White Paper

PKI Investments Help Organizations Improve Security and Modernize Business Processes, Study Finds

Sponsored by: DigiCert Inc.

Frank Dickson Robyn Westervelt
January 2021

EXECUTIVE SUMMARY

IT security professionals and operations teams are under increased pressure to manage the security and resiliency of mission-critical systems in support of rapidly evolving enterprise digital transformation (DX) initiatives. In a bid to alleviate that pressure and allocate resources more effectively amid the growing hybrid and multicloud environments, CIOs, chief information security officers (CISOs), and security architects are now addressing public key infrastructure (PKI) implementations that are often disjointed and poorly managed.

PKI is the backbone of many organizations that value cybersecurity resiliency because it enables organizations to automate the process of enforcing data security policies and procedures using digital certificates and public key encryption. PKI was designed to establish validated and trusted connections between systems and provide unhindered user access to sensitive resources. Over time, PKI grew to protect document, email, and code integrity through cryptographic signing certificates as well as protect assets and individuals with digital identities using device certificates.

Today, as security teams are under more pressure than ever before, PKI is being thoroughly tested and relied upon. Teams are using PKI to remediate risks as the business grows its use of cloud services, and attackers in turn seize on complexity and configuration issues caused by fragmented security infrastructure. CISOs are making it a priority to address this challenge, according to IDC's *Data Security Survey,* 2020, which reached more than 400 IT security and data management specialists in Europe and North America. In the survey, about 78.9% of organizations reported enterprise key management to support a variety of functions, including:

- **Secure remote access:** To strongly authenticate employees and partners to a wireless network or VPN for secure access
- **Secure BYOD:** To support unmanaged BYOD initiatives and maintain secure access to enterprise resources without sacrificing the mobile user experience
- **Secure authentication:** To strongly authenticate individuals to applications containing sensitive information
- **Secure email:** To enable email users to send encrypted and digitally signed emails across all corporate devices
- **Document signing integrity:** To validate the integrity and authenticity of digital signatures on critical documents

- **Secure Internet of Things (IoT) devices:** To provide device identity and establish root of trust and maintain the integrity of software and firmware on sensitive IoT devices
- **Sign code and digital binaries (including containers):** To validate the provenance and veracity of software and code components

As organizations continue to use PKI for security on many fronts — and attackers continue to ramp up both their sophistication and frequency against sensitive data — security teams must implement more comprehensive and coordinated approaches to support evolving business strategies.

IT transformation (ITX) is a key component of a DX strategy, and data security and availability are cornerstones of ITX. PKI plays a significant role in maintaining the integrity, availability, and resiliency of an organization's IT infrastructure, but managing data protection across these increasingly hybrid environments is becoming more complex as threats become more diverse and sophisticated. The latest string of high-profile data breaches illustrates the problems created by today's highly distributed and convoluted corporate environments. Attackers are seizing on costly mistakes that leave database servers open to the public internet. They continue to exploit weak, default, and stolen passwords and are constantly probing for vulnerabilities created by data management across distributed environments. More than 30% of those surveyed cited the difficulty of integrating their hybrid and multicloud environments with existing IT infrastructure, and 37% called the complexity of security solutions one of the top 3 greatest threats — after rising attacker sophistication and cloud adoption risks — their organization faces in the next two years. The problem is often compounded by poorly managed PKI operations that can inhibit user productivity, erode customer and partner trust, and lead to costly security incidents and data breaches.

PKI Support of Critical Business Applications Is "Highly Effective"

Interviews conducted for this study conveyed an overwhelmingly positive impression of how PKI can seamlessly integrate with a variety of industry-specific enterprise business applications. PKI deployments were praised for scaling to handle complex payment applications and point-of-sale (POS) terminals for remote access, integrating with various back-end systems, including advanced analytics repositories in support of encryption, and enabling digital document signing to maintain the integrity of contracts in the field using a custom content management system.

