ENCRYPTION CONSULTING

ENCRYPTION CONSULTING PKI & IoT TRENDS SURVEY - 2022

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

A. Introduction

STUDY BACKGROUND:

Digital certificates are becoming a necessity in today's encryption landscape. With the increase in regular usage of cloud applications, Internet of Things (IoT) security became the top most concern for the companies with high critical data. Public Key Infrastructure (PKI) solves this concern as it provides core authentication and security for these technologies. International Data Corporation (IDC) predicts by 2025 there will be 41bn+ IoT devices connected to various sector & generate about 80 zettabytes of data.

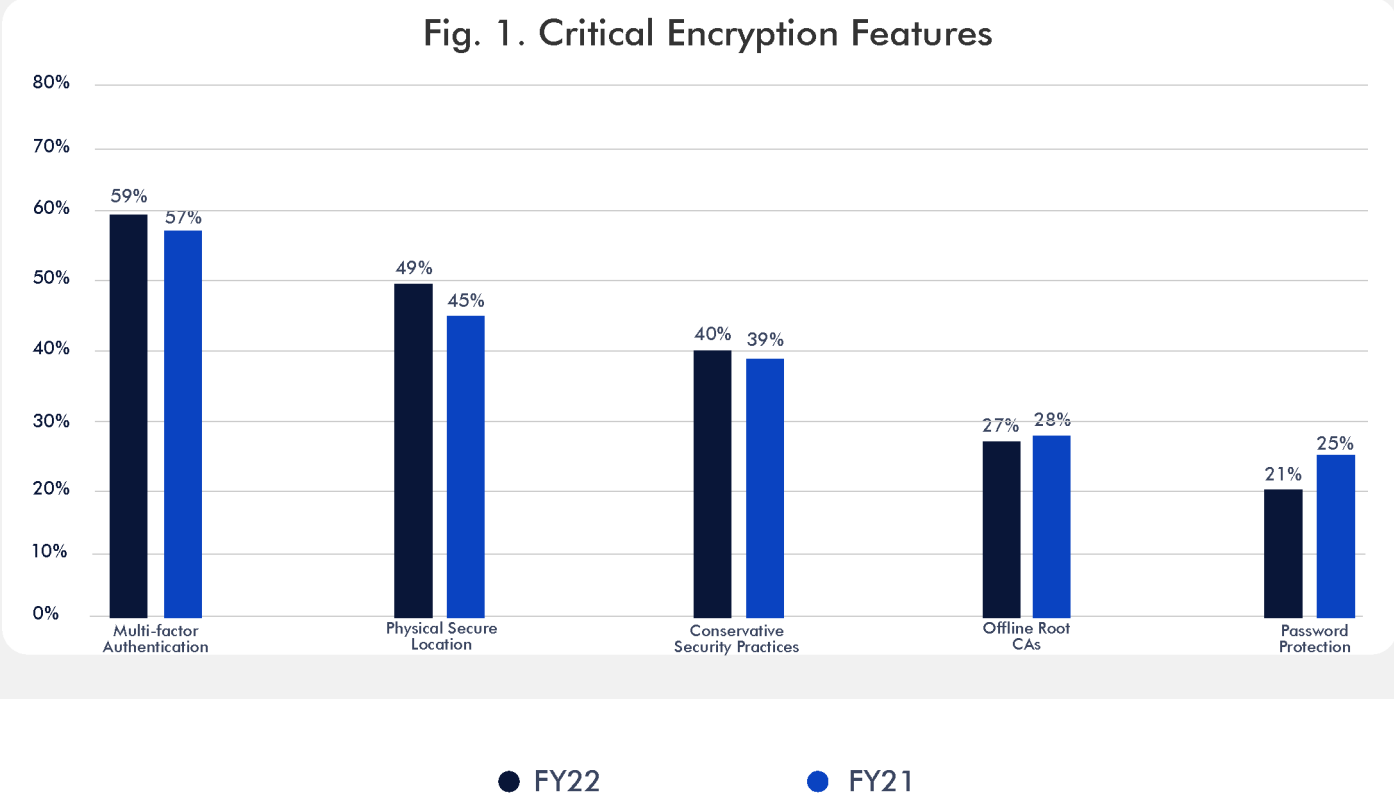
So, this current survey is focused on the global trends followed across industries & organizations in leveraging PKI for the year 2022. This study circle for the research was restricted to 3,520 from various countries across the globe. This report primary focus is on the analysis of the findings based 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.

The first section of the survey covers the steps taken by various organizations in securing the Public Key Infrastructure (PKI) and Certificate Authorities (CAs). Majority of the respodents are leveraging multi-factor authentication for protecting their infrastructure. Percentage increased from 57% to 59%. This is followed by physical security which is about 49% and then conservative security methods which are documented. The trend remained same comapred to last year i.e. about 40%. Offline root CAs seen a declining trend compared to 2021 and fared 27%. Similarly, usage of traditional password protection took a big hit as straight decline from 25% in FY21 to 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 practices. 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 authencity for the report.

Figure 1. **Practices used to secure PKI and Certificate Authorities**



B.

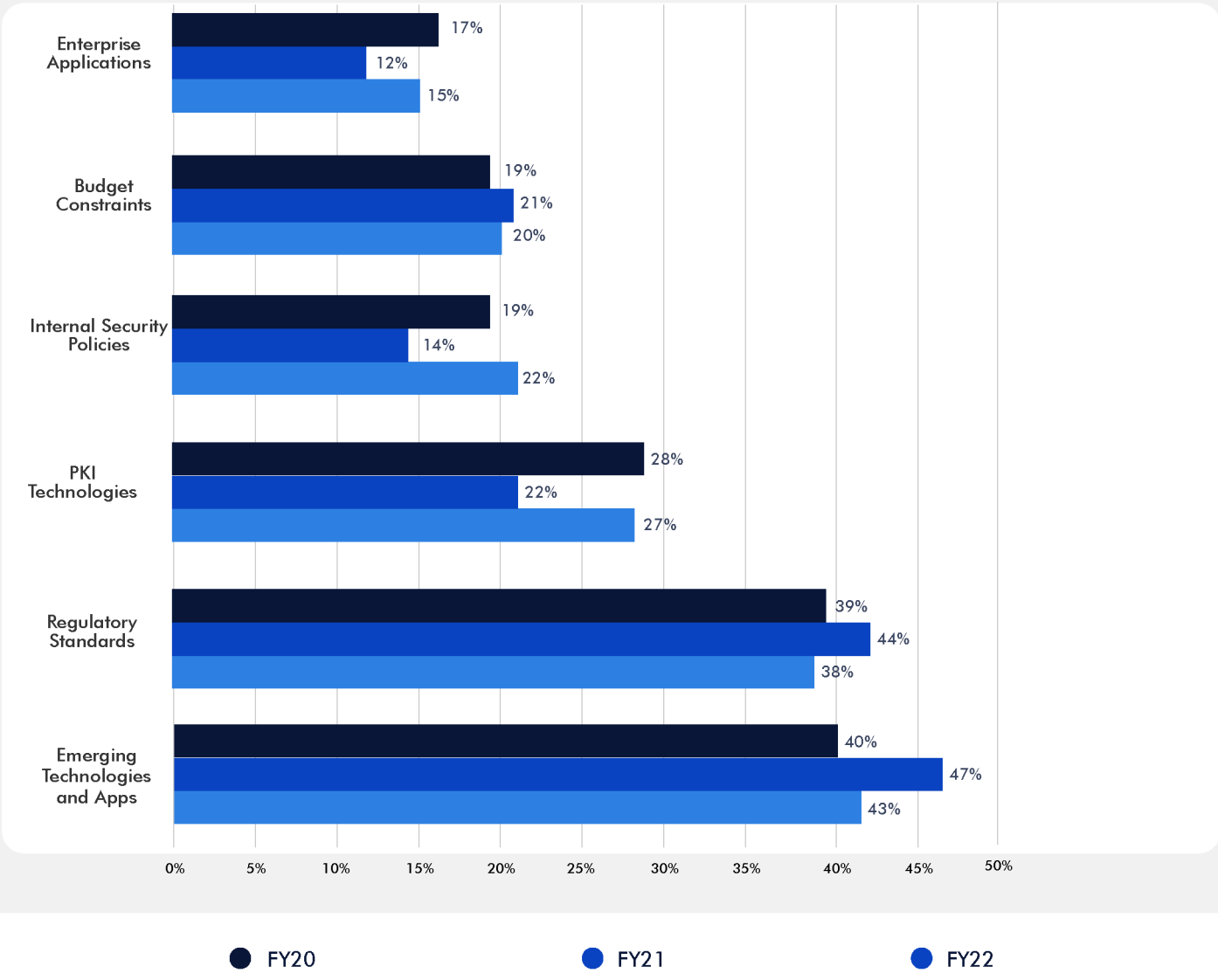
Key Findings

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

IoT Key Management Complexity

Figure 2 provides the information on the factors/drivers contributing to the uncertainty in the PKI trends across various sectors. 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. Whereas budget constraints remained constant across the years with around 20% voting. Other major influencing factors are PKI technologies and enterprise applications showing a constant increasing trend over the past three years.

