ENCRYPTION CONSULTING

Encryption Consulting PKI & IoT Trends Survey - 2023

A study on global usage trends on Public Key Infrastructure (PKI) and Internet of Things (IoT) along with their application possibilities.

Contents

Study Background

Digital certificates have become an essential part of the encryption landscape. As the use of cloud applications and IoT devices continues to grow, ensuring the security of sensitive data has become a major concern for companies. Public Key Infrastructure (PKI) offers a solution by providing crucial authentication and security for these technologies. According to the International Data Corporation (IDC), by 2025, there will be more than 41 billion IoT devices connected across various sectors and generating approximately 80 zettabytes of data. The International Data Corporation (IDC) predicts that by 2023, there will be an even greater number of IoT devices connected across various sectors, generating an even larger amount of data.

With this in mind, this study will focus on the global trends and usage of PKI in various industries and organizations for the year 2023. The research will include a sample of participants from countries all around the world.

This report's primary focus is on the analysis of the findings based on the survey conducted among professionals working in cyber security domain across various organizations around the globe.

Survey Demographics:

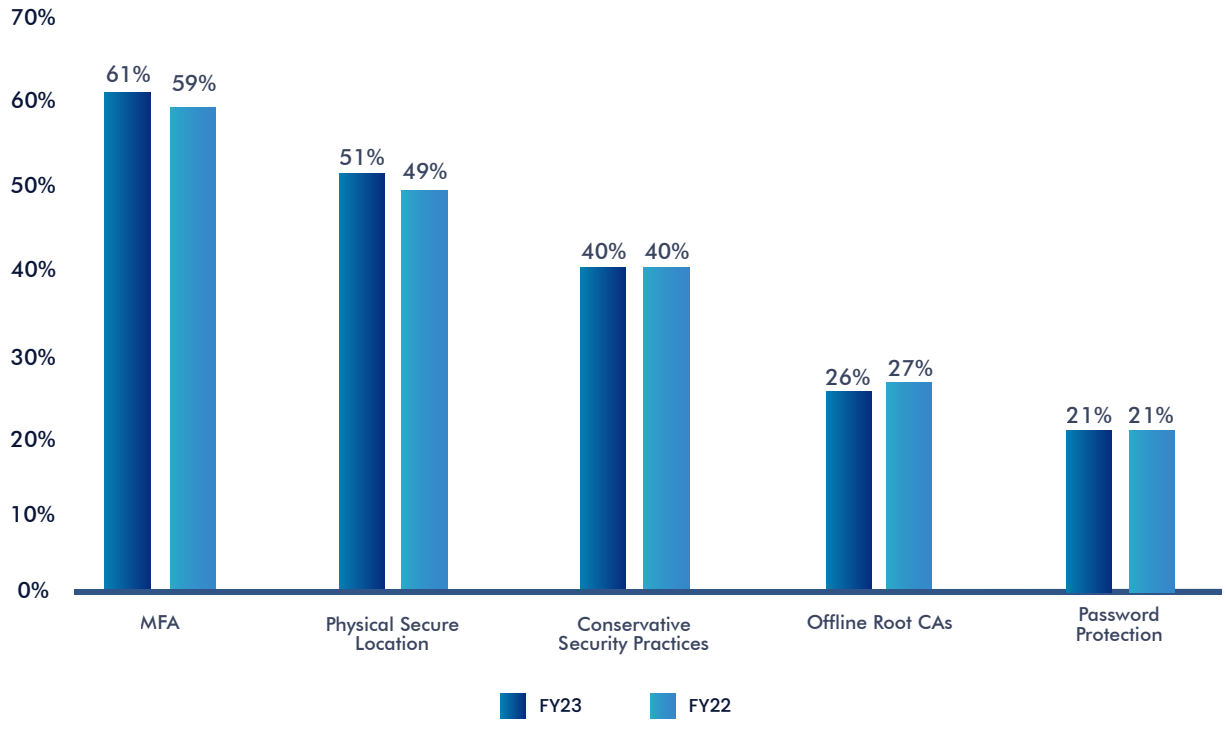
Some of the countries that participated in the encryption consulting survey are: United States, Germany, Japan, Korea, Brazil, France, Hong Kong, and Southeast Asia to name a few. Proper precaution is taken to include various demographics in the survey to get an unbiased opinion on the PKI trends.

Study Background

The survey focus is on practices used to secure Public Key Infrastructure (PKI) and Certificate Authorities (CAs). About 61% of the respondents are leveraging multi-factor authentication for protecting their infrastructure. This is a 2% increase from FY22. This is followed by physical security which is about 51% and then conservative security methods which are documented. The trend remained the same compared to last year i.e. about 40%. Offline root CAs again went into a declining trend compared to 2022 and fared at 26%. Similarly, usage of traditional password protection also remained the same as last year from 21% in FY22.

This survey report primarily focuses on the impact and influence of cloud computing, the Internet of Things and major industry trends on the cyber security and its best practice in FY23. Employees/personnel who are directly involved in management and maintenance of PKI and its applications were selected as participants for this survey as it creates more authenticity for the report.