CISOs and security architects found overwhelmingly positive impressions of PKI, calling it "highly effective," when the technology is properly implemented and proactively managed. Most of the interviewees are working with multiple PKI implementations integrated with industry-specific business applications and Active Directory. They have managed or overseen the management of PKI long enough to have experienced growth and change at their organizations and have worked with multiple updates to their existing PKI implementations to maintain a strong security posture. IDC recommends that IT organizations take the following actions to reinforce the effectiveness of PKI:

- Identify if the organization can attract, train, and retain security architects to manage the existing PKI implementations and determine if the team has the expertise to support new business objectives requiring the scalable application of digital certificates.
- Consider leveraging managed PKI services to streamline management and reduce complexity. Once PKI operations are designed and implemented, changing specifications and processes can be cumbersome. The investment made up front is crucial.

METHODOLOGY

This IDC study interviewed chief information security officers and security architects at several major businesses about their existing PKI infrastructure and how it was adapted to support their organization's cloud adoption and digital transformation strategies. The insights gleaned from these interviews were combined with new survey data about the challenges of securing hybrid and multicloud environments. The study identified improved efficiencies and lower management costs associated with a variety of use cases, including managed and on-premises PKI implementations that support code signing to validate the authenticity of software updates on IoT devices, document signing to eliminate paper and manual processes, secure email, secure remote access, and user and machine authentication to sensitive company resources.

SITUATION OVERVIEW

PKI Essentials for Preventing Successful Attacks and Protecting Critical Resources

Many organizations are seeking help from PKI specialists to streamline, centralize, and automate the management of digital certificates as part of digital transformation initiatives to eliminate fragmented and redundant infrastructure and cut costs. This help includes automating the management of one or multiple PKI implementations supporting various business units to a managed PKI service to ensure proactive maintenance and reliability.

This study found cost reductions and efficiency improvements frequently cited as reasons behind many PKI investments. However, the major drivers for PKI implementations were the weaknesses and vulnerabilities that arise from the complexity of implementing and managing security products. Nearly 40% of IT security, line-of-business, and data management specialists cited the rising sophistication of attacks and the increasing complexity of managing and supporting security products as significant challenges, according to IDC's *Data Services for Hybrid Cloud Survey.* IDC research has found that security teams face growing security and privacy concerns. They are under increased pressure to meet and maintain a growing number of compliance obligations and are constantly defending against growth of targeted and multipronged cyberattacks against critical corporate resources.

In addition to the reputation damage, direct costs, and regulatory sanctions mentioned previously, cyberattacks can result in unplanned downtime, loss of competitive trade secrets, and permanent data loss. IDC research has found that the average cost of downtime industrywide is $250,000 per hour. Comparing the cost of attack prevention and recovery software with even one hour of downtime often justifies the cost. In many cases, breaches now require public disclosure, ensuring reputational damage that is often long lasting with no way to recovery permanently lost customers or data. IDC research has found that reputational damage occurs in almost half of data breach situations, further increasing recovery and remediation costs.

Increasingly publicized security breaches constantly remind both businesses and consumers that identity credentials are at the heart of security. Countless studies have shown that vulnerability and configuration issues, often stemming from increased complexity, contribute to security incidents. Reducing fragmented and disjointed PKI implementations can help reduce user and system errors that attackers seize upon and prevent data leakage in the process. PKI, if properly deployed and managed, is one of the most powerful tools that organizations can use to avoid costly and embarrassing data breaches. A growing number of organizations are revisiting their encryption and key management strategies to gain situational awareness and in turn bolster their security postures.

The security professionals interviewed for this study called PKI an essential, time-tested component for supporting data encryption and validating data and transaction integrity and said that it is critical in verifying user and machine identities at their organizations. PKI can raise the barrier an attacker must overcome to gain access to critical resources. PKI also supports the scalable security required for high-speed or multipronged important business processes and has been proven to improve user productivity and customer retention by remaining transparent to end-user activities.