Figure 2. **Areas expected to experience the most change and uncertainty**

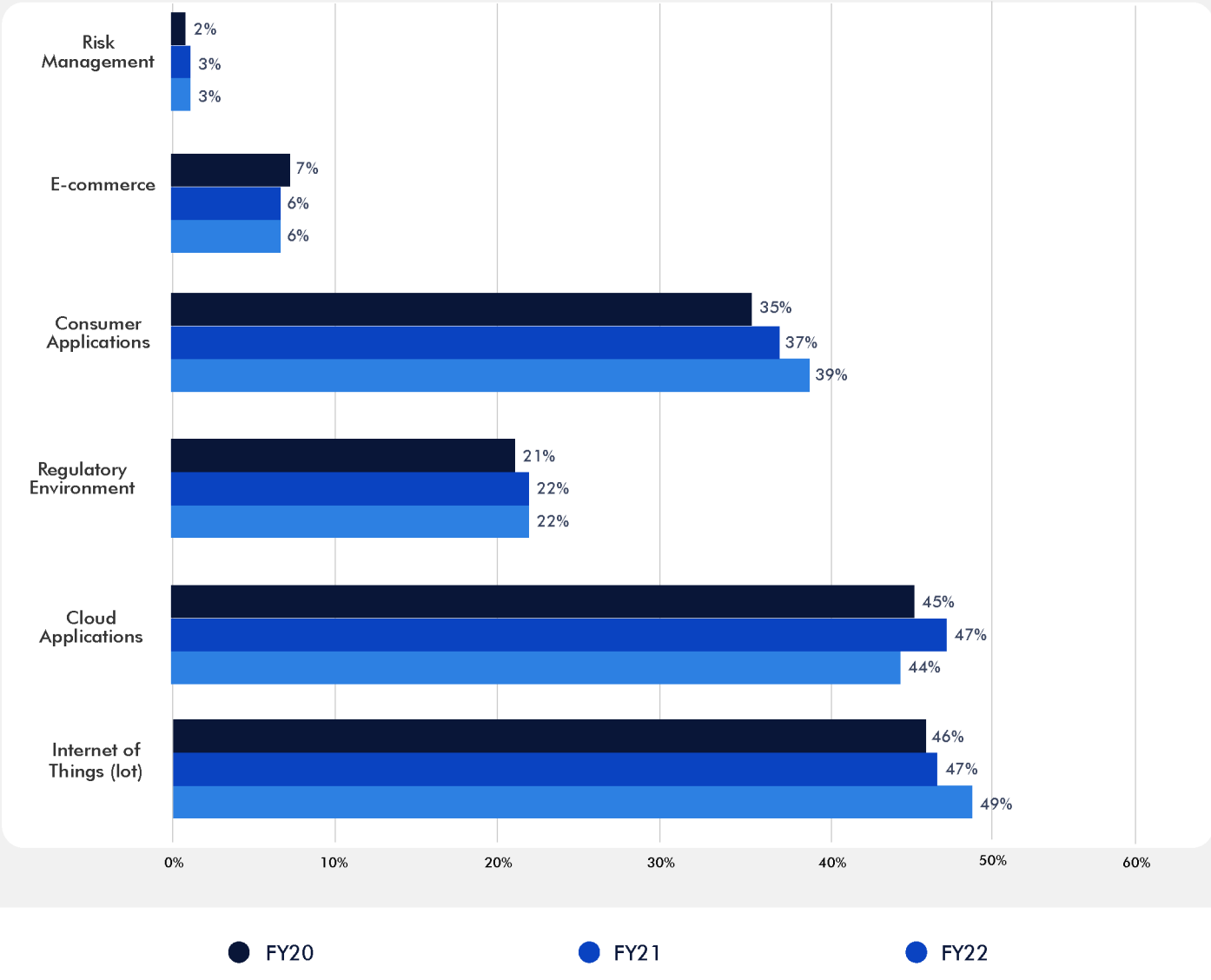


The significance of Internal Security Policies increased from 14% in FY21 to 22% in FY22. This might be due to enhanced awareness across security landscape.

What are the major factors impacting the deployment of PKI applications? Internet of Things, which is the current fast-growing trend, is a major factor chosen by 49% of the respondents.

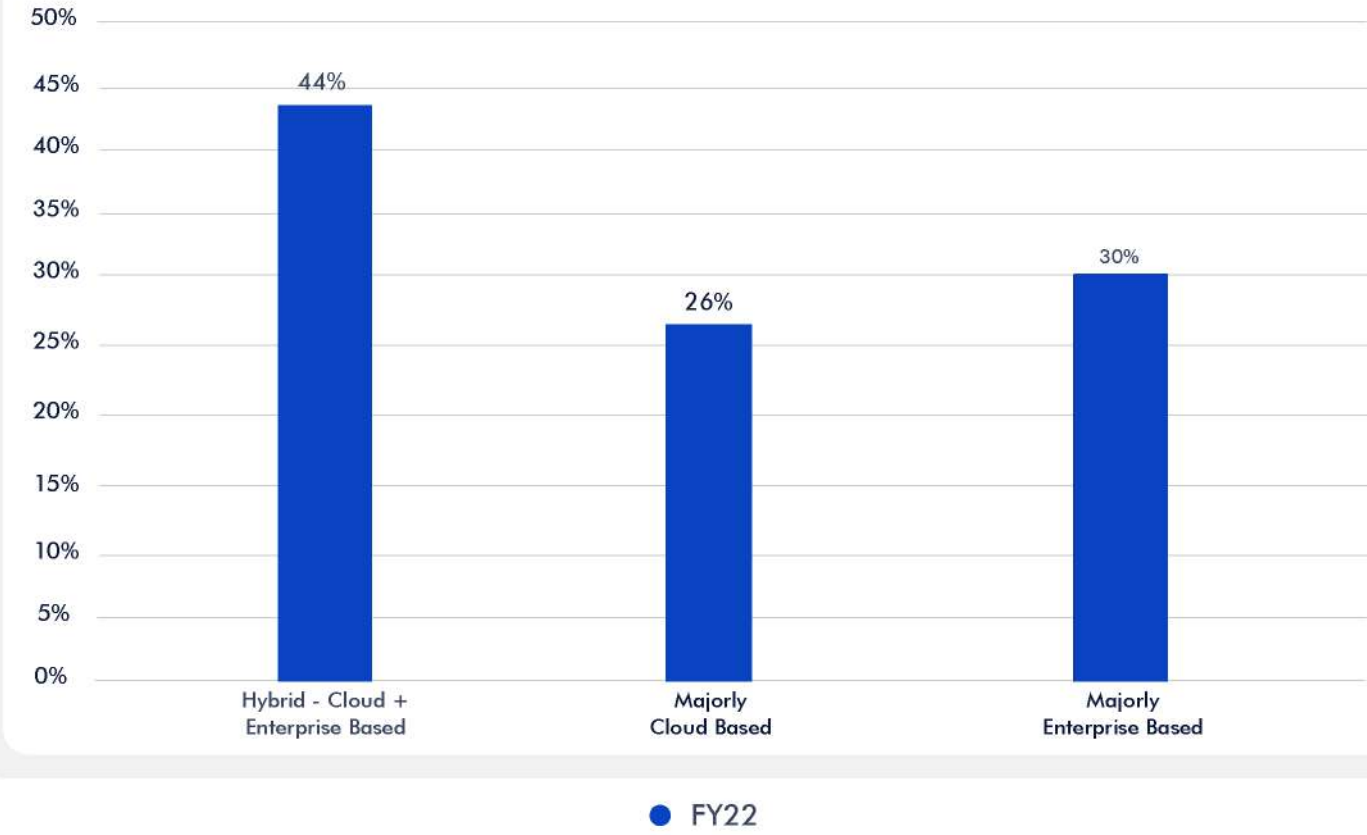
This is a 2% increase from FY21. A major factor for this trend would be the trust placed on PKI in providing the core authentication for IoT devices. This also suggests the increasing adoption of Internet of Things by various sectors across the globe. On the contrary, cloud based services took a bearing in the survey with a decrease in percentage from 47% to 44%. Regulatory environment remained a constant factor compared to last year with 22%.