Fig. 1 - Practices used to secure PKI and Certificate Authorities



Key Findings

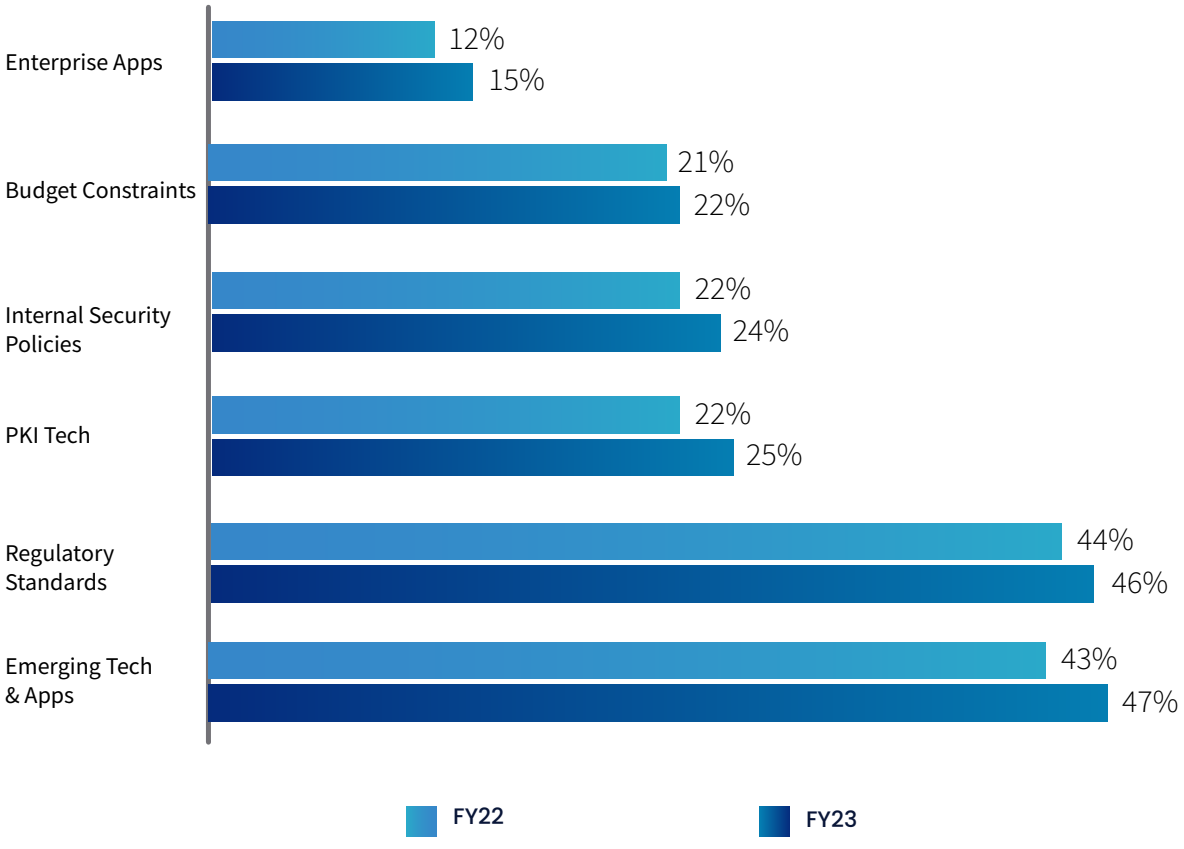
In this section, we focus primarily on the analysis of global PKI trends survey results over the spread of years.

PKI Management Complexity

The next survey question focuses on the areas expected to experience the most uncertainty in FY23. As it is evident, emerging technologies and applications such as IoT contribute to the majority of the uncertainty with more than 40% of the respondents choosing this option in FY23 followed by "Regulatory Standards". Budget constraints are the constant choice opted across the years with around 20% voting. Other major influencing factors are PKI technologies and enterprise applications showing a constantly increasing trend over the past three years.

Fig. 2 - Areas expected to experience the most change and uncertainty

Multiple responses permitted per user



The significance of Internal Security Policies increased from 22% in FY22 to 25% in FY23.

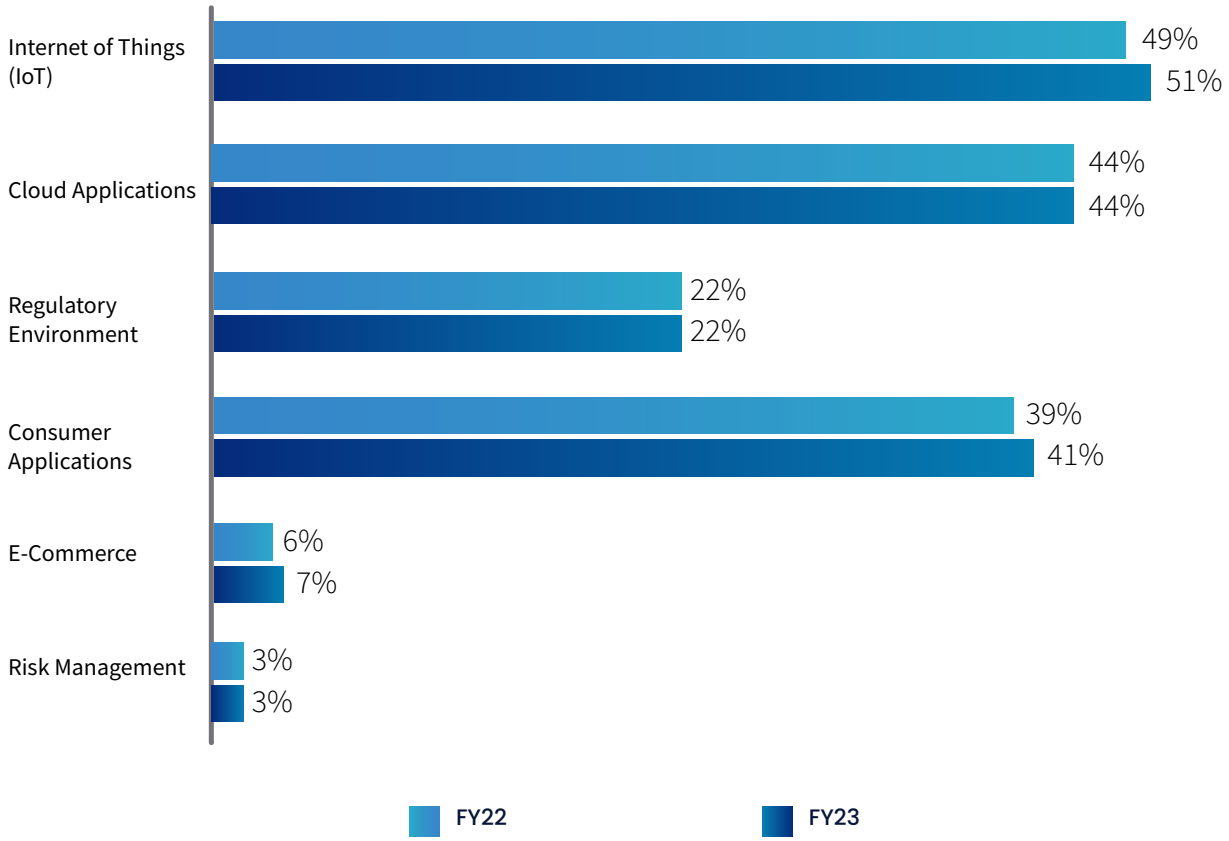
What are the major factors impacting the deployment of PKI applications?

The Internet of Things, which is the current fast-growing trend, is a major factor chosen by 51% of the respondents.

