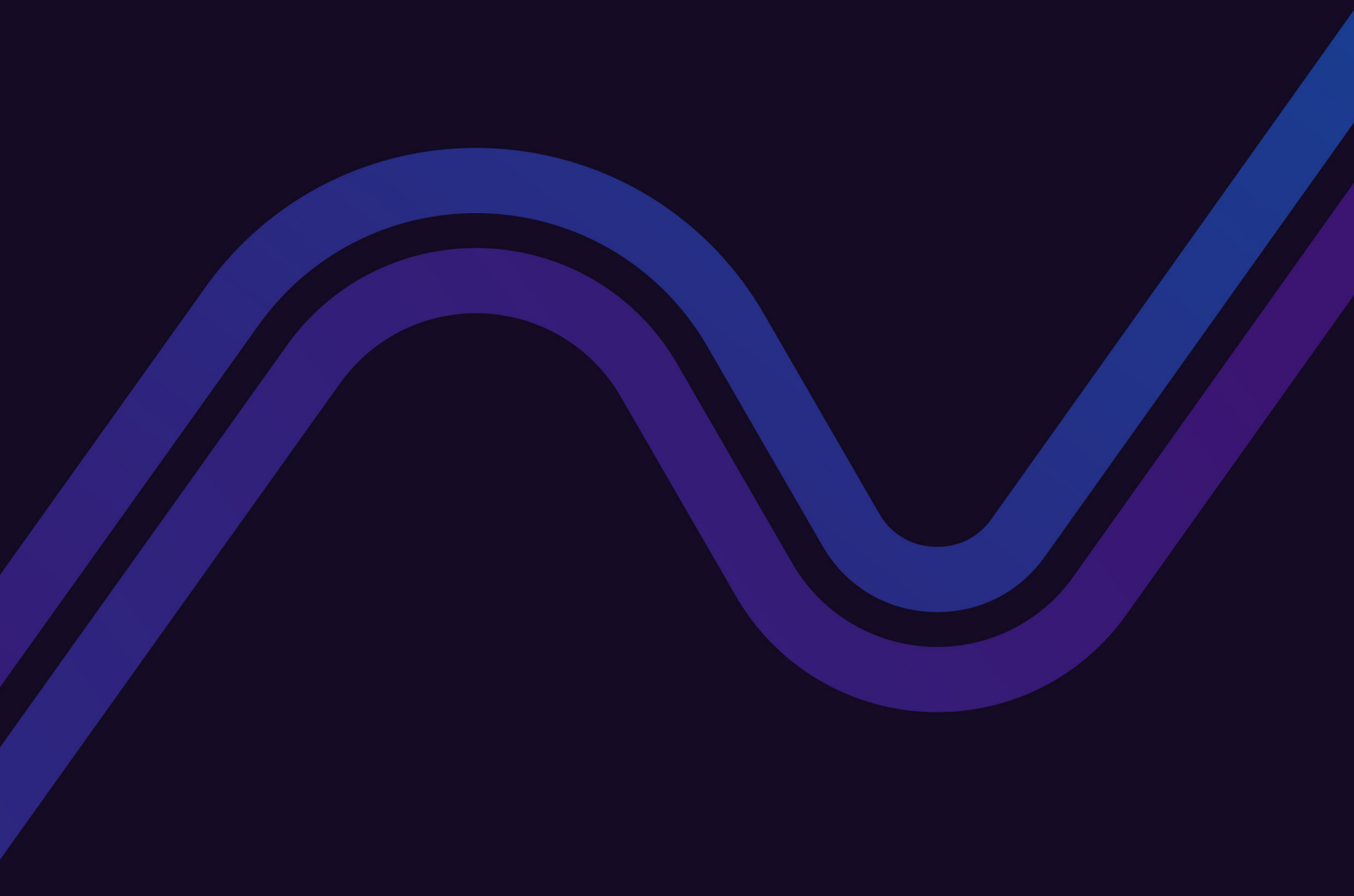
INDUSTRY REPORT

2022 Emerging Trends in Cryptography

KEYFACTOR

PrimeKey by KEYFACTOR



Introduction

Cryptography is the foundation of the digital world. Why?