Figure 3. **The Most Important Trends Driving the Deployment of Applications Using Of PKI**



As observed from this survey, it is clearly evident that IoT is going to be the next big thing in the technology space and out of these, more than 45% will leverage digital certificates for security and data protection.

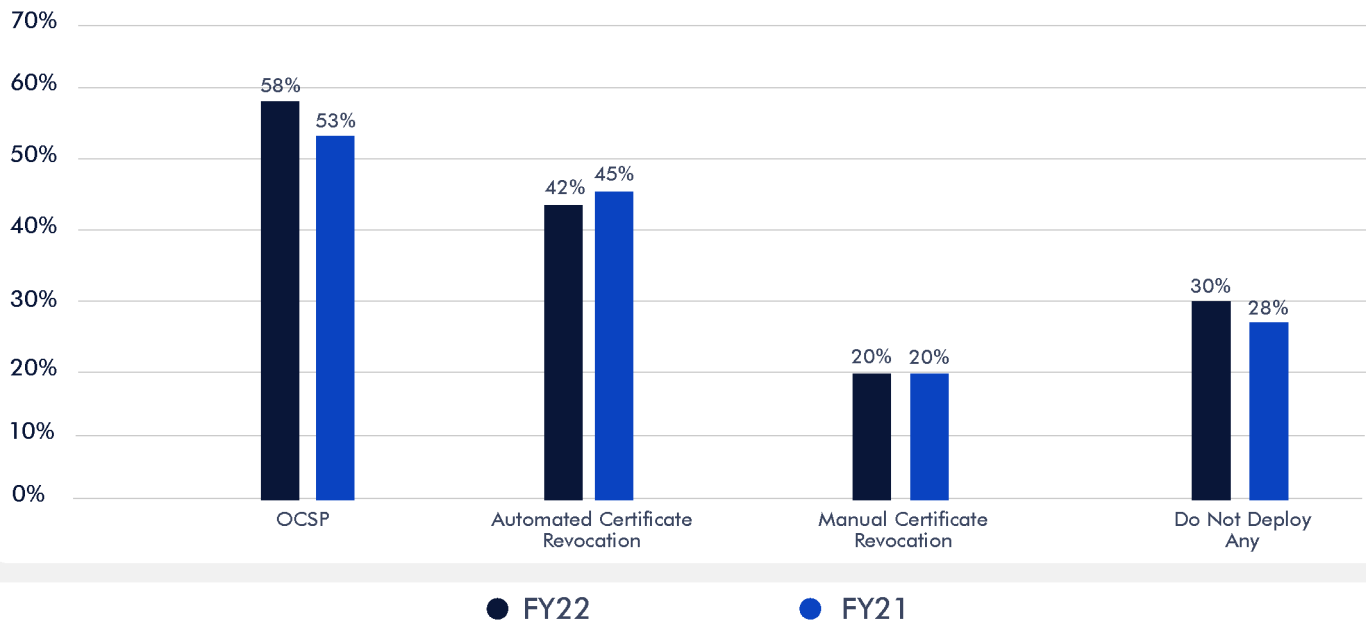
Figure 4. **Types of PKI deployment for IoT credentialing**



PKI Revocation

The certificate revocation technique is one of the key factor in the PKI technology where certificates are validated and revoked as per the requirement. Figure 5 indicates the organizations take on certificate revocation techniques followed. A majority of the respondents are in favour of using OCSP – Online Certificate Status Protocol (OCSP) for certificate revocation. According to 42% of the respondents, automated certificate revocation list is the next sought after technique. It is a 3% decrease when compared to last year - FY21. Intrestingly, 30% of the respondents mentioned that they do not deploy any certificate revocation mechanism. However, the reasons are not clear.

Figure 5. **The certificate revocation techniques used in enterprises**

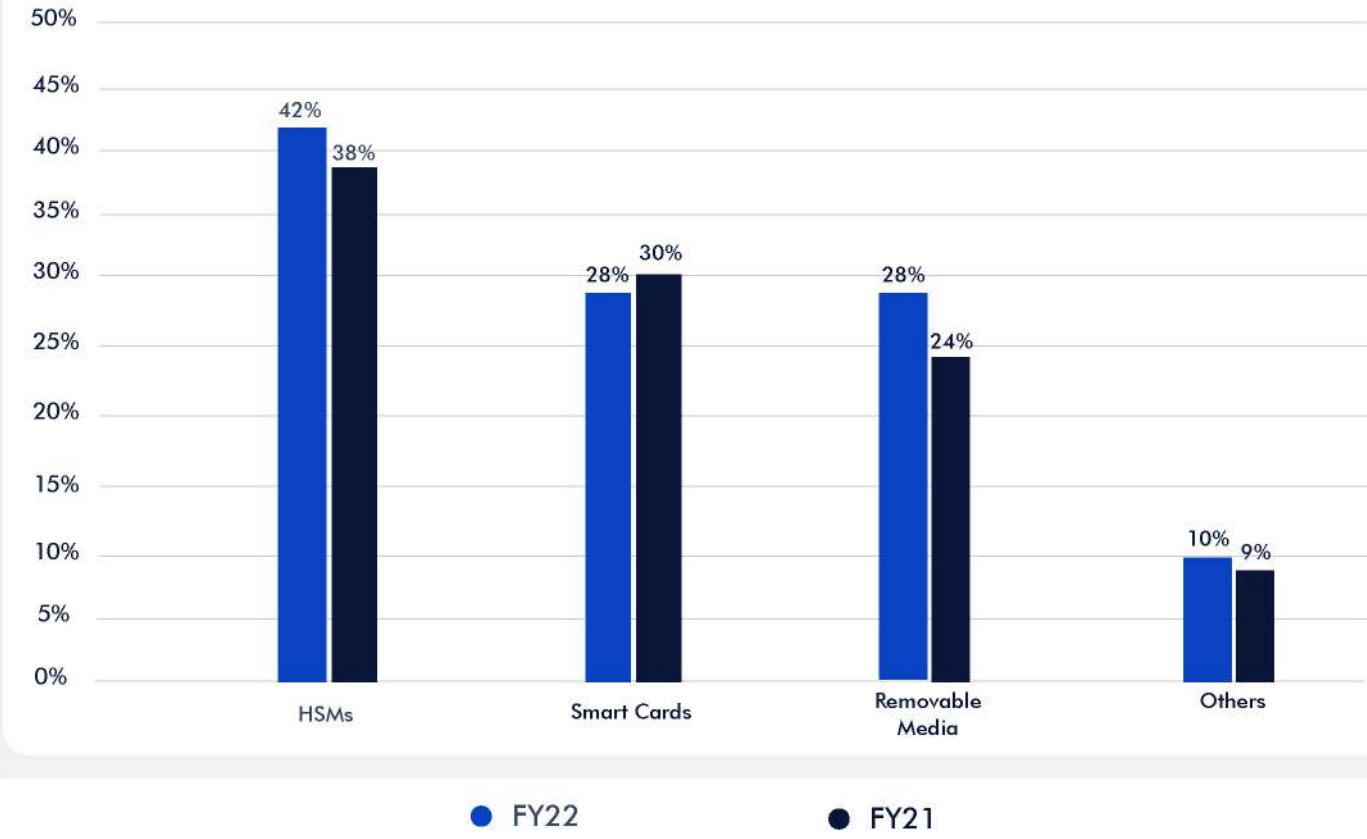


51% of the responding organizations have an overall encryption strategy deployed in their firms and it is a 11% increase when compared to the trend from FY18.