This is a 2% increase from FY22. Major factor for this trend would be the trust placed on PKI in providing the core authentication for IoT devices. This also suggests the increasing adoption of Internet of Things by various sectors across the globe. On contrary, cloud-based services stayed at the same percentage as last year i.e. 44%. Regulatory environment remained a constant factor compared to last year with 22%.

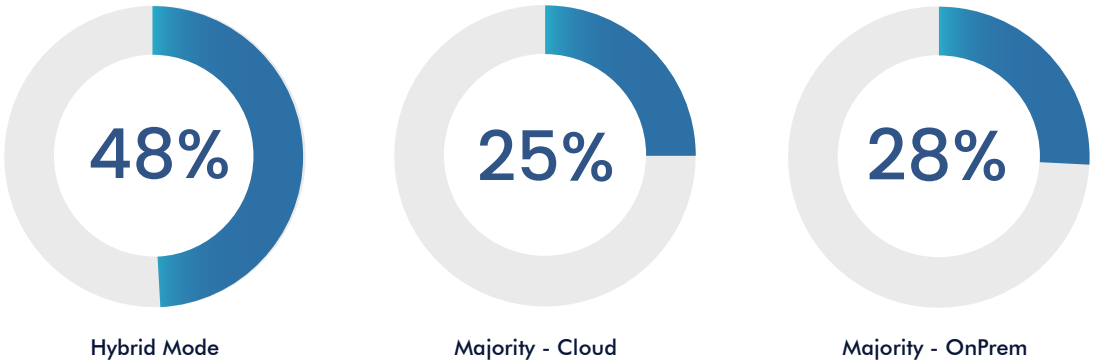
Fig. 3 - The most important trends driving the deployment of applications using PKI

Consolidated view – two responses permitted



Internet of Things is prospected to popularize in the digital space. Public Key Infrastructure is also expected to play a crucial role in this space in FY23. Responses from the firms that participated in the survey confirm the same. IoT devices are spread across locations and firms are leveraging. Digital certificates to protect the devices connected through IoT credentialing. Figure 4 projects the percentage of respondents opting for IoT credentialing categorised by the type of deployment of devices.

Fig. 4 - Types of PKI deployment for IoT credentialing

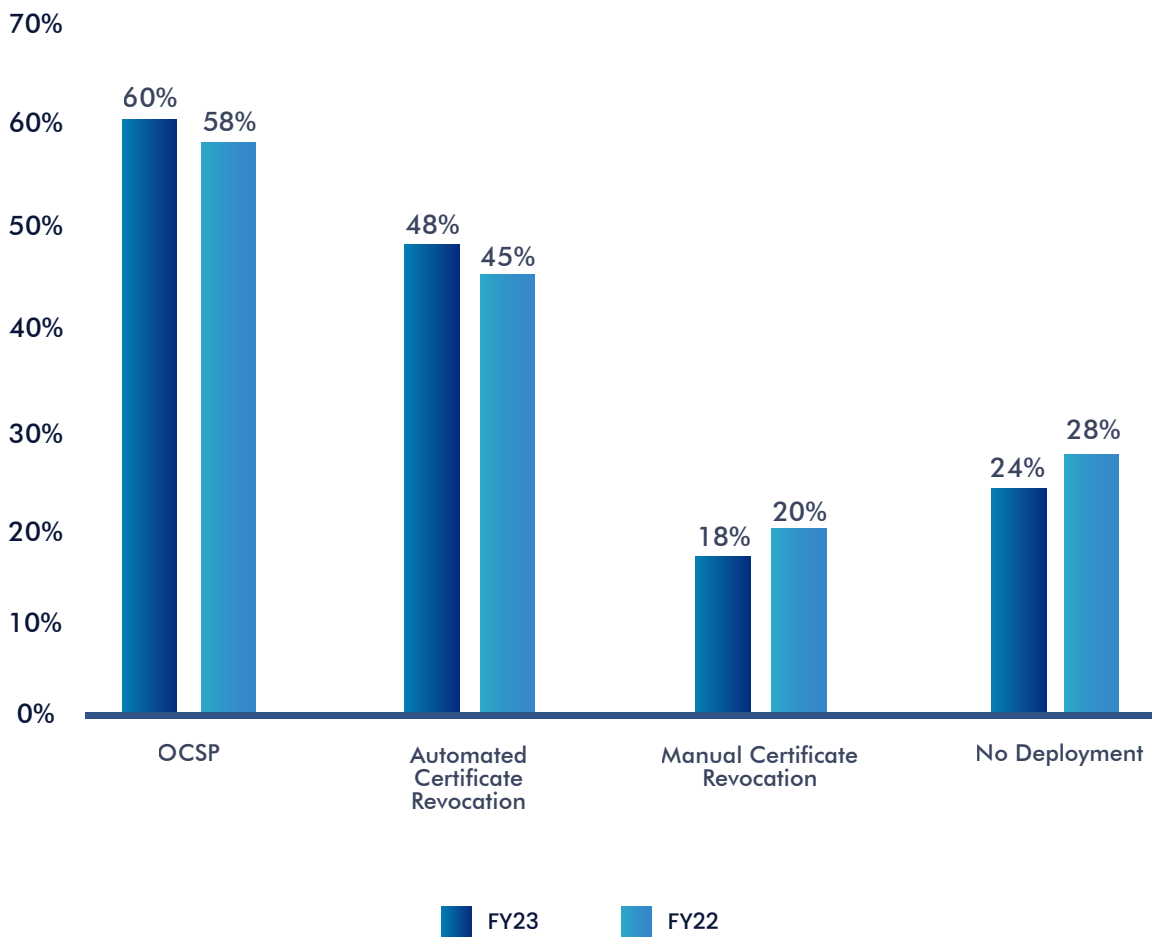


PKI - Certificate Revocation

Certificate revocation is a critical component of Public Key Infrastructure (PKI) technology, where certificates are validated and revoked as necessary. As shown in Figure 5, the majority of respondents favor using the Online Certificate Status Protocol (OCSP) for certificate revocation. About 60% of the respondents are leveraging OCSP for revocation.

According to a survey, 48% of respondents stated that automated certificate revocation lists are the next most popular technique. This represents a 6% increase compared to the previous year. Notably, 24% of respondents indicated that they do not utilize any certificate revocation mechanisms. However, this trend appears to be decreasing year over year.