For CxOs, digital business is everything. And their digital business requires digital trust. Organizations rely on public key infrastructure (PKI) and cryptography to establish the digital trust needed across their corporate IT infrastructure and connected product solutions.

Without cryptography, the modern digital world could not exist.

Cryptography plays a vital role in many parts of daily life, and this role will only grow over time. Recent events, such as the SolarWinds and Kaseya hacks, have underscored the importance of supply chain visibility and management for modern businesses. Closing the supply chain visibility gaps and improving software security via the adoption of DevSecOps practices will require increased use of cryptography.

As companies address these supply chain security challenges and work to implement zero-trust architectures, the number of digital identities, access controls, code signing requirements, and trust relationships that they will need to manage will grow exponentially.

Doing so in a scalable and secure way requires a focus to manage cryptography as critical infrastructure, ensuring that attempts to solve modern security challenges do not create new ones in the future.

Anticipating and planning for future needs requires keeping close tabs on changes that can impact a company's business and cryptographic needs.

To that end, let's explore some of the biggest emerging trends in cryptography in 2022 and beyond.

Meet the Contributors:

Thomas Gustavsson
Chief PKI Officer

David Hook
VP of Software Engineering & Cryptography

Admir Abdurahmanovic
SVP of Strategy

Sami Van Vliet
Principal Product Manager

Ellen Boehm
VP of IoT Strategy and Operations

Chris Hickman
Chief Security Officer

Contents

TREND 1:

The Emergence of PKI Governance

Manual certificate management processes have not kept up with the evolution of IT environments. As enterprises continue to deploy new PKIs for new use cases, PKI governance inevitably becomes siloed.

Enterprises can facilitate the management of their PKI by performing PKI consolidation and migrating several disparate PKIs into a single multi-tenant PKI solution (such as EJBCA). Another trend in this area is using PKI as a Service (PKIaaS).

However, even though PKI consolidation and PKIaaS are gaining popularity and it's easy to believe either is a one-stop-shop. The reality is that large organizations will continue to have several PKI silos.

For bad and sometimes for good, PKI silos occur everywhere.

Thomas Gustavsson
Chief PKI Officer

Find me on LinkedIn

Different Providers for Different Needs

Identity management and access control are crucial for a zero-trust security strategy.

PKI is vital to implementing zero trust because it ties assigned permissions to an entity's identity and provides strong user authentication.

However, the evolution of IT environments means that PKI certificates are applied in many ways and in various environments. Web servers need certificates from a public certificate authority (CA) to prove their identities, while internal identity management is under a private CA.

Digital certificates used in DevOps practices have short lifecycles compared to longer-lived SSL certificates for websites. On-prem and cloud-based infrastructure both have their preferred root CAs.

Meeting the needs of all PKI users requires support for a dizzying number and variety of digital certificates. However, allowing these various PKI applications to become siloed places the organization at risk.

The Need for a Common PKI Platform

As companies pursue their zero-trust security goals, overhauling their PKI governance is a must.

Centralized visibility and control over an organization's various applications of PKI are crucial to achieving the access control required for regulatory compliance and enterprise cybersecurity.