One theme that did come up in the interviews is the ongoing battle between the application of security and end users who are often frustrated by security measures. In response, security practitioners are increasingly turning to PKI providers to architect a solution that can run reliably with existing IT and security infrastructure once the risks of a business endeavor are identified. For organizations that choose to architect and proactively manage a PKI solution, security becomes the enabler of functionality or productivity. If properly implemented, modern PKI can reduce the number of steps that end users must take to complete tasks requiring authentication. Once onerous security procedures that created friction among business users can largely be automated. Security considerations are often paramount following an audit finding, a data breach, or a security incident, and/or — as is often the case — to meet some regulatory compliance or company policy requirement. Today, organizations are adding on capabilities supported by PKI, such as multifactor authentication, encryption, and mobile enablement.

Some CISOs interviewed for this study were driven by the CIO to cut costs and support cloud-first initiatives and given budget to assess the state of their PKI infrastructure. They identified and documented PKI implementations that were beginning to buckle under the strain caused by rapid technology adoption and business growth. In some situations, the existing infrastructure at these organizations was poorly maintained because of the inability to attract and retain skilled IT security specialists. Some organizations maintained fragmented PKI implementations as a result of mergers and acquisitions or separate business units that demanded separate environments because of security or process restraints. The complexity challenges are nearly always compounded by the growing, distributed nature of corporate environment resources. IDC's *Data Services for Hybrid Cloud Survey* indicates that organizations continue to struggle with these issues. PKI was mentioned as a significant challenge by organizations and viewed as challenging as implementing and managing encryption or deploying and tuning data loss prevention platforms.

PKI USE CASES

The case studies in the sections that follow highlight how organizations are bolstering PKI to meet their specific requirements.

Digital Certificates Essential to Company's Mobility Strategy and Employees' Remote Access Requirements

A global electronics testing firm uses a mix of user and device certificates to grant user access to sensitive company resources on company-issued and employee-owned laptops and mobile devices. The result is a strong employee retention rate and an innovative engineering team, according to the CISO, who takes pride in using digital certificates to maintain a strong security posture while giving employees the flexibility to work comfortably.

"We decided that certificates were our best component to use for a variety of our use cases and because all our business partners have certificates for the VPN as do the users via mobile device management for BYOD," the CISO said.

The hardest work associated with PKI is getting trust chains installed and touching all the clients. There is no interoperability between the company's PKI implementations because neither the company's development and engineering teams nor the company's marketing and sales operations are interested in exploring interoperability. The company's operations depend on a separate trust chain for each PKI implementation, while a centralized approach may be more efficient and cost effective because only one trust chain has to be rolled out.

As part of the company's efforts to maintain strong security, the PKI implementation for mobile and VPN access is almost entirely customized for certificate profiles on the Microsoft side. To reduce the risk of stolen certificates and brute-force attacks designed to gain access to critical resources, the company developed a custom certificate tie. When users log in, they get only a password prompt and not a certificate prompt, which makes certificates work only for individual users. It is a one-to-one relationship to ensure that a certificate and a password would never work together. "That, in my mind, is a key essential security component of a certificate rollout," the CISO said.

PKI for Email Security, Authentication Bolsters Manufacturer's Security Posture

Cybersecurity for this global consumer product manufacturer had never been a significant priority. The lack of a reliable and effective way to authenticate employees accessing sensitive resources or validate the integrity of remote employees requesting access led to serious weaknesses that the company largely ignored. A disruptive ransomware outbreak in the form of SamSam malware finally got the attention of senior management at the manufacturer's parent company; investing in PKI to support email security and user authentication at the manufacturer was among senior management's first set of actions.

The attackers behind the SamSam malware easily identified and targeted a vulnerability associated with the company's file transfer protocol (FTP) servers and unleashed a brute-force attack against weak passwords to gain an initial foothold. The costly breach forced the company to shut down nearly all production, costing millions of dollars a day. Because there was no effective backup, employees assisted in recovering valuable intellectual property (IP) they had on paper, and some of the IP was restored from tape backup. To improve security infrastructure, the company committed to making large investments, including the use of PKI to secure email.