Fig. 5 - The certificate revocation techniques used in enterprises



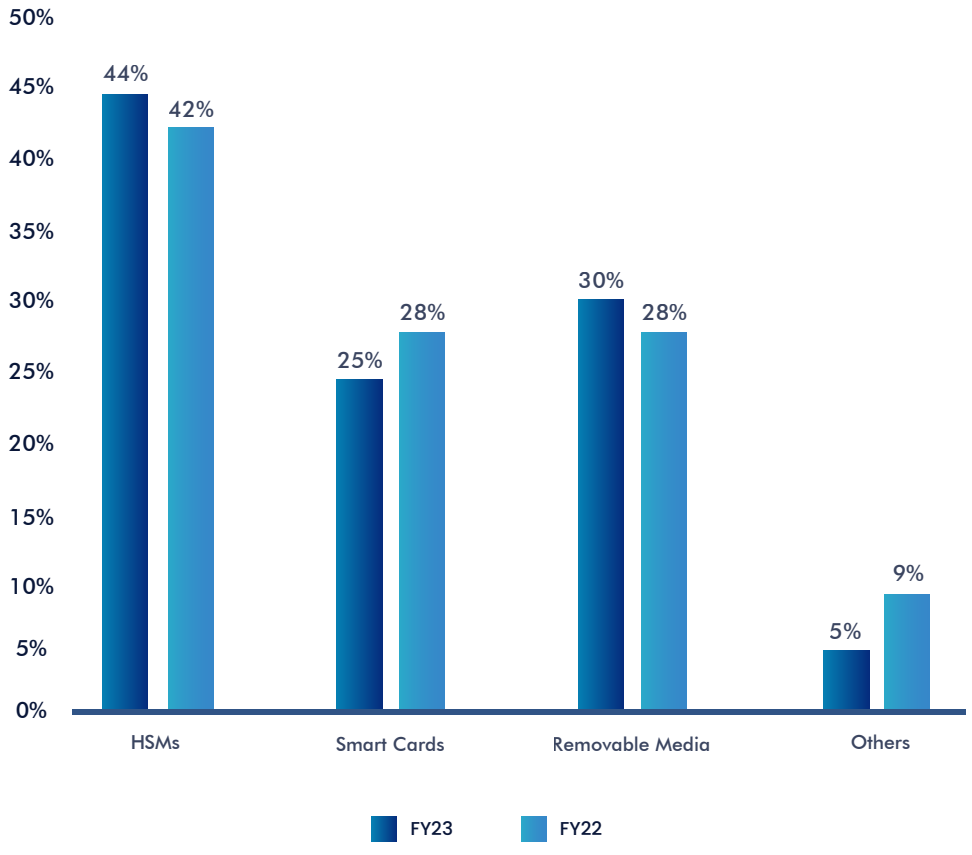
60%

of the total respondents mentioned that OCSP: Online Certificate Status Protocol is being leveraged for the certificate revocation process.

Most of the respondents favored Hardware Security Modules (HSMs) for managing their root/policy CA private keys. Figure 6 indicates the responses from the participants and around 44% chose HSMs.

Around 25% prefer smart cards for CA key protection. There is a 3% decline compared to FY22. Removable media for CA key management is an equal contender as smart cards with about 28% voting.

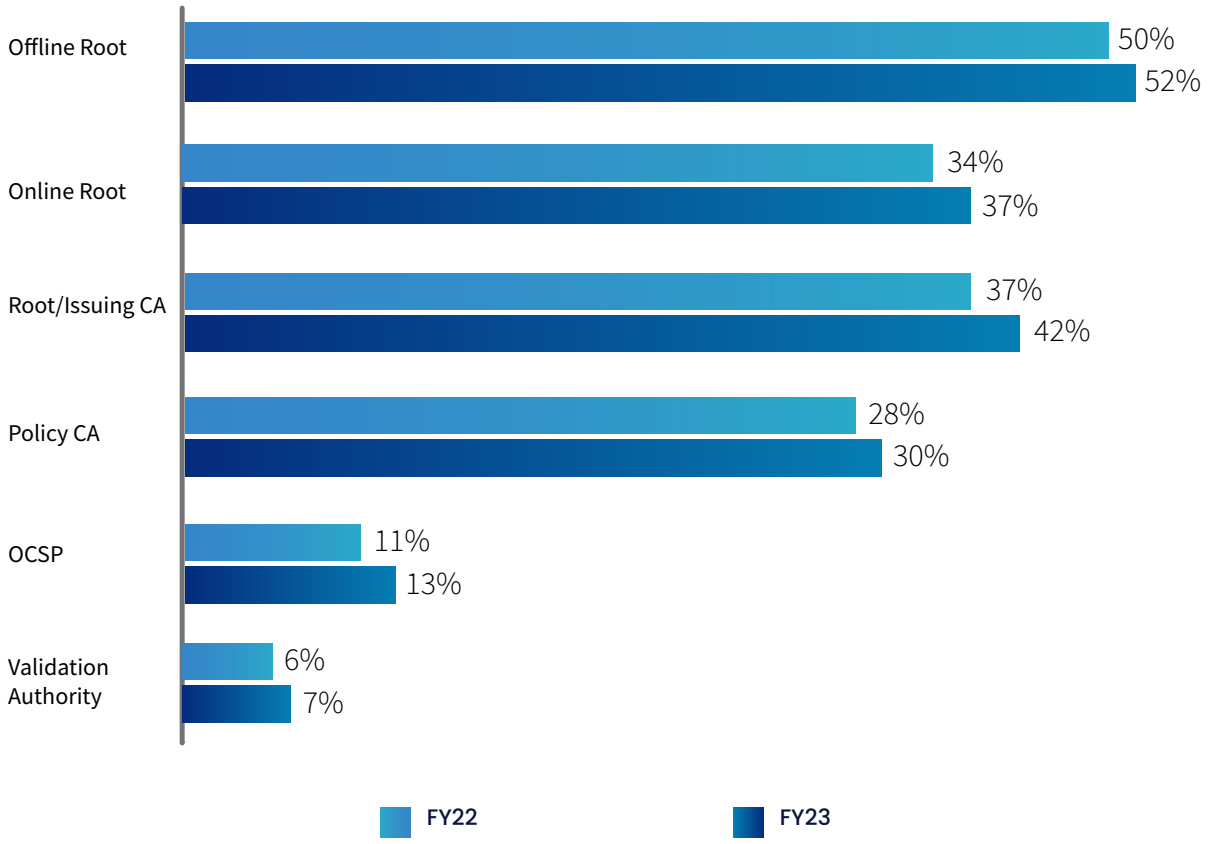
Fig. 6 - Private Key Management for Certificate Authority (CA)