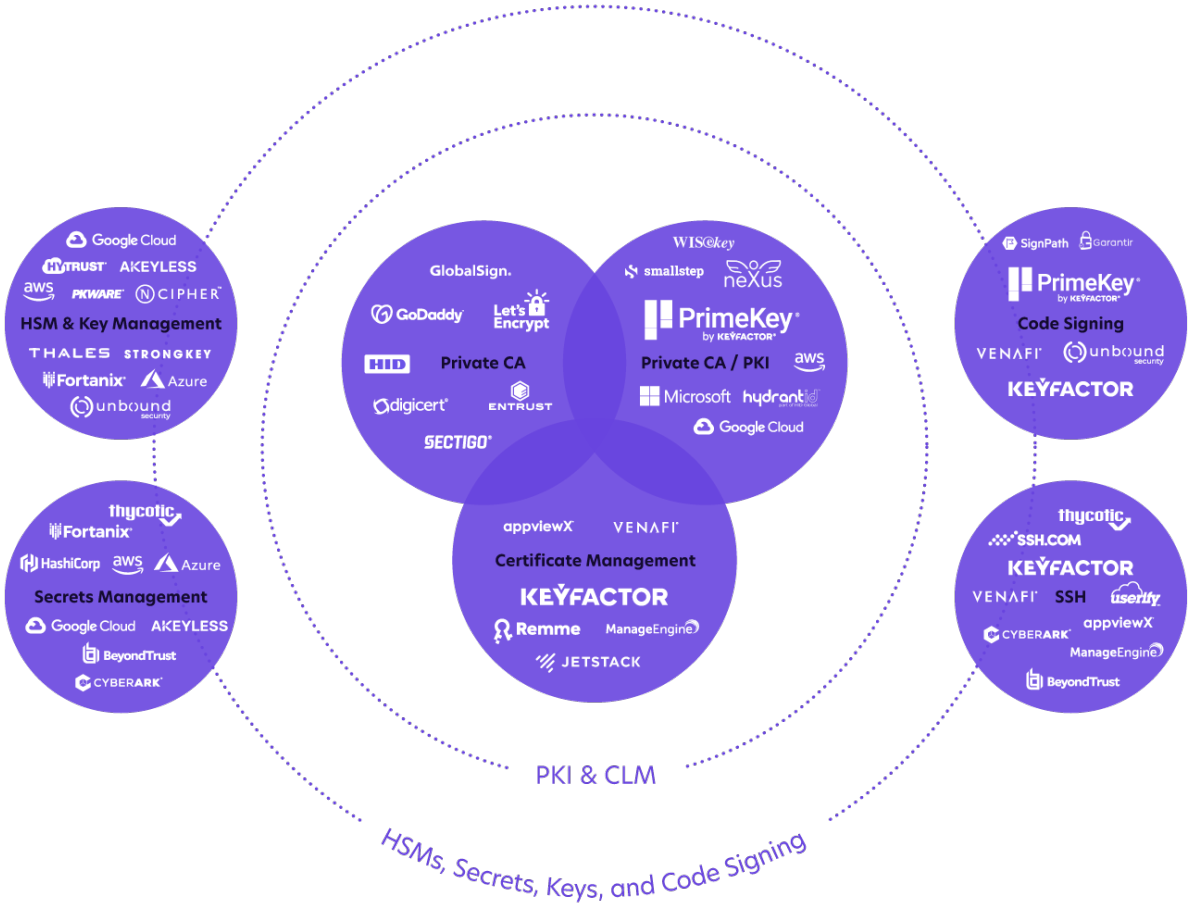
The diversity of PKI used in the modern enterprise is driving a shift to vendor-agnostic PKI platforms with the ability to monitor and manage digital certificates from different root CAs, in different environments, and with different lifecycles and applications.

The convergence of machine identity management tools

Now that's a lot of tools.

Use this graph and take an audit of your existing machine identity management practices (PKI, certificate management, secrets, etc.) to determine where the gaps are.

This will help you find the tools and processes that fit the unique requirements of the various teams within your company.



TREND 2:

Post Quantum Cryptography (PQC) Comes Alive

Quantum computing poses a significant threat to classical asymmetric encryption algorithms. These algorithms are based on mathematical operations that are relatively easy to perform but exponentially more difficult to reverse. Quantum computing breaks this asymmetry by offering more efficient methods for these inverse operations. Without asymmetric complexity, it is impossible to create an algorithm that is both asymmetric and secure.