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 42% chose HSMs.

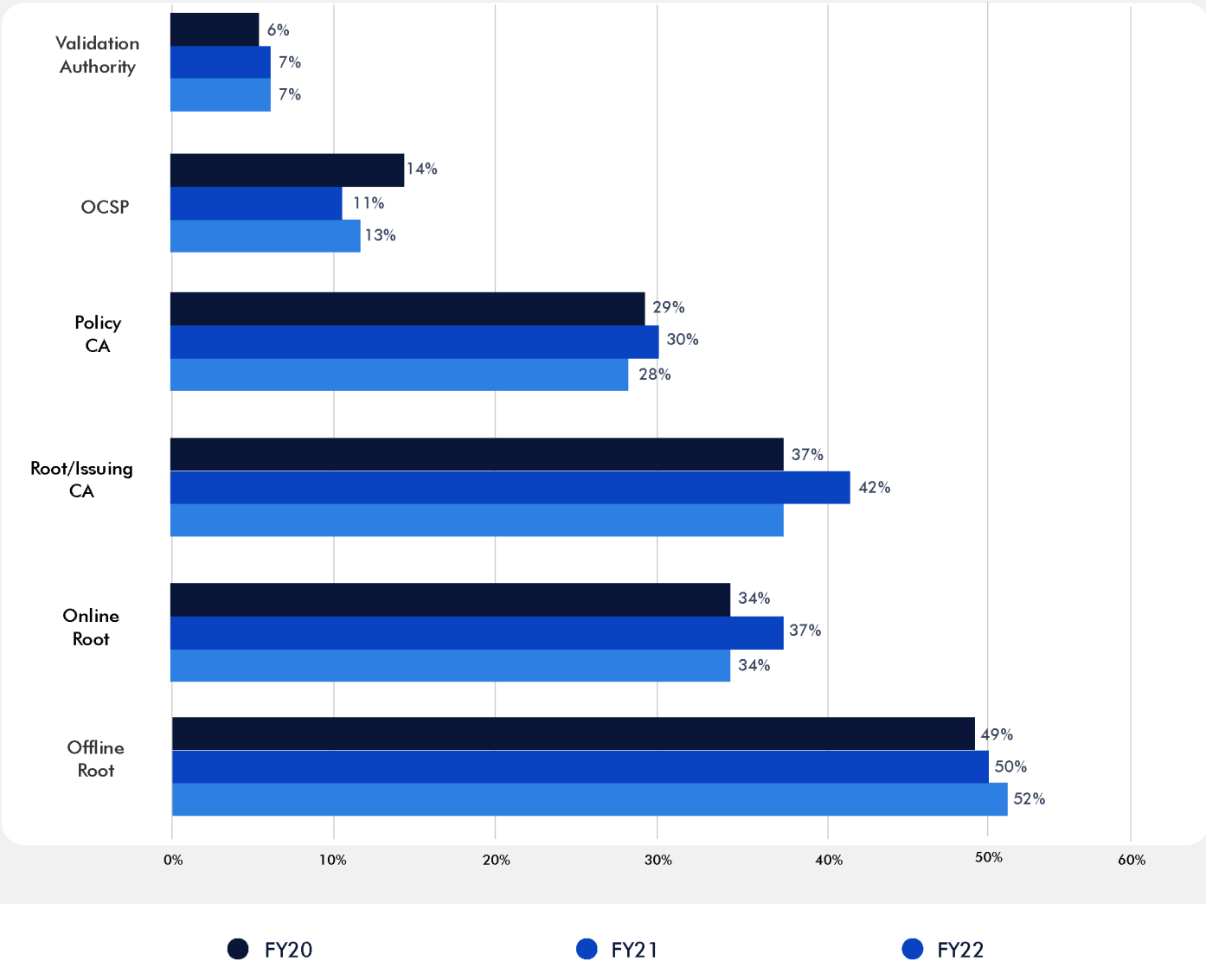
This might be due to the enchanced security provision with HSMs. Around 28% prefer smart cards for CA key protection. There is a 2% decline comapred to FY21. Removable media for CA key management is an equal contender as smart cards with about 28% voting.

Figure 6. **Private Key management for Certificate Authority (CA)**



As it is observed from Figure 6, HSMs are the most sought after protection method to secure the private keys of various Certificate Authorities (CAs). Now, we would like to understand where HSMs are deployed to secure PKI across the organization. Around 52% of the organizations participated in this survey mentioned that they deploy HSMs in offline CA for protection whereas only 32% agreed in using HSMs with Online CAs. This is a significance difference between two types of CAs. One of the interesting revelations during the survey was that the organizations are unintrested in deploying HSMs and OCSP responders in spite of this being mentioned as oe of the best practices by major standards and frameworks across the world. Respondents were least interested in HSMs deployment at validation authority. The 7% response projects this conclusion.

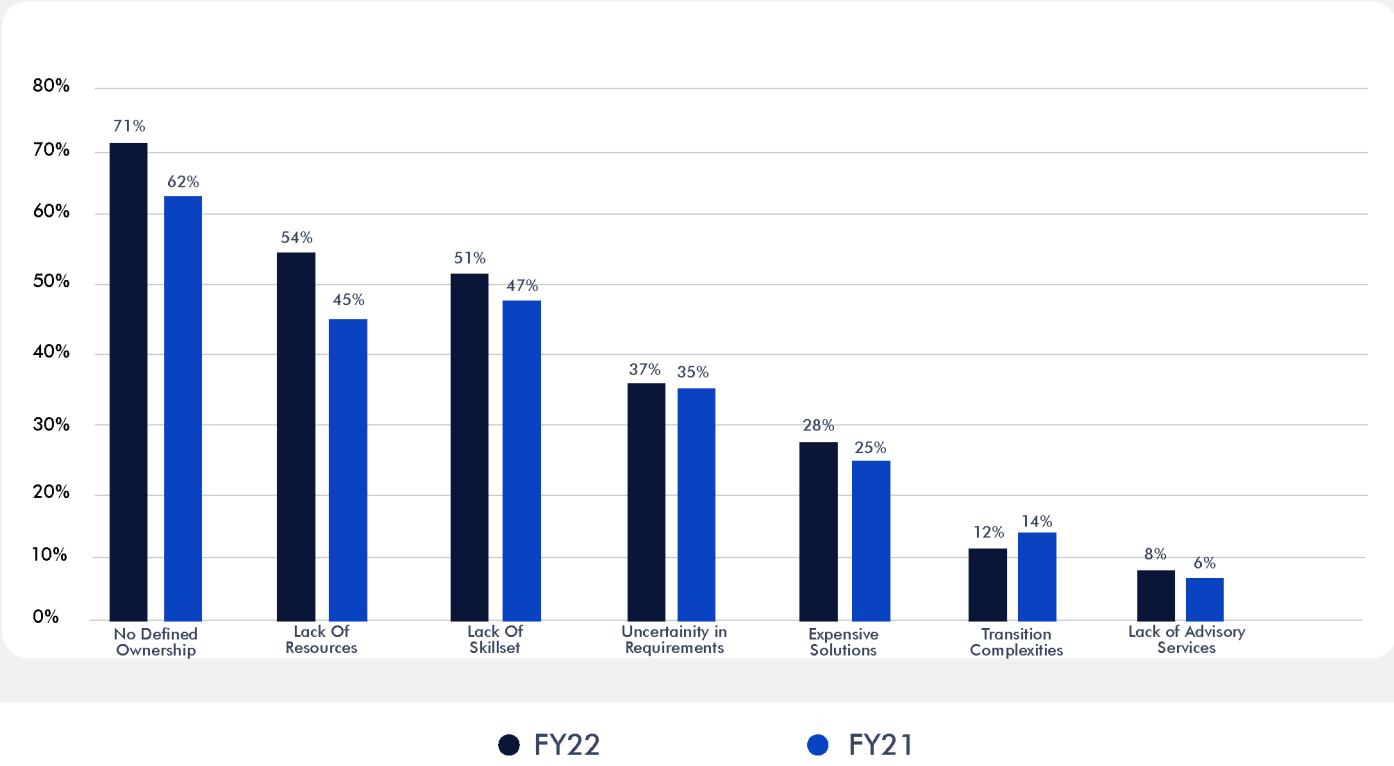
Figure 7. **PKI security through HSMs deployment**