As evidenced by the data presented in Figure 6, Hardware Security Modules (HSMs) are widely considered to be the most effective means of safeguarding the private keys of various Certificate Authorities (CAs). In order to gain a deeper understanding of the utilization of HSMs within organizations, a survey was conducted to determine where they are deployed to secure Public Key Infrastructure (PKI) across the organization. The results of the survey revealed that a majority of the organizations surveyed, 52%, reported that they utilize HSMs in offline CA to protect their keys, while only 34% indicated that they use HSMs with Online CAs. This represents a significant disparity between the two types of CAs. A noteworthy revelation from the survey was that organizations demonstrated a lack of interest in deploying HSMs in OCSP responders, despite this being widely recognized as a best practice by numerous industry standards and frameworks globally. Furthermore, the survey participants were found to be least inclined towards deploying HSMs in validation authorities, as evidenced by the 6% response rate.

Fig. 7 - PKI security through HSMs deployment

Multiple responses permitted

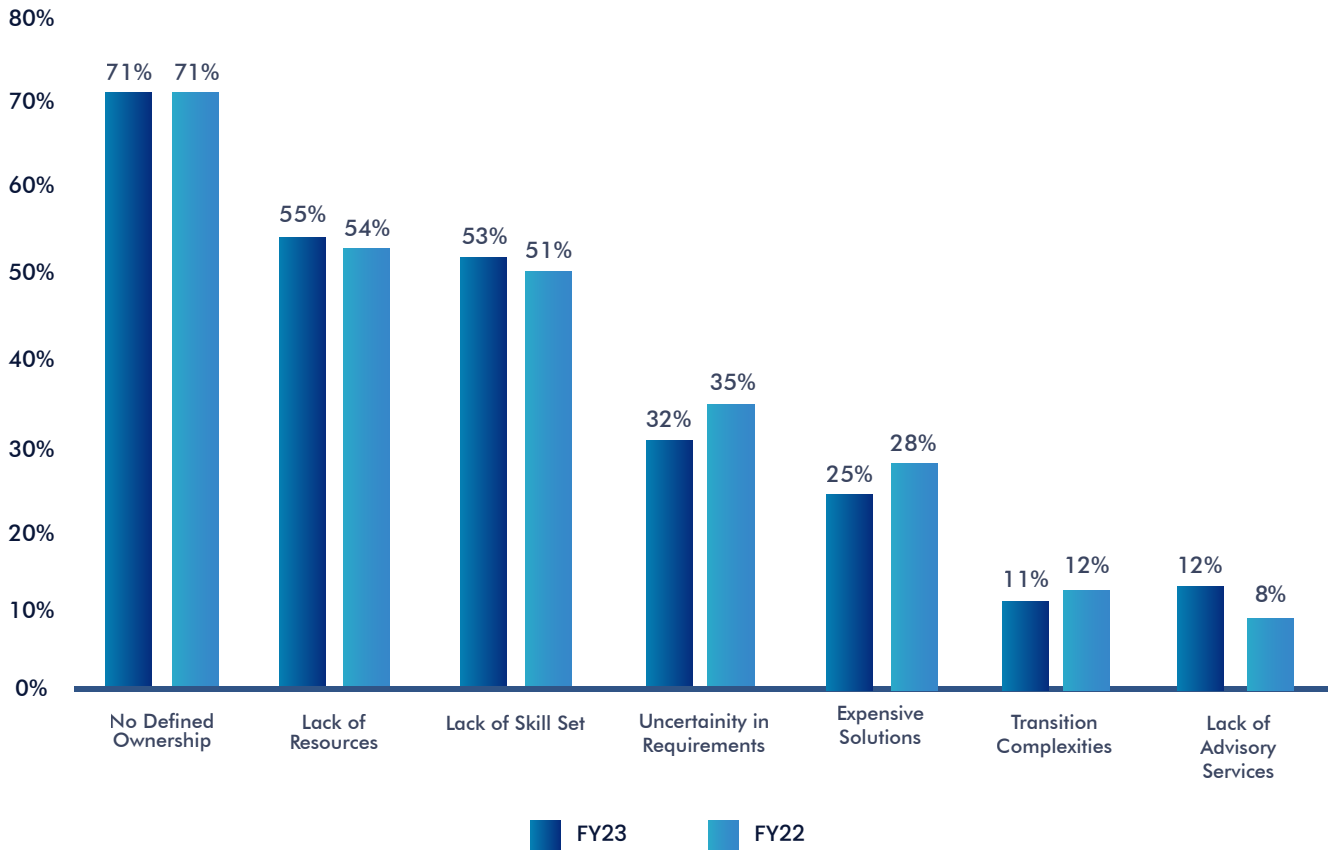


PKI Deployment Challenges

There are several challenges in deploying and managing Public Key Infrastructure in any organization. This survey question focuses on understanding several challenges faced by organizations in deploying PKI. The top challenges are no defined ownership and lack of skill-set among the employees as majority voted for these two options.

No defined ownership stayed constant at 71% in FY23. Lack of skill set and resources were chosen by 53% & 55% respondents. This clearly indicates the complexity involved in PKI. Uncertainty in understanding the requirements has seen a decrease of 3% from 35% to 32%. This trend indicates that organizations are looking for consulting firms with knowledge and expertise in PKI.