While quantum computers capable of breaking classical asymmetric encryption algorithms are still several years in the future, they will pose a very real security threat to the unprepared. To address this issue, new post-quantum cryptographic (PQC) algorithms based on problems that retain their asymmetric complexity in the face of quantum computing have been in development for several years now.

NIST has been running a multi-year competition to evaluate various PQC algorithms and select the ones that will be endorsed as standards for PQC. The third and final round concludes in December 2021, with the results expected to be announced at the end of the year.

This means that beginning in 2022, draft standards will start to come out, with the final standards expected in 2024. With the arrival of official standards, both from the IETF and NIST, PQC is finally coming into its own. The new standards will establish the expectations for what should be provided in solutions targeting a wide range of Government and Industry sectors.

Quantum computing is not an immediate threat, but quantum computers capable of breaking classical cryptography will likely emerge during the lifecycle of solutions being developed today. NIST's endorsement of PQC standards lays the groundwork for developers to start planning and building for the future.

David Hook
VP of Software Engineering & Cryptography

Find me on LinkedIn

51%

of enterprises have identified crypto-agility as a leading strategic priority for preparing for quantum computing.

2021 State of Machine Identity Management Report

Inside the NIST Post-Quantum Cryptography Standardization Process

NIST has hosted a five-year contest for selecting candidate algorithms for future PQC standards. Key milestones in this process have included:

DECEMBER 20, 2016

Call for Proposals

NIST solicits proposed algorithms for PQC standards.

NOVEMBER 30, 2017

Submission Deadline

The submission window closes for PQC standard candidates.

DECEMBER 21, 2017

Round 1 Algorithms Announced

NIST announces accepted 69 "complete and proper" submissions.

APRIL 11-13, 2018

First PQC Standardization Conference

Authors of candidate algorithms discuss and explain their algorithms.

JANUARY 30, 2019

Round 2 Candidates Announced

NIST announces the 26 algorithms that moved to the second round of the competition.

AUGUST 22-24, 2019

Second PQC Standardization Conference

Round 2 candidate algorithms are discussed, and NIST solicits feedback on potential finalists.

JULY 22, 2020

Round 3 Candidates Announced

NIST announces seven finalists and eight alternates for PQC standards.

JUNE 7-9, 2021

Third PQC Standardization Conference

Round 3 candidate algorithms are discussed, and NIST solicits feedback for final selections.

DECEMBER 2021/ JANUARY 2022

NIST is expected to announce the results of Round 3

2022-2024

Draft standards are developed and published

TREND 3:
eIDAS Gets Extended

In 2014, the European Union (EU) implemented a regulation for electronic authentication systems (eIDAS). This regulation defines a framework for digital authentication and trust management for digital transactions within the EU's internal market.

In June 2021, the EU announced the intention to expand eIDAS to create a framework for developing a "trusted and secure" European eID. This eID would expand the applications of eIDAS.

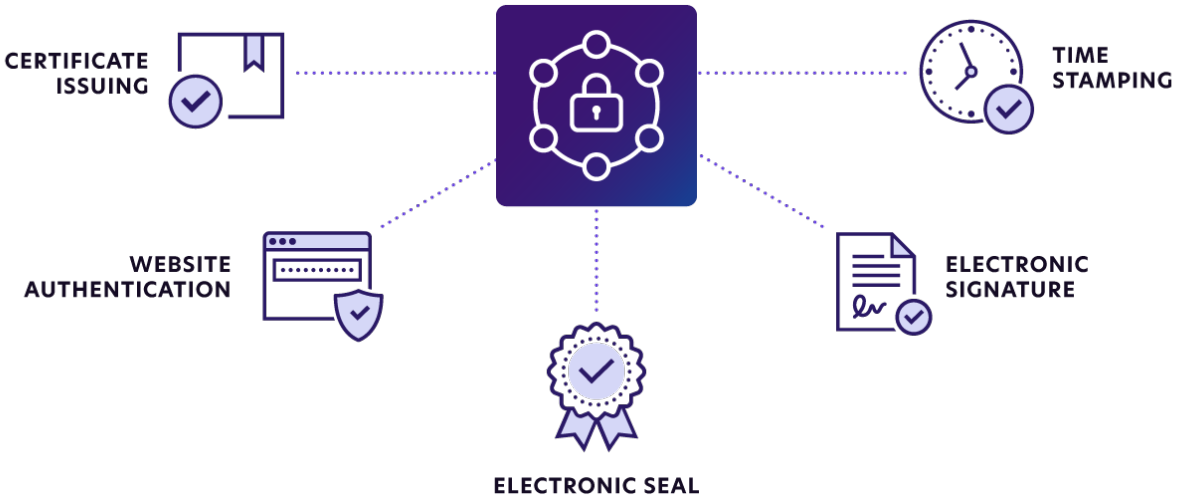
It would allow European citizens to link various personal attributes (driver's licenses, bank account data, etc.) to their eID and store them within digital wallets. Within these wallets, it should also be possible for EU citizens to generate digital signatures using their eID.