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. Top challenges are no defined ownership and lack of skill-set among the employees as majority voted for these two options. No defined ownership increased from 62% in FY21 to 71% in FY22. Lack of skill set and resources were chosen by 51% & 54% respectively. This clearly indicates the complexity involved in PKI. Uncertainity in understanding the requirements has seen a decrease of 2% from 37% to 35%. This trend shows that organizations are looking for consulting firms with knowledge and expertise in PKI.

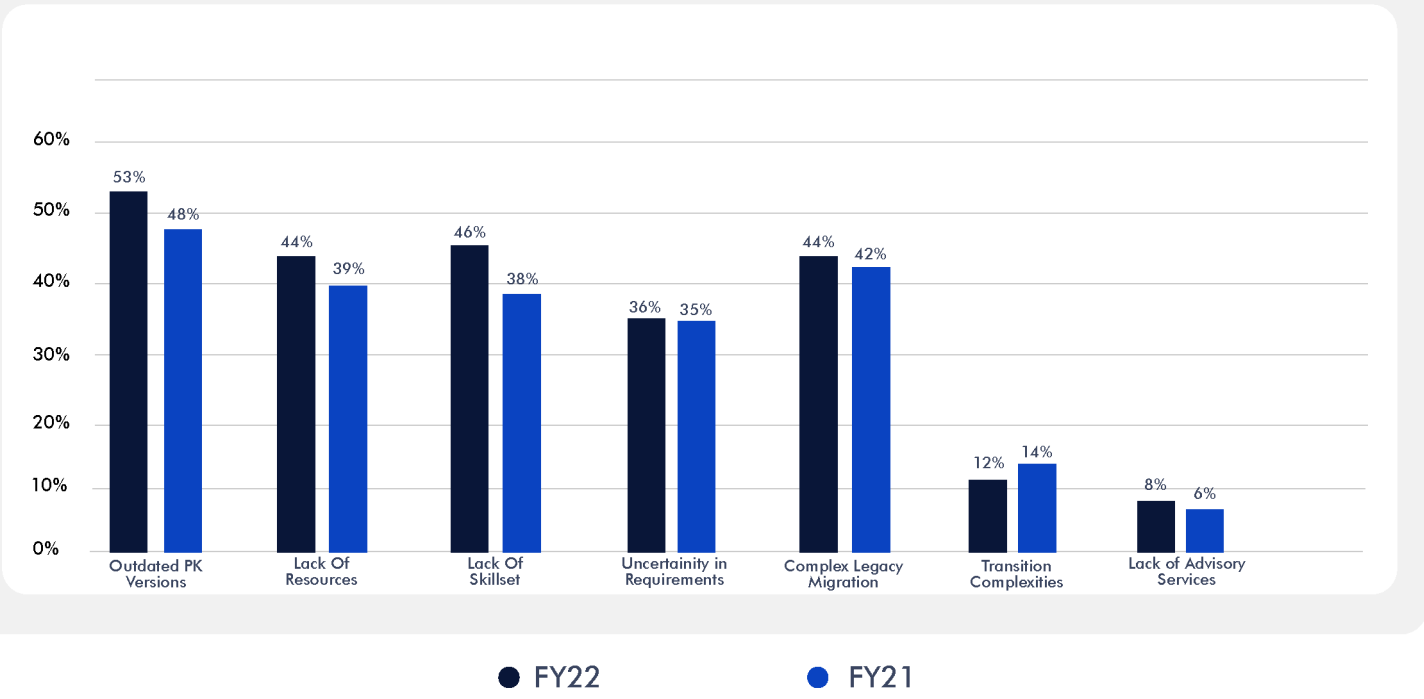
Figure 8. **The challenges in deploying and managing PKI**



PKI compatibility with existing/new applications:

There are several reasons for incompatibility of PKI with the organization's applications. Around 53% of organizations feel that no upgrade to existing PKI is the major reason for incompatibility with apps. This is followed by the lack of skill-set which increased from 38% in FY21 to 46% in FY22. Uncertainity in understanding the requirements and complexity in legacy apps migrations are the next major challenges with 36% and 44% respectively opting for these options. Our analysis indicate that other than organizations with better encryption maturity, a good portion of respondents are willing to hire consulting firms from their expertise in PKI.

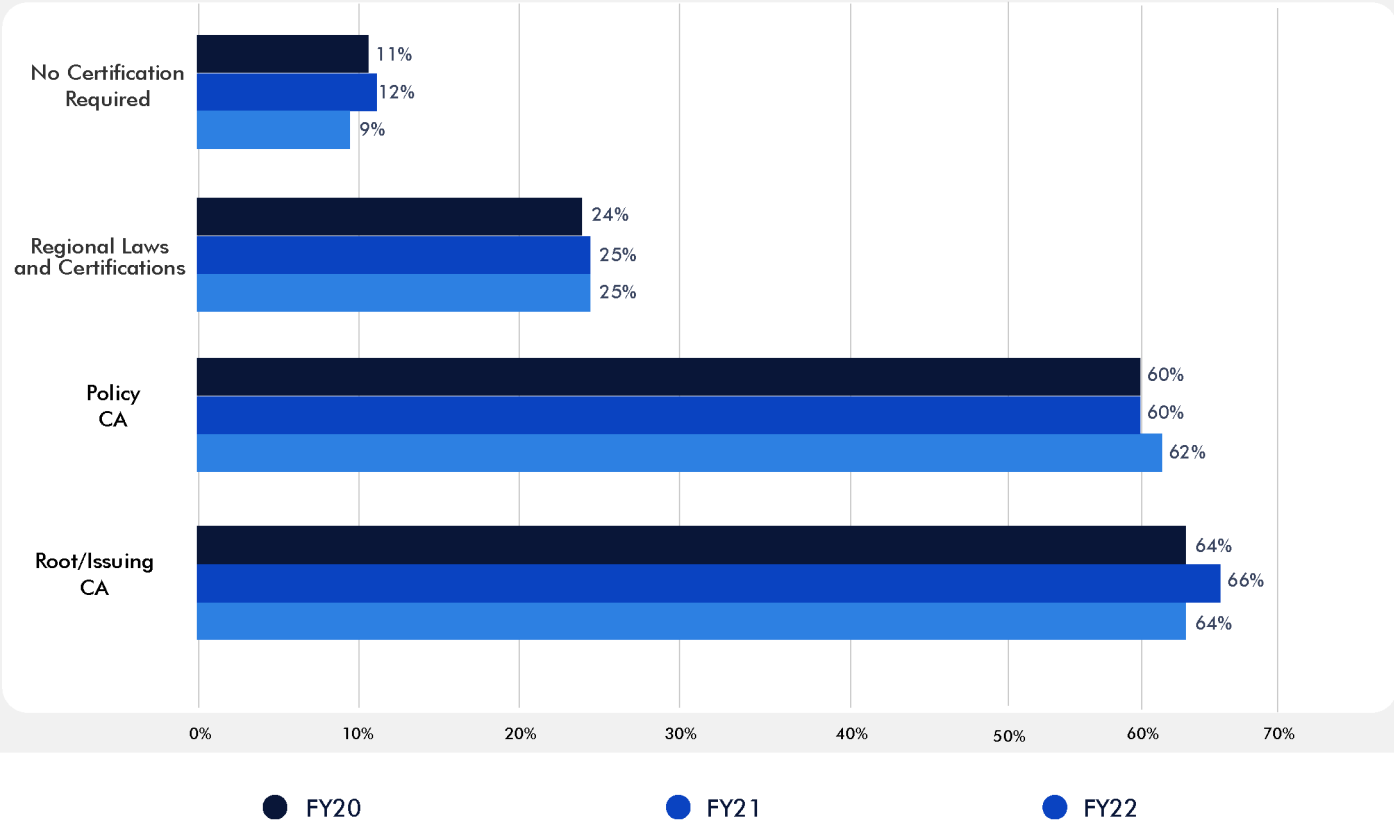
Figure 10. **PKI compatibility with existing/new applications**