Fig. 8 - The challenges in deploying and managing PKI



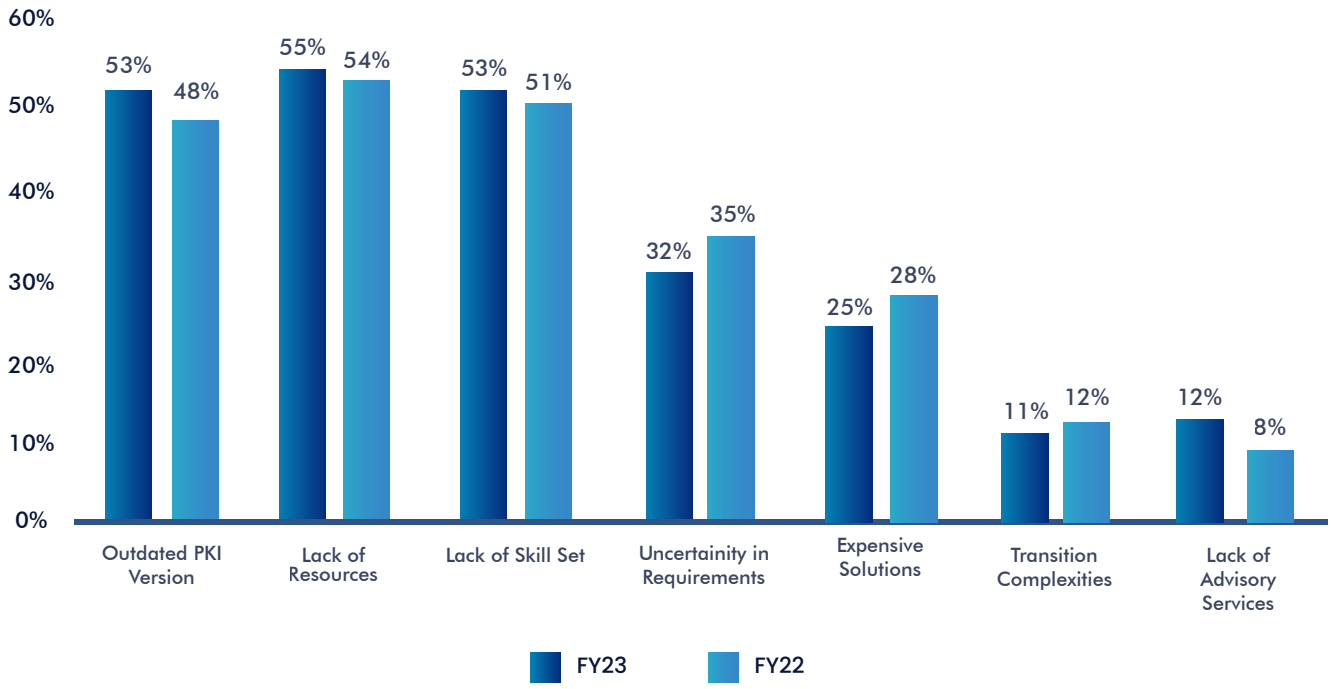
PKI Compatibility with Existing/New Applications:

There are various factors that contribute to the mismatch between PKI and an organization's applications. One of the primary reasons cited by organizations is the lack of necessary upgrades to existing PKI infrastructure, with 55% of respondents indicating this as the primary cause. Another significant contributor is the absence of the required technical expertise, which has risen from 46% in the fiscal year 2022 to 48% in fiscal year 2023.

In addition to the aforementioned challenges, uncertainty regarding necessary requirements and complexity in migrating legacy applications are also significant obstacles. These were cited by 36% and 44% of respondents, respectively. Our analysis suggests that, aside from organizations with a strong understanding of encryption, many respondents are willing to engage the services of consulting firms for their PKI expertise.

Fig. 9 - PKI compatibility with existing/new applications

Multiple responses permitted

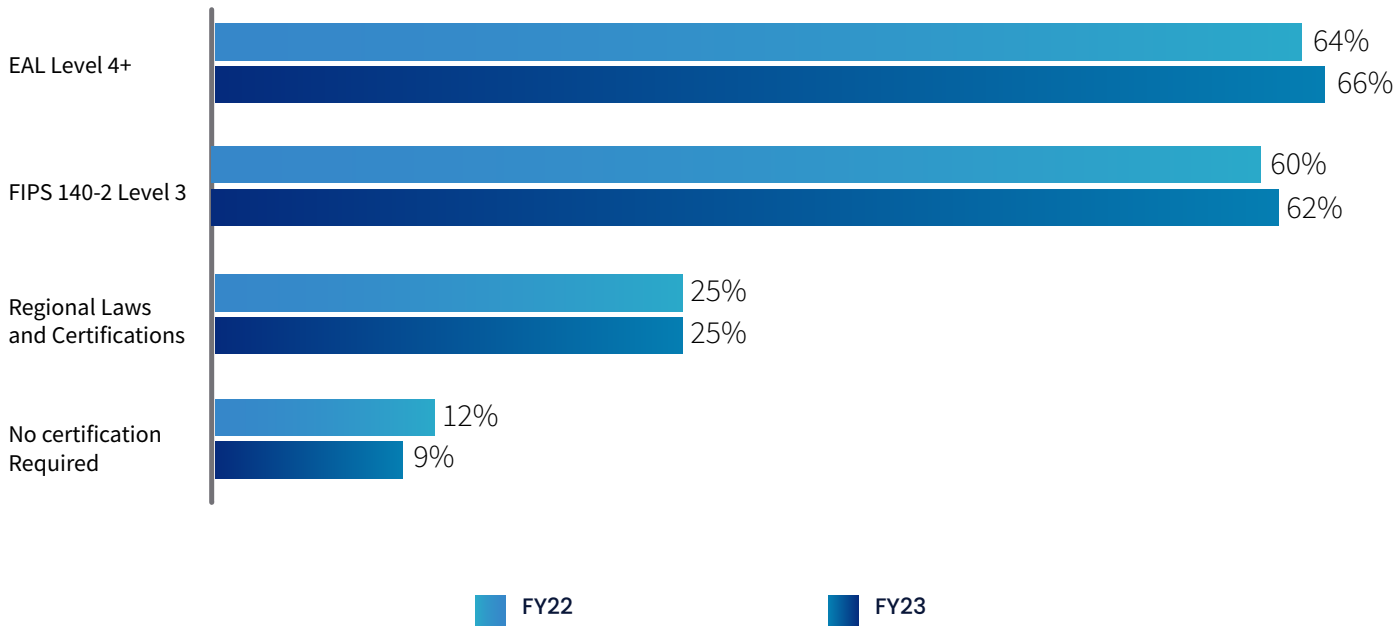


Certifications Considered Important For PKI:

It is evident from the previous survey responses that organizations are finding it more difficult to identify appropriate and skilled resources on PKI technology. Figure 11 depicts the responses from organizations on their understanding of PKI certifications either by their own resources or by consulting firms. The majority of the respondents believed that common criteria EAL Level 4+ is the most critical certification required for PKI deployment. About 66% of the respondents voted for this option followed by FIPS 140-2 level 3 which gave a tough competition with 62% selecting this certification.

Around 25% of the respondents trust the local laws and regulations for the certification guidance on PKI. This includes regional digital signature laws and certifications. A minor share of respondents (8%) believes there is no certification necessary to handle PKI. One strong observation is organizations are in search of skilled consulting firms with adequate certifications for handling their PKI.