Admir Abdurahmanovic
SVP of Strategy

Find me on LinkedIn

In its announcement, the European Commission has invited the Member States to create a common toolbox — including technical architecture, standards, and best practice guidelines — for the eIDAS by September 2022. This involves creating standards for applying PKI and the functions of audited Trust Services Providers to serve a wider range of purposes and meet the targets and goals of the EU Commission's 2030 Digital Compass.

If successful, the EU's eID will enable EU citizens to unify their digital identities without using single sign-on (SSO) platforms that collect and send personal information back to the service provider. It also could improve the use of digital services within the EU and serve as a model for similar services globally, enabling secure digital identities across geographic regions.



TREND 4:

Companies get their house in order

In 2021, cyber threats exploded into public awareness. The SolarWinds hack demonstrated the potential impacts of software supply chain exploits, and the Colonial Pipeline hack showed that cyberattacks also posed a threat to physical supply chains. Attacks against a Florida water treatment plant and hospitals demonstrated that cybercriminals could place health and safety at risk.

These high-profile attacks impacted ordinary citizens and drew attention to cybersecurity shortcomings in critical infrastructure and the private sector. The attacks inspired the United States President's Executive Order (EO) on Improving the Nation's Cybersecurity (14028) and increased scrutiny regarding how well companies are protecting themselves against cyber threats in general and supply chain attacks.

As supply chain attacks become more common and visible, software vendors and service providers will need to demonstrate that they are taking steps to protect themselves and their customers against cyber threats.

Software vendors will need to demonstrate best practices, assure quality control, and validate third-party components used in their products. Service providers that experience outages or are used as a stepping stone to attack their customers (as occurred in the Kaseya hack) may face steep penalties from their customers, regulators, and consumers.

The many high-profile attacks made it clear to companies that legacy security models are no longer adequate to protect against modern cyber threats. Organizations must implement zero-trust architectures — built on strong user authentication and identity management to minimize their risk of high-profile and embarrassing cyberattacks.

Sami Van Vliet
Principal Product Manager

Find me on LinkedIn

96%

of IT security leaders agree that PKI and digital certificates are essential to Zero Trust.

2021 Executive Survey on PKI in Zero Trust

Top 2021 Cyberattacks: Key Takeaways

High-profile cybersecurity incidents in 2021 inspired an Executive Order on Cybersecurity and drew additional attention to the shortcomings of legacy cybersecurity strategies.

SolarWinds

The SolarWinds attacker exploited access to the company's network to insert malicious code into an update to its Orion network monitoring software. This provided backdoored access to the networks of Orion users.

KEY TAKEAWAY

Regularly test your certificate re-issuance and revocation capabilities to ensure you can respond effectively to a compromise.

Colonial Pipeline

The DarkSide ransomware group infected Colonial Pipeline's IT network with ransomware. This prompted the company to shut down operations to prevent its spread. This attack shut down a pipeline that supplies nearly half of the fuel to the US East Coast.

