Market Pulse

How PKI-as-a-Service can Help Accelerate Digital Evolution

DIGITAL TRANSFORMATION PROJECTS HAVE CATAPULTED UP ORGANIZATIONS' PRIORITY LISTS in the post-pandemic era. But they require enabling technologies such as public key infrastructure (PKI), which is core to IT security in that it protects people, systems and machines across organizations through encryption, authentication and signing.

Unfortunately, 66% of respondents in a Foundry MarketPulse survey of 321 decision- makers reported that their legacy PKI wasn't up to the task and was actually inhibiting digital transformation to some extent.

This report will describe the key use cases for PKI in 2023 and the challenges organizations face with their PKI. It will also detail how a cloud-based, managed PKI service like PKIaaS can go beyond securing traditional business use cases, help enable digital transformation initiatives, and future-proof the organization from threats such as those that will come with the rise of post-quantum computing.

Why PKI?

The mission-critical importance of PKI is being driven by a number of factors, including the need to protect communications generated by IoT devices, as well as enterprise requirements for compliance, authentication, security, and privacy.

66% of respondents reported that their **legacy PKI was inhibiting digital transformation** to some extent.

The shift to remote and hybrid work, as well as the migration of data and applications to the cloud, have also contributed to the heightened sense that a distributed, multi-cloud organization needs a comprehensive PKI strategy.

The Foundry MarketPulse survey identified the top use cases for digital certificates for 2023. They are:

- **Microsoft Active Directory (69%):** Companies use digital certificates to authenticate devices, users and services.
- **Private TLS/SSL: (61%):** Secures common use cases such as access to an organization's private network or VPN.
- **Code signing (59%):** Verifies the integrity of software code.
- **Secure S/MIME email (51%):** Authentication and end-to-end encryption of private emails.
- **Microsoft Intune (46%):** Manages user access and protects data on mobile devices.
- **IoT devices (40%):** Authenticates devices and encrypts communications.

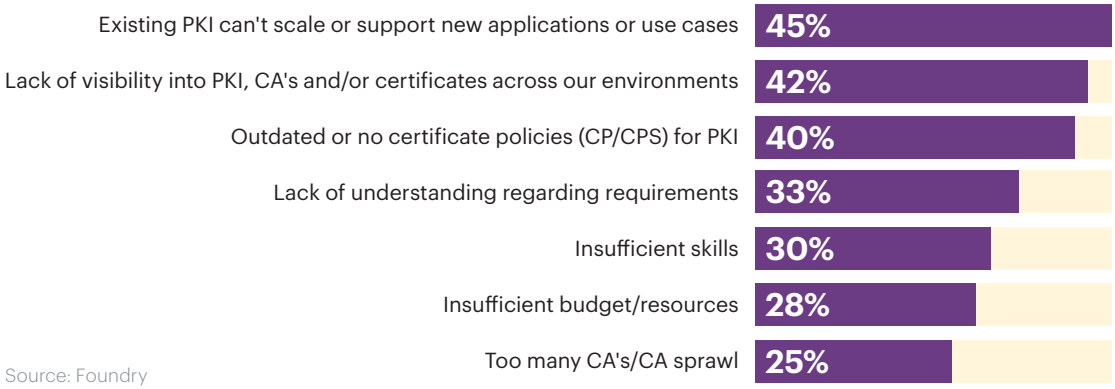
PKI Challenges

When organizations assess their existing PKI, they are often surprised to find that it falls short in a number of areas. The technology might be outdated. There might be a lack of policies governing when and how to deploy PKI. In a worst-case scenario, there is no longer a PKI expert within the company.

According to the survey, the primary challenges associated with enabling or managing PKI are: the inability of existing PKI to scale or support new applications or use cases (45%); lack of visibility into PKI or certificate authorities (CAs) across the enterprise environment (42%); outdated or no certificate policies for PKI (40%); lack of understanding

Market Pulse

Primary challenges in enabling or managing PKI



Source: Foundry

regarding requirements (33%); insufficient skills (30%); insufficient budgets (28%); and too many CAs or CA sprawl (25%).

Respondents outside of North America are more likely to report that skills gaps are inhibiting PKI management. North American respondents were more concerned about scalability, visibility and policies. European respondents expressed concern over CA sprawl and the inability to move away from legacy applications.

Why PKIaaS

PKIaaS has already been adopted as the primary PKI by 25% of survey respondents; another 15% have adopted it in some business units or departments, or for some use cases. Another 6% will adopt PKIaaS in 2023, with 20% of respondents in the evaluation and research stage and 17% indicating that PKIaaS is on their radar.

Large enterprises are more likely to be researching, planning to adopt, or using PKIaaS. (100% of larger enterprises at a minimum have PKIaaS on their radar, versus 70% of those with between 1,000 and 5,000 employees).

The key drivers for PKIaaS are proven security (64%); ease of use (62%); scalability (60%); speed to deploy (55%); integration with cloud migration strategy (50%); relieves burden from internal staffers (48%); and provides a unified platform for private and public PKI (43%).

Speed to deployment is more likely to be cited as a top PKIaaS benefit in North America (63% versus 46% in Europe and 56% in Asia-Pacific), while a unified platform is a top attraction in Asia-Pacific (51% versus 39% in North America and 40% in Europe). Those who have already adopted PKIaaS cite scalability as the biggest benefit (59% versus 45% among those who have not yet adopted PKIaaS).

Preparing for Post Quantum

PKIaaS addresses current concerns. It will also be a required solution to help future-proof organizations against the impact of quantum computing on cryptography. Quantum computers exist today, and experts predict that within the decade they will be able to crack the standard public key encryption we currently rely on.

Survey results indicate that only 26% of respondents are building a quantum cryptography strategy, while 55% either have not considered the impact or have not taken any action to prepare. Lack of the right technology to support the extra computing power required (51%) is the top concern regarding quantum computing. Respondents are also concerned about prioritizing data and data flows (45%) and having the required resources and expertise to oversee the transition to post-quantum cryptography (45%).

When an organization is investing in a critical piece of IT security, such as PKIaaS, it's important to make sure the service provider is post-quantum ready. This will enable the organization to start testing post-quantum algorithms ahead of the threat, and to have confidence that they will have the proper technology in place to protect data in a post-quantum world.

For more information on PKIaaS, visit **Entrust.com**