Certifications considered important for PKI:

It is evident from the previous survey responses that organizations are finding it more difficult to find appropriate and skilled resources on PKI technology. Figure 11 depicts the responses from organizations on their understanding of PKI certifications by either their own resources or consulting firms. A majority of the respondents believed that common criteria EAL Level 4+ is the most critical certification required for PKI deployment. About 64% 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 of PKI. This includes regional digital signature laws and certifications. A minor share of respondents (9%) believes there is no certification necessary to handle PKI. One strong observation is that organizations are in search of consulting firms such as Encryption Consulting etc. which has a substantially skilled resource set and certifications for handling their PKI.

Figure 11. **Security certifications important when deploying PKI infrastructure**

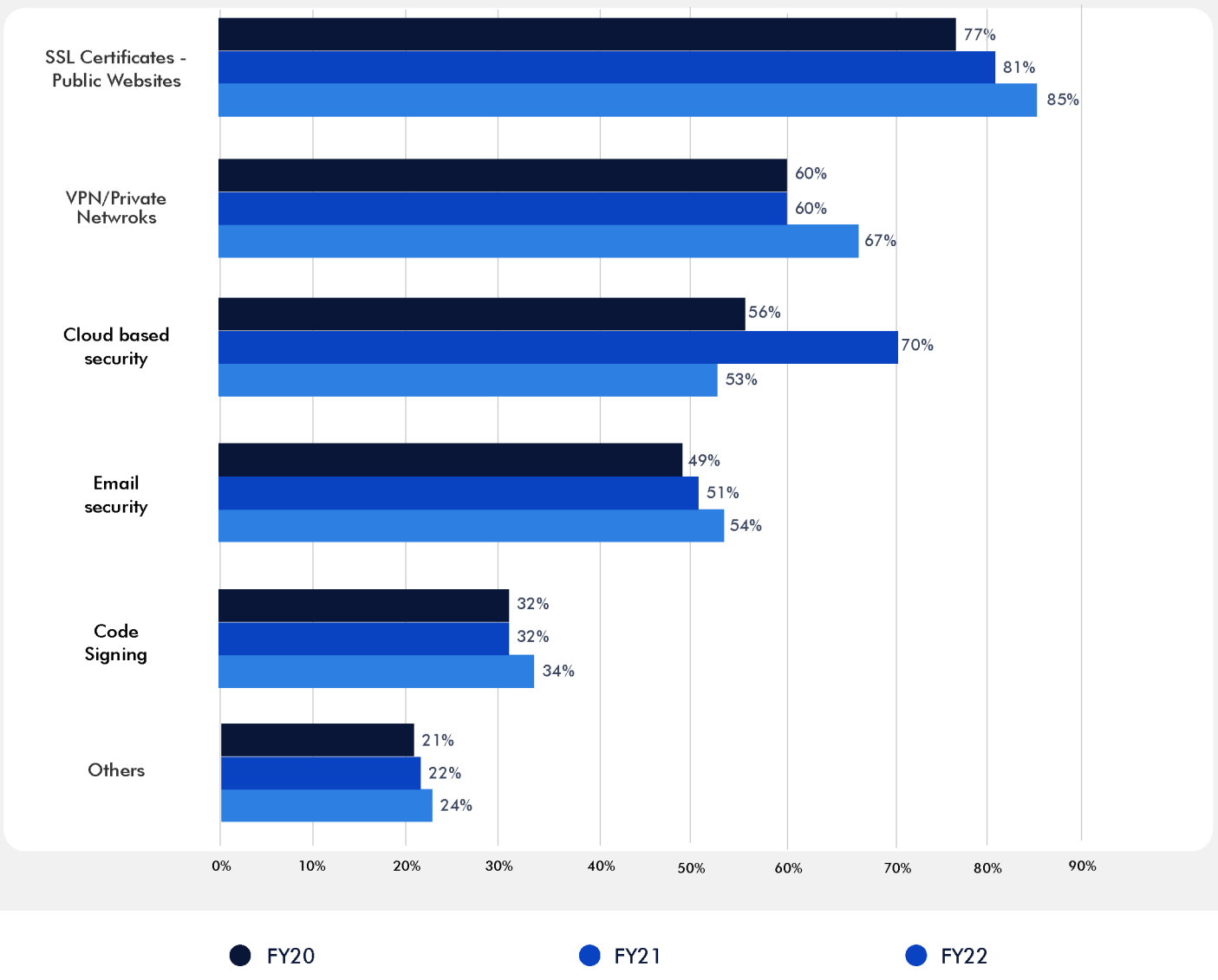


Where is PKI used?

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 85% 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 a drastic decrease in usage of PKI. The drop in the percentage is seen from 70% to 53%. VPNs/Private networks have seen an increase in usage of PKI in FY22, and this might be attributed to increase in work from home culture due to pandemic. The increase is seen from 60% to 67%.