"I was hired to build a security program from scratch. They had policies in place but nothing beyond the policies," said the CISO, who came on board shortly after the attack to build a security program and raise the standards to the level of the manufacturer's parent company. "Our applications were not up to date, and our supporting security infrastructure was poorly configured or nonexistent. Once we got a good understanding of where our sensitive data resides, we felt like we needed to get the right tools in place, and that's why we re-architected our security infrastructure using modern PKI for user authentication and secured email across all our users regardless of their location or the device they are using."

The security team needed to ensure that future emails and data files being transferred were secure and worked with its parent company to roll out PKI as part of a migration from an outdated implementation of Lotus Notes to Microsoft Office 365. The company started with mandating two-factor authentication and used client certificates to eliminate weak passwords and validate the identity of all 1,300 Office 365 accounts, integrating PKI with Microsoft Active Directory Federated Services.

The company enabled S/MIME certificates, which can be used by default to support encryption and integrity by providing employee digital signatures, including the functionality to request a receipt for a

message when working with other internal employees, partners, or external collaborators. An email appliance scrubs inbound and outbound messages, and web proxies are in place to protect both email and web. This approach greatly increased the manufacturer's security posture because enabling S/MIME can prevent man-in-the-middle (MITM) attacks and provide an even higher benefit by encrypting critical intellectual property when necessary.

In addition to security tools, the company invested in training and awareness initiatives. "If it is restricted or highly restricted content they are dealing with, our employees know they have to use encryption, even if they are emailing someone else internally," according to the CISO.

The manufacturer's parent company worked with a PKI specialist to architect the implementation and tune it to avoid disrupting email. There were some enrollment issues and problems with existing security policies rejecting or quarantining encrypted traffic that disrupted email delivery, and the CISO pointed out that, in hindsight, more planning could have gone into managing the training program. "Employees accepted the new policies and changes to their processes because of the malware incident," he said. Today, the company continues to make gains in maturing its security program. It launched a data discovery and classification exercise and continues to roll out improvements to perimeter-based security around its on-premises assets.

PKI Used to Secure Modern Lending Experience and Integrate with Advanced Analytics

A major bank attempting to modernize its lending processes to boost customer experience turned to a managed PKI solution to protect its digitalized lending documents and ensure documents remained encrypted to meet compliance obligations. Security was a significant part of the investment and couldn't be a hindrance to the overarching goal of creating a dynamic and streamlined experience with new customers.

The bank evaluated security solutions that could bolster the business strategy of speeding up its loan processes from origination to close. The evaluation team sought PKI solutions that were flexible enough for deployment in the field and integrated with the existing back-end infrastructure. Employee churn in some areas required a solution that not only was easy to use and robust but also had a low footprint and good performance despite being integrated with multiple certificate authorities.

The bank had to design a solution that could parse unstructured content within the big data lake into structured content that supports the artificial intelligence engine running the virtual assistant. The bank had the resources necessary to invest in data scientists as well as a development team to take on this task. PKI solutions were the obvious choice to support the security of this data.

A PKI service was required to integrate with internal compliance software that monitors the onboarding of new clients. The security requirements also called for high availability, strong disaster recovery capabilities, and a dedicated instance of the PKI service to function within the bank's virtual private cloud. In addition, the PKI solution had to support the encryption of lending documents while integrating with the bank's content repository and an advanced analytics environment heavily used to support customer retention and enhance the bank's service offerings.

"Downtime was not an option and we needed assurance that we were in full control in owning the keys on our side," the CISO told IDC. "We know that PKI is the best way to solve our security requirements around highly critical assets. We've seen numerous improvements on the business side and, so far, it has instilled confidence in our ability to secure these critical transactions and meet our compliance obligations."