Fig. 10 - Security certifications important when deploying PKI infrastructure

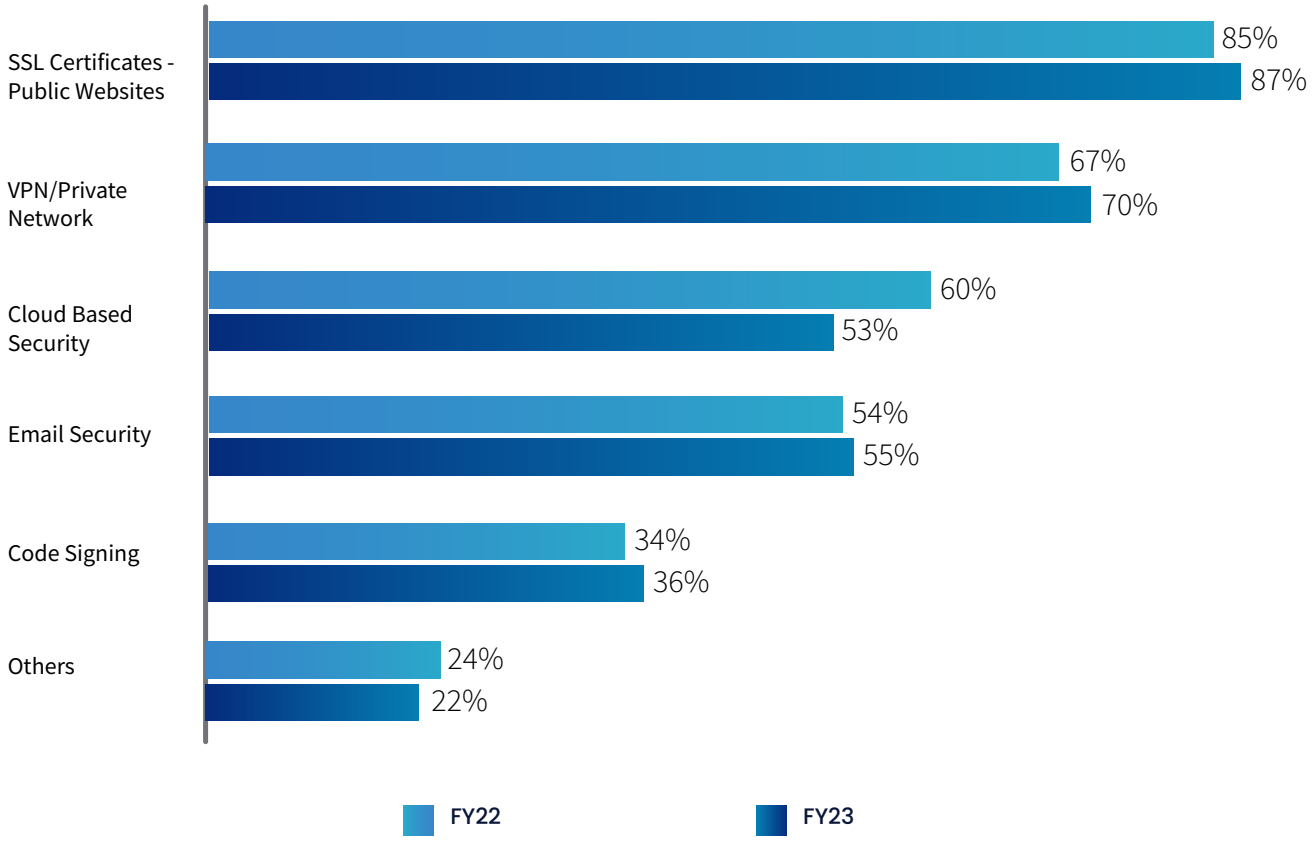


Where is PKI used?

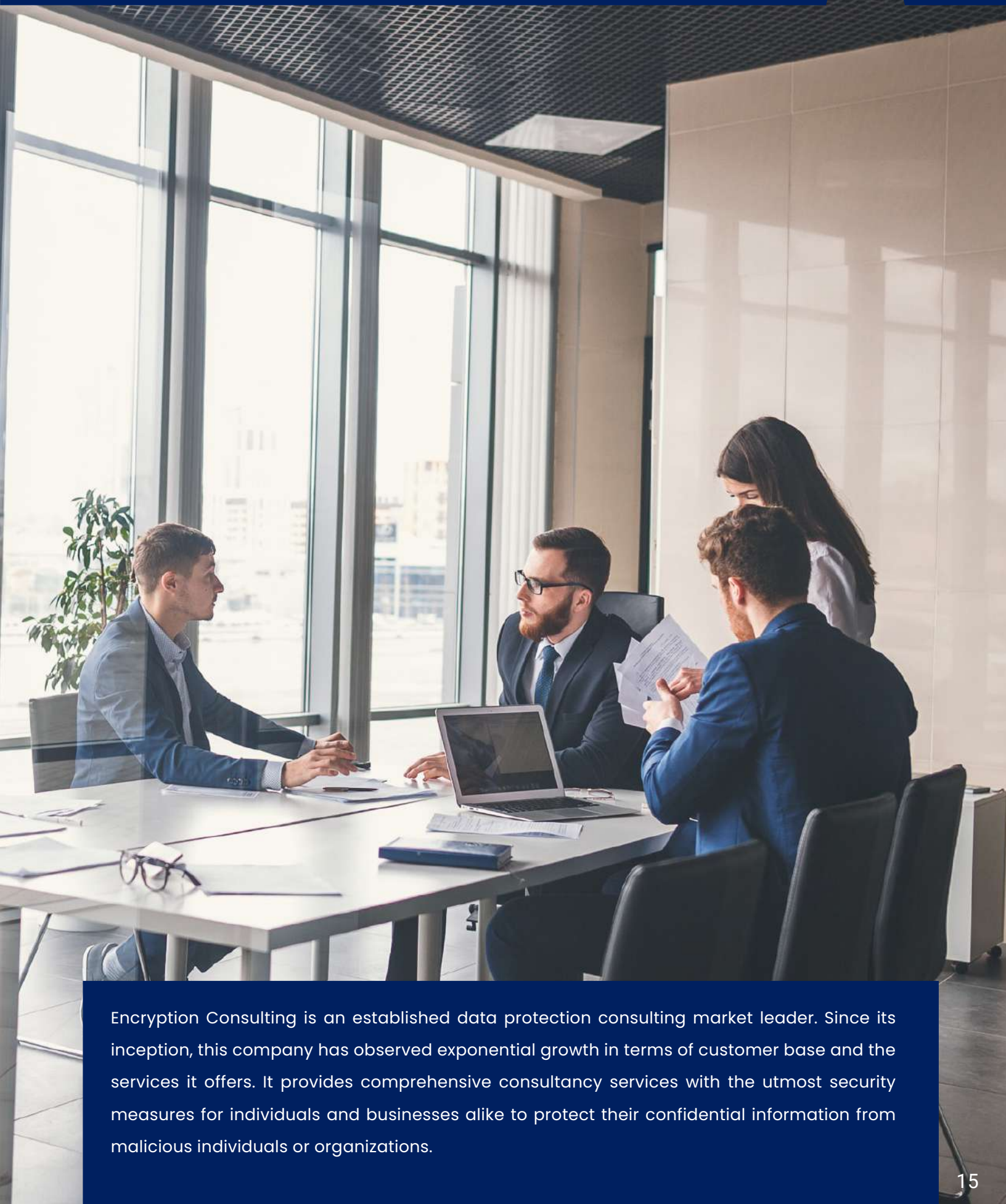
Figure 12 represents the responses from organizations on the major applications where PKI is deployed. PKI is extensively used for Public websites – SSL certificates. More than 87% of respondents mentioned that SSL certificates signing for public facing websites is the primary usage of PKI.