KEY TAKEAWAY

Overly permissive access controls can force unnecessary shutdowns of critical systems to manage cybersecurity incidents.

Oldsmar Florida Water Treatment Plant

A cyberattacker gained remote access to a computer operating industrial control systems via an unsecured instance of TeamViewer. An attempt to increase levels of lye in treated water was detected and reversed in time by the system's operator.

KEY TAKEAWAY

Insecure remote access solutions place critical infrastructure and corporate systems at risk.

Kaseya

Cyber threat actors exploited a vulnerability in a Kaseya product designed to allow Managed Service Providers (MSPs) to manage their clients' environments. This provided the attacker with the access necessary to infect the customer networks with ransomware.

KEY TAKEAWAY

Trusted third parties can pose significant cybersecurity risks to corporate systems.

TREND 5:

Digital Machine Identities are the Future of Manufacturing

In the past, digital identities and identity management were mainly restricted to humans. However, companies across all industries are increasingly adopting machine identities, assigning unique roles and permissions to software and systems.

Ellen Boehm
VP of IoT Strategy and Operations

Find me on LinkedIn

Digital Identities for Connected Vehicles

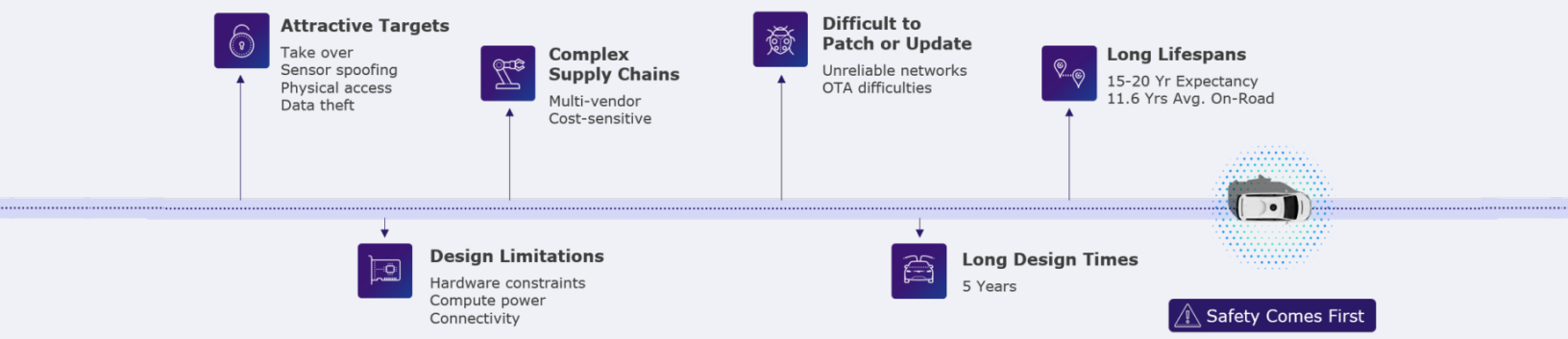
The automotive industry is steadily moving towards the connected car. With the ability to communicate with manufacturers, other vehicles, and transportation infrastructure, vehicles can be safer and more efficient.

Digital identity is essential for communications between vehicles and other entities. A vehicle with a unique identity can communicate with its owner, manufacturer, maintenance providers, electronic charging stations, and more. PKI for connected cars also ensures the confidentiality, integrity, and authentication of messages between connected vehicles and other entities.

Why Securing Vehicles is Hard

The security weaknesses that have plagued the first generation of connected vehicles are not due to negligence.

Rather, they've surfaced because securing connected vehicles is particularly challenging, even in comparison to securing other IoT devices. Some of these challenges are inherent to automotive IoT security, but some are specific to vehicles.



Machine Identity Governance for Supply Chain Management

Supply chain visibility and management is a growing concern across industries for various reasons. Defective or compromised components can undermine the security of a manufacturer's products. Market competition drives innovation and increased efficiency in supply chain management. Consumers demand products that are developed using sustainable and ethical practices.