The implementation requires a server-side code base and leverages agents on the endpoints to meet encryption and digital signature requirements at document creation and submission. The entire workflow is monitored and logged across the web using the HTTPS protocol. Document authoring is done by employees at the endpoint, but the repository is on the server.

The bank's content repository and an advanced analytics environment is being integrated with a new virtual assistant designed to automate the process of getting borrower signatures and take the stress out of the lending process. Loan applications are no longer being scanned, printed out, and faxed. Once the PKI solution validates the borrower's identity, the borrower no longer needs to visit a branch office and sit next to a private banker or relationship manager to finalize the documents. An applicant can now conduct every step securely online from the comfort of his or her own home. Today, the solution scales to support up to 20,000 people, including legal personnel, risk and compliance officers, loan officers, customers, and others involved in the lending process.

"The implementation of the PKI solution requires careful planning," the CISO said. "Streamlining and centralizing your security infrastructure makes sense, but there are always political obstacles, including the risk of data exposure," he said. "If you put all your eggs into one basket, you might get hacked. What you must have for centralization is your user behavior analytics solution that cuts across all silos."

Regional Bank Upgrades to Managed PKI for Mobility and Expanded Verification Support

A large regional bank built out its PKI program over the course of many years, managing the infrastructure to support its internal certificate authority (CA), but it faced the growing struggle of recruiting skilled security professionals and training and retaining them to manage the security infrastructure. The complexity of managing a fragmented PKI program prompted some members of the security team to "run away," according to a lead security engineer at the bank interviewed by IDC.

The internal IT team struggled to manage multiple PKI implementations that hamstrung user authentication. Separate solutions had been designed over the course of nearly a decade to support smart cards, a solution for VPN and mobile device access, and a parallel system supporting email encryption and signing. The complexity of these separate solutions often disrupted end users because of an antiquated certificate issuance mechanism. The internal CA would fail to publish new access control lists, and people often couldn't authenticate to the network. There were multiple reasons why a failure could occur; sometimes it was a hardware failure with a hardware security module or a Windows server failure. "A lot of things can happen," a security engineer said.

"We feared that we got to the point where we could potentially bring down the network. If all our users can't get to certain applications or authenticate if PKI becomes unavailable, our team would be in hot water," the security engineer told IDC.

Today, the bank has eliminated complexity for mobile device and VPN users by integrating PKI with a modern mobile device management platform, streamlining credentials into a single mobile device smart card application monitored by a managed PKI service. "The IT team is slowly reducing the number of redundant systems starting by modernizing its device issuance processes and using smart cards more aligned with Active Directory," the security engineer said.

Turning to a managed PKI service has made life easier for the IT team as well. "With an all on-premises infrastructure and the level of security we were trying to reach came a lot of complexity and overhead that

we couldn't support with our staff," said the security engineer. "Unless you are in a large organization with huge teams, then managing your PKI program internally is probably not a venture for you."

In addition, the internal IT team is working with the PKI specialist to integrate certificate issuance with its smart cards and has also replaced a disjointed system in favor of a streamlined managed service to support secure email. The company manages its own Active Directory and continues to consolidate its processes for managing certificate authorities and publishing certificates. Since its smart card management platform is now integrated with certificate management, digital certificates are used to support VPN access. The adoption of managed PKI has greatly streamlined certificate life-cycle management at the 40 branches, freeing the IT teams from yet another task and providing an opportunity for them to focus on other projects.

High-Tech Manufacturer Chooses PKI to Support Device Identity and VPN Access and Achieve Zero-Trust Environment for Critical Assets

A provider of power management solutions locked down its environment by fully leveraging the built-in capabilities of the Microsoft Active Directory Certificate Services environment and mandating that managed devices be validated using device certificates and its PKI infrastructure. The goal was to lock down access to critical resources by establishing a method to validate the authenticity of users requesting VPN access into its environment and checking the health of managed devices before granting access to private network resources. The company wanted to ensure secure connectivity and speed up the process of getting users access to company resources regardless of their location. Using digital certificates tightly controls employees by requiring a fully managed endpoint to access critical resources and can restrict contractors and business partners by issuing user authentication certificates set to restrict access and apply firewall rules as necessary.