Figure 12. **What applications use PKI credentials in organizations?**

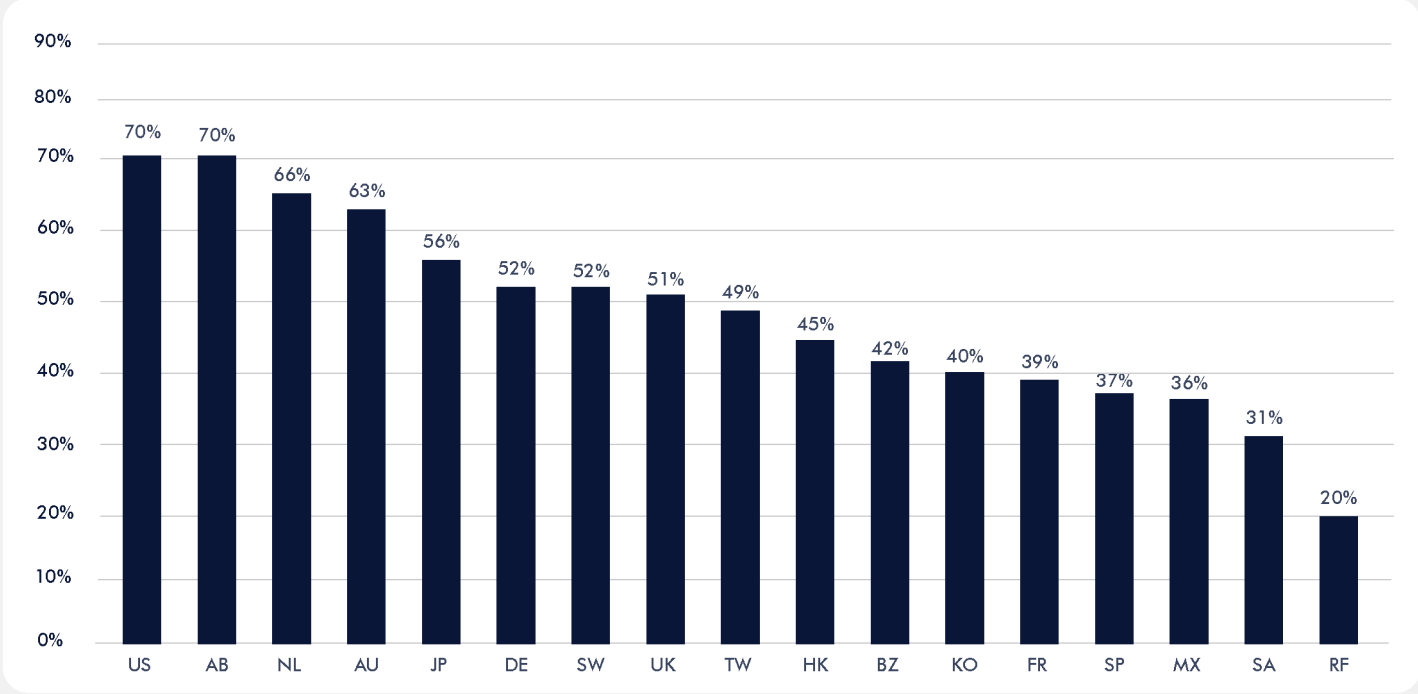


ANALYSIS ON HARDWARE SECURITY MODULES

Hardware Security Modules (HSMs) are playing a crucial role in today's organization Cyber Security landscape. The global deployment rate of these devices has risen from 43% in 2018 to 52% in 2021 according to our research performed on hetero demographic respondents. With technology's ever-changing environment, organizations must keep up to be successful. These changes can lead an organization down one of two paths: One may lead to growth and prosperity, but the other may lead to destruction and despair. Figure 13 projects a clear picture about the deployment projections as per the respondents from the survey.

HSM deployment rates varied from country to country. In the near future, The United States, Germany, Middle East and Japan organizations are more likely to deploy HSMs with an average response as "Yes" by 67% of respondents. Figure 19 summarizes the percentage of respondents that deploy HSMs. The United States, Germany and Japan are more likely to deploy HSMs than other countries. The overall average deployment rate for HSMs is 49%. HSMs are almost tamper resistant hardware devices used prominently in key management. This trend shows a few of the countries which are willing to go the extra mile for protecting customer sensitive information by preserving keys in hardware security modules.

Figure 13. **Willingness of Countries to deploy HSMs**



HSMs are devices specifically built to create a tamper-resistant environment in which to perform cryptographic processes (e.g., encryption or digital signing) and to manage the keys associated with those processes. These devices are used to protect critical data processing activities associated with server based applications and can be used to strongly enforce security policies and access controls. HSMs are typically validated to formal security standards such as FIPS 140-2.

The deployment of HSMs continues to increase steadily. Figure 14 shows a four year trend for HSMs. As can be seen, the rate of HSM deployment has constantly increased across the globe.

HSM primary usage is key management for cloud based applications. We asked organizations about the operation of HSM in line with Cloud applications and responses are shown in Figure 15. As shown in Figure 15, 53 percent of respondents own and operate HSMs on-premise for cloud-based applications and 47 percent of respondents rent/use HSMs from a public cloud provider for the same purpose. There is a significant increase in respondents who would like to handle the ownership and operation of HSMs on-premise and the integration with a Cloud Access Security Broker to manage keys and cryptographic operations for data-in-motion encryption.

Figure 14. **HSM deployment rates over four years consolidated across countries**

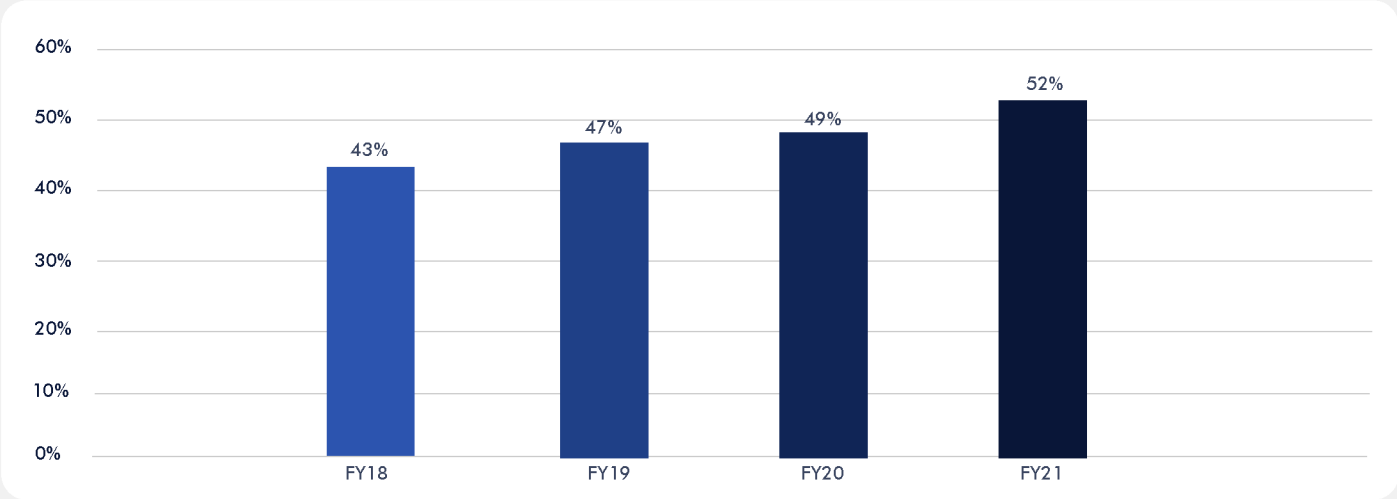
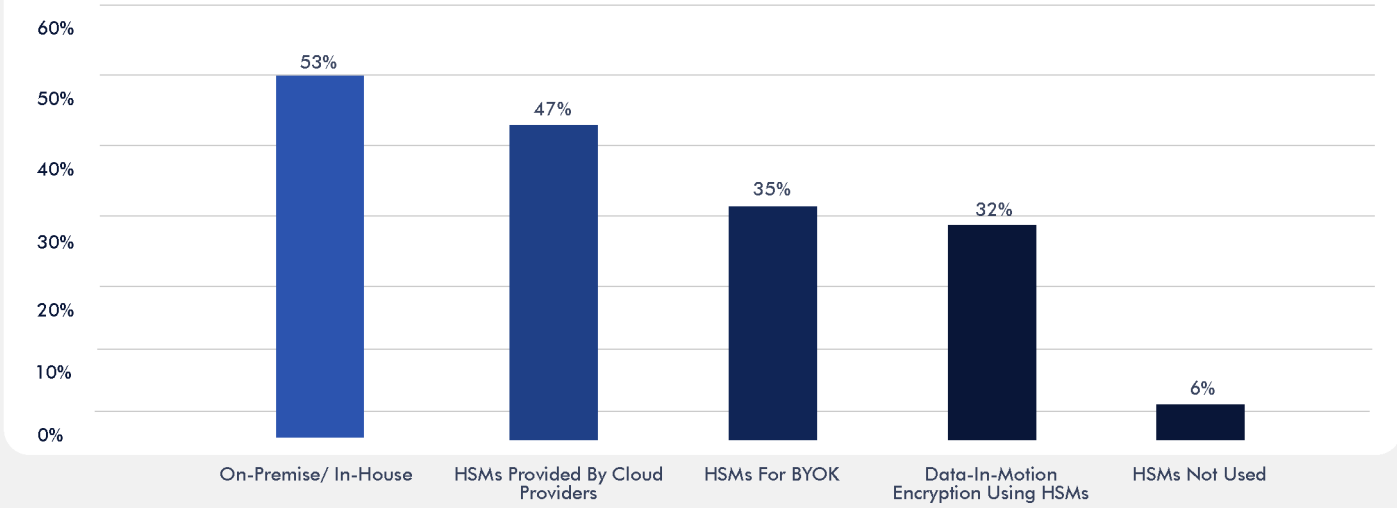


Figure 15. **HSM usage trend with Cloud applications**



A similar study conducted by the Ponemon Institute revealed the following analysis on HSMs: Figure 16 summarizes the percentage of respondents in 17 countries that rate HSMs as either very important or important to their organization's encryption or key management program or activities. The overall average importance rating in the current year is 66 percent. The pattern of responses suggests the United States, the Middle East and the Netherlands are most likely to assign importance to HSMs as part of their organization's encryption or key management activities. Figure 17 shows a nine-year trend in the importance of HSMs for encryption or key management, which has steadily increased over time.