Achieving supply chain visibility and security goals requires flexible and scalable PKI infrastructure.

Companies need to be able to balance their need to be open and flexible with security requirements. A zero-trust infrastructure built on strong digital identities and PKI enables companies to scalably, securely, and sustainably manage their trust relationships up and down their supply chains.

TREND 6:

Crypto-Agility Goes Mainstream

Cryptography lies at the heart of the digital ecosystem. Cryptographic algorithms are used to prove identities and to protect data integrity and confidentiality. Without cryptography, most of the modern Internet falls apart.

The face of cryptography and companies' applications of cryptography are evolving rapidly. The growth of quantum computing and post-quantum cryptographic algorithms create the need to update cryptographic algorithms currently in use.

Expanded use of digital identities for supply chain management, software development, cloud computing, and other applications creates new PKI challenges. Even small changes to certificate lifespans can have a dramatic impact on the software that relies upon them.

Chris Hickman
Chief Security Officer

Find me on LinkedIn

Most companies lack a true understanding of what it means to achieve crypto-agility. For example, the ability to change cryptographic algorithms in use or update a protocol only represents a small part of crypto-agility.

True crypto-agility is the ability to use cryptography to its full potential, rolling out digital identities as needed, securing the software supply chain, deploying PKI to support DevSecOps, all with the ability to respond to changes rapidly.

A growing awareness of supply chain risk, the global drive toward zero trust, and the widespread adoption of PKI for software security make crypto-agility vital for companies looking to compete in the modern, increasingly digital marketplace.

Next Steps

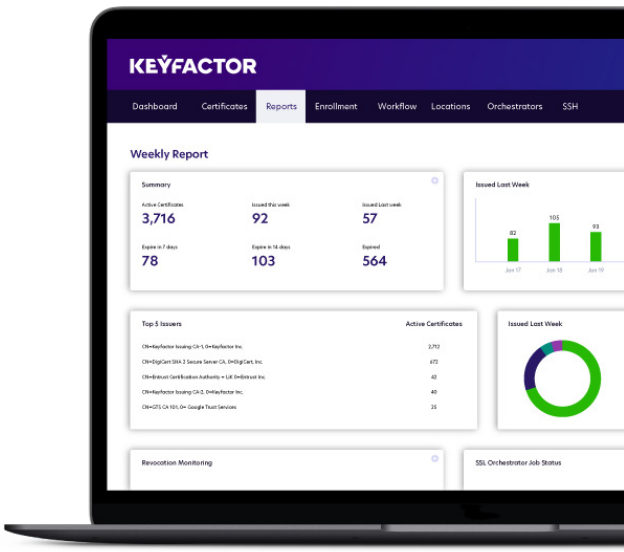
Is your company ready for these trends?

Current events can have a sudden and significant impact on an organization's cybersecurity and cryptographic needs. High-visibility cybersecurity incidents in 2021 created a sudden focus on supply chain security challenges and the need for improved third-party risk management.

Keyfactor is the industry leader in crypto-agility solutions. We can help you adapt to rapidly changing circumstances by providing your team with the tools needed to deploy, manage, and automate digital certificates and key management across your business.

Ready to take your first steps toward crypto-agility?

SIGN UP FOR A FREE DEMO TODAY



KEYFACTOR

Keyfactor is the leader in cloud-first PKI as-a-Service and crypto-agility solutions. Our Crypto-Agility Platform empowers security teams to seamlessly orchestrate every key and certificate across the entire enterprise.

For more information, visit www.keyfactor.com or follow us on LinkedIn, Twitter, and Facebook. Built on a foundation of trust and security, Keyfactor is a proud equal opportunity employer, supporter and advocate of growing a trusted, secure, diverse and inclusive workplace.

Contact Us

- www.keyfactor.com
- +1.216.785.2990