"Our defense posture is built around being incredibly difficult to extract keys off the Microsoft devices," said the company's CISO, who added that the manufacturer is making phased investments toward achieving a "zero trust" environment. The challenge of managing this is compounded by an ongoing rollout of Macs on its network for engineers, marketing, and other special use cases. The company is working with a PKI specialist to architect a way to deploy an authentication certificate to the Macs and ensure the private key is stored securely and can't be exported.

As the company's rollout continues, it will add metadata in newly issued certificates to allow device fingerprinting. Certificates will be leveraged as part of the authentication process and VPN connectivity to its on-premises web access management platform. The company likes the flexibility of the platform, which enables employees to access a portal containing Office 365 and other company resources from their mobile devices.

The company's chief security architect provides a word of caution over certificate-based authentication on mobile devices. "Just because the company can get a certificate on a device doesn't mean that everything on that device is capable of interacting with the certificate. If the application developer hasn't written the application in a way that can leverage a generally deployed certificate on a device, the application will never use it," he said. The application might not be able to receive the certificate from the device that has the certificate on it. As a result, the company is working out a new strategy for cloud identity that supports both apps developed internally and third-party apps that employees consume.

Payment Processor Secures Thousands of POS Devices Using PKI

Manufacturers are under increased pressure to add hardware-based and software-based security mechanisms to Internet of Things devices to support encryption, authentication, and authorization and validate the integrity of the device firmware, operating system, and applications. Digital certificates are the trust anchors used to achieve this foundational level of security on embedded systems.

A payment processor in Europe is securing tens of thousands of POS system devices using a managed PKI service that enables trusted, third-party, mutual authentication of devices to networks. The new approach developed by the payment processor requires the installation of digital certificates for device identity and a device agent that can communicate to the payment processor's cloud-based platform; the platform is used for provisioning, monitoring, and maintaining the POS systems and establishing a secure mechanism to rotate certificates.

A security architect who oversees the implementation said the use of digital certificates reduces fraud at the manufacturer level and gives his company more oversight into device use. "PKI was chosen because certificates can be managed throughout the entire life cycle at volumes that can scale," he said. "A key requirement was the establishment of a solution that couldn't be hijacked by an attacker using fraudulent digital certificates," according to the security architect. The mechanism developed ensures that data at rest or in transit is secure and validates that the entities sending and receiving information are who they claim to be.

In addition to maintaining oversight of device provisioning and credential management over the POS systems, the solution enables the provider to sell policy-driven encryption services and ensures that merchants are meeting compliance obligations.

Other high-risk devices used by the provider do not support an agent approach. An embedded systems manufacturer that works with the payment processor and others ships products that don't have the space or power to support an agent or client software. The manufacturer told IDC that its engineering team uses PKI when it is produced to support secure machine-to-machine communication and code signing. "Our customers required us to establish a practice to ensure the integrity of any code we ship to our customers," according to the security team lead who worked with the engineering team. The goal was to choose a managed PKI solution rather than incorporate it into the manufacturer's existing PKI implementation.

"We've been looking for ways to automate the process without burdening the team focused on our internal processes," he said.

CONSIDERING DIGICERT

DigiCert is a provider of TLS/SSL, IoT, and PKI solutions for identity and encryption. DigiCert's approach to modernizing PKI management, DigiCert ONE, offers multiple management solutions and is designed for multiple PKI use cases. It can be deployed on premises, in country, or in the cloud to meet compliance requirements, custom integrations, and air gap needs. DigiCert Enterprise PKI Manager, built on top of DigiCert ONE, is designed for the management of device identity, authentication, encryption, and integrity.

Enterprise PKI Manager gives organizations the ability to:

- Enable API-based automated device and user enrollment with digital certificates.
- Integrate with leading MDM/UEM platforms for secure device enrollment and management.