Enterprise user authentication and Cloud based services has seen an increase in usage of PKI. Percentage increased from 53% to 60%. VPNs/Private networks has seen a good increase in usage of PKI in FY23 and this might be attributed to increase in work from home culture due to pandemic. The increase is seen from 67% to 70%.

Fig. 11 - What applications use PKI credentials in organizations?



About Encryption Consulting



Encryption Consulting is an established data protection consulting market leader. Since its inception, this company has observed exponential growth in terms of customer base and the services it offers. It provides comprehensive consultancy services with the utmost security measures for individuals and businesses alike to protect their confidential information from malicious individuals or organizations.

Strategic Technology Partnerships

We work with the industry's best technology providers and have broad experience deploying, managing, and integrating our integrating our solutions with their products and services. We also pride ourselves on our flexibility and are always open to help our clients achieve their data security success with the technology of their choice. If you have products and services already deployed or are considering, we'd be glad to help you evaluate these to get the most out of your investment.

nCipher Security, a leader in the general purpose hardware security module market, is now an Entrust Datacard company, delivering trust, integrity and control to business critical information and applications.

Thales-e-Security is a leader in encryption, advanced key management, tokenization, priveleged user control and meets the highest standards of certification for high assurance solutions.

Fortanix is a leader in runtime encryption and it protects applications even when the infrastructure is compromised.

Keyfactor has its roots in the trenches of IT security, deployment and operations. We understand how companies work because of our deep industry experience - we know firsthand the challenges of competing agendas, budget constraints and time pressures.

Microsoft Corporation is an American multinational technology company with headquarters in Redmond, Washington.

Micro Focus and HPE Software have joined to become one of the largest pure-play software companies in the world.

Cryptomathic is a global provider of secure server solutions to business across a wide range of industry sectors, including banking, government, technology manufacturing, cloud and mobile.

For those shaping the digital interactions of tomorrow, we provide the digital security that enables the trusted connections of today.

Fornetix Key Orchestration TM is a scalable and Aexible solution designed to simpligy key management. Granular ploicy tools, user access controls, and powerful automation enable organizations to manage hundreds of millions of encryption keys while integrating seamlessly with existing technology investments.

AppviewX is revolutionizing the manner in which NetOps and SecOps team.

PrimeKey's technology is used by organizations and enterprses to securely implement PKI solutions used for ePassports, eBanking, ePayment, mobile/Internet security, IoT and more.

Unbound protects secrets such as cryptographic keys, credentials or private data by ensuring they never exist in complete form.

Venafi Cloud helps organizations prevent outages and secure their keys and certificates.

Prime Factors software products help business leaders implement and manage enterprise-wide data protection policies to secure sensitive information being used by or stored in virtually any application or system.

Utimaco is a leading manufacturer of Hardware Security Modules(HSMs) that provide the Root of Trust to all industries, from financial services and payment to the automotive industry, cloud services to the public sector.

The Only Data-First Security Solution. Protect sensitive enterprise data at rest, in motion, and in use with Protegrity's best-in-class data discovery, de-identification and governance capabilities.

Secure your data, minimise risk, and meet compliance and regulation requirements. Find out more about Comforte's Data Security Services.

Why Encryption Consulting LLC?

ENCRYPTION CONSULTING

Encryption Advisory Services

Encryption is used for securely protecting data from unauthorized accees. Data encrypted can only be seen by those that possess the key to change the data back to plain text. Encryption is now one of the oldest yet still most effective technology solutions able to have data security for organizations.

Public Key Infrastructure

PKI is a security ecosystem that has stood the test of time for achieving secure Internet-based transactions by the use of digital certificates. Digital certificates that provided security to servers and routers from the very early stages of the Internet through Public Key Infrastructure.

Hardware Security Module - HSM

Hardware Security Modules provides protection and strong authentication with cryptographic processing by the use of digital keys inside a physical computing device. This device offers an isolated tamperproof environment which can create and secure cryptographic keys, protecting critical cryptographic operations, all while enforcing self-implemented policies over the keys.

Certificate Lifecycle Management

Certificates typically have a 4-phase lifecycle -Discovery, Enrollment, Provisioning, and End-of-life. To make your PKI mature and reliable, you must have more control over all the phases.

Enterprise Encryption Platforms

Does your business have the need to encrypt large amounts of data-at-rest found in structured databases or in unstructured files across physical, cloud, or both types of environment? Do you want to protect data without disruptive changes to applications or business practices?

Cloud Data Protection Services

The transition towards uploading data on the public cloud is now becoming the normal standard. With relying on the cloud for data storage, cloud security must now become the number one priority for organizations.

See it in action

Encryption Consulting LLC is a customer-focused cyber security consulting firm providing an array of services in all aspects of data protection.

Contact Us

encryptionconsulting.com

linkedin.com/company/encryptionconsulting

facebook.com/encryptionconsulting

twitter.com/encryptioncons