Figure 16. **Perceived Importance of HSMs as part of encryption or key management**

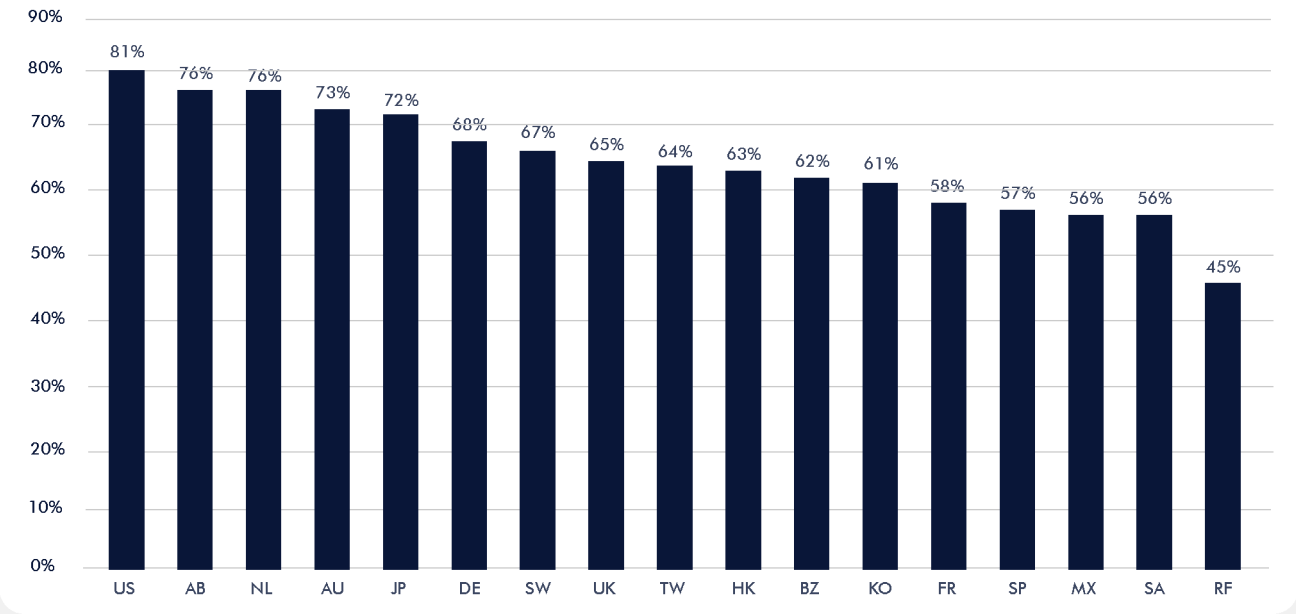


Figure 17. **Perceived Importance Of HSMs As Part Of Encryption Or Key Management Over 9 Years**

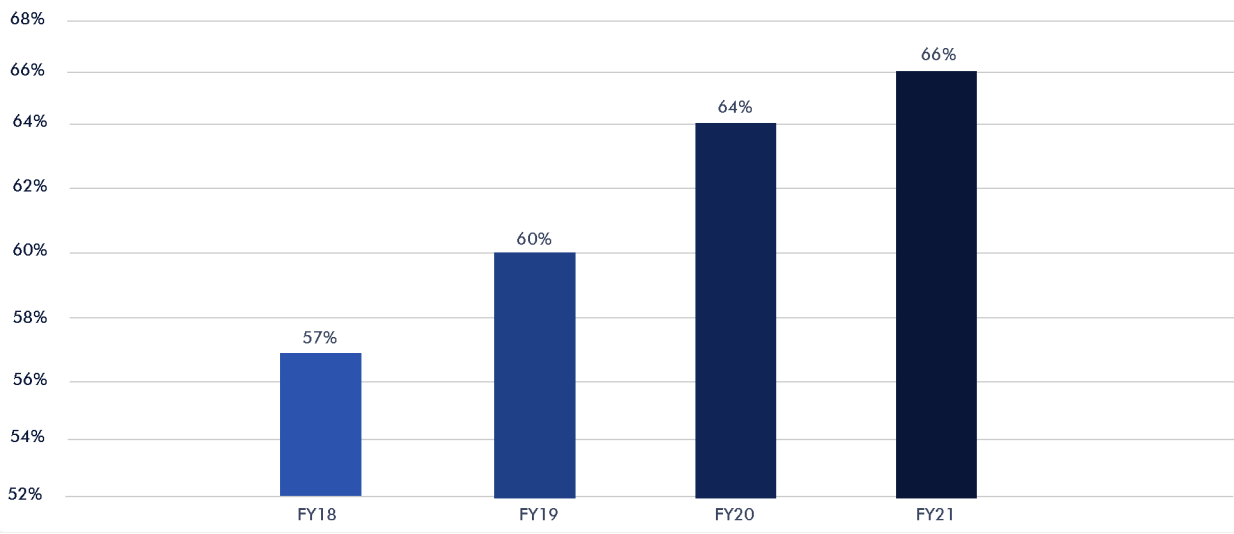
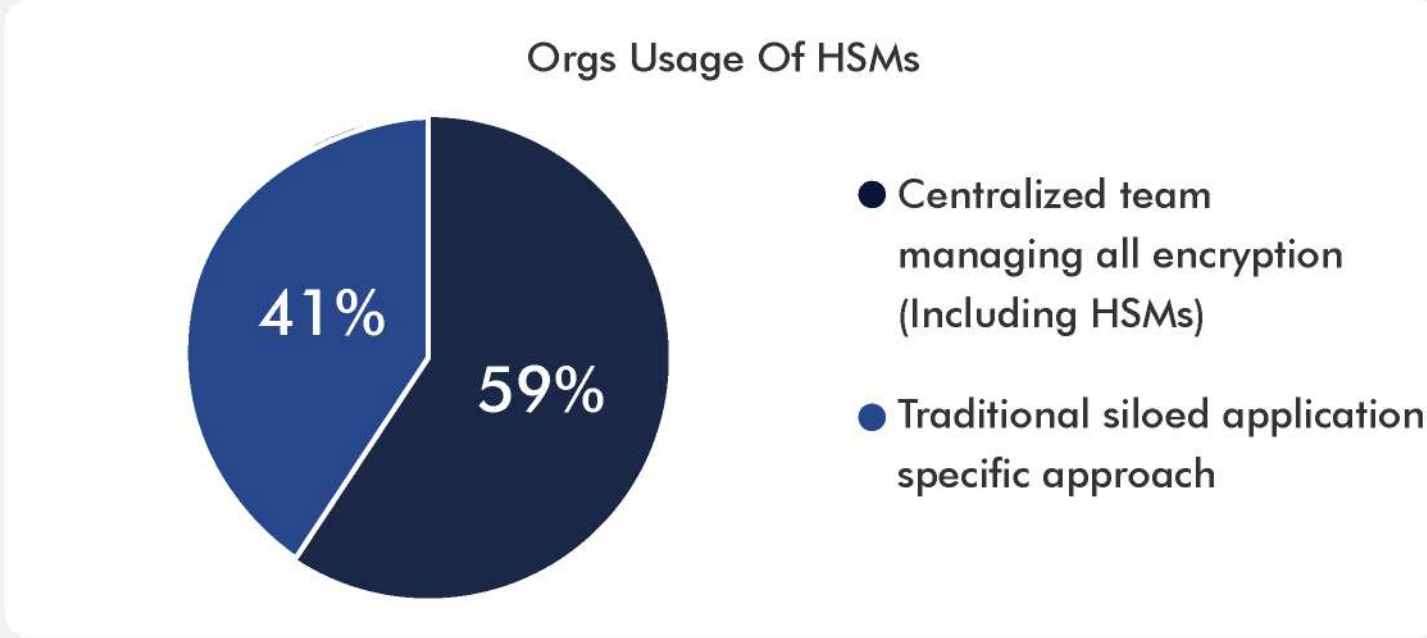