- Secure emails with authentication and encryption via S/MIME certificates.
- Enable secure document signing across the organization's physical and virtual network environments.
- Integrate with the other DigiCert ONE workflow managers for secure code signing for software and IoT device security.

CHALLENGES/OPPORTUNITIES

Organizations have made long-standing investments in their existing PKI infrastructure. The security professionals interviewed by IDC said the process of streamlining and automating the often complex and fragmented PKI ecosystem they are trying to maintain is a multipronged, multiyear endeavor. This effort requires an up-front investment and PKI specialists who are knowledgeable about the organization's existing business processes and IT infrastructure, the location of critical resources, and management's existing risk tolerance and growth strategy. Rapid growth, mergers and acquisitions, the adoption of new technology, business strategy changes, and other external factors can heavily impact and even derail improvement projects if they are not adequately planned and systematically executed.

CONCLUSION

Given the continued increase in cloud adoption and the number of organizations managing access to data and other corporate resources across hybrid and multicloud environments, PKI technology will be increasingly relied upon to play a key role in validating the integrity of business transactions and establishing a secure and trusted connection between humans and systems. IDC's *Data Security Survey,* 2020, validates this. In 2020, over 95% of organizations with more than 5,000 employees indicated that they were encrypting data at rest in public IaaS and PaaS environments. The key findings that suggest why PKI has grown in importance are as follows:

- **Scalability:** The interviewees represented in this study leveraged PKI at considerable scale and size, providing us data on the size of their user base, number of domains, and volumes of authentication requests. These IT organizations dealt with considerable requirements for scaling. The corporate respondents ranged in size from 1,000 employees to 120,000 employees, and all expressed satisfaction with performance and viability and felt confident that they could continue to grow using PKI technology for their future needs around mobility, remote access, secure wireless connectivity, document signing, encryption, and secure email.
- **Managed PKI services:** Existing problems and concerns were associated with multiple implementations of PKI technology, creating complexity as well as a lack of skilled network and security engineers to manage the complexity. This is fueling adoption of managed PKI services to augment existing personnel and limit disruption by automating common PKI activities, such as onboarding new employees and certificate issuance and revocation.
- **Attacker sophistication:** Interviewees stated that when PKI is integrated and "not broken," their IT teams frequently say they don't want to mess with it. But it is clear that increased complexity and a lack of proactive oversight result in vulnerabilities and configuration issues that attackers can seize upon. By taking advantage of configuration weaknesses, attackers can conduct a man-in-the-middle attack to surveil specific employees or, a more likely scenario, steal sensitive data for financial gain.

This IDC study found that PKI is essential in securing digital transformation initiatives across a variety of business and use cases. Today's business processes can be supported by PKI to increase automation, reduce friction, and streamline the processing of digital information and electronic transactions. PKI is also an essential element used by security teams that face new data privacy and data security regulations. CISOs agree that streamlined PKI implementations reduce complexity and that the option of adopting managed PKI services can reduce management overhead and costs, freeing up security teams to work on other pressing matters. In addition, this study validated that digital certificates are essential components that can thwart targeted attacks and assist in ensuring the integrity of sensitive transactions and that the parties involved in business transactions are who they say they are. Even more importantly, this study found that PKI is used as an enabler of new business projects designed to improve customer satisfaction by allowing customers to securely conduct sensitive transactions from the comfort of their homes.

MESSAGE FROM THE SPONSOR

DigiCert is a leading provider of scalable TLS/SSL, IoT and PKI solutions for identity and encryption. The most innovative companies, including 89% of the Fortune 500 and 97 of the 100 top global banks, choose DigiCert for its expertise in identity and encryption for web servers, enterprise and Internet of Things devices. The company is recognized for its enterprise-grade certificate management platform, fast and knowledgeable customer support, and market-leading security solutions. For the latest DigiCert news and updates, visit digicert.com or follow @digicert.

About 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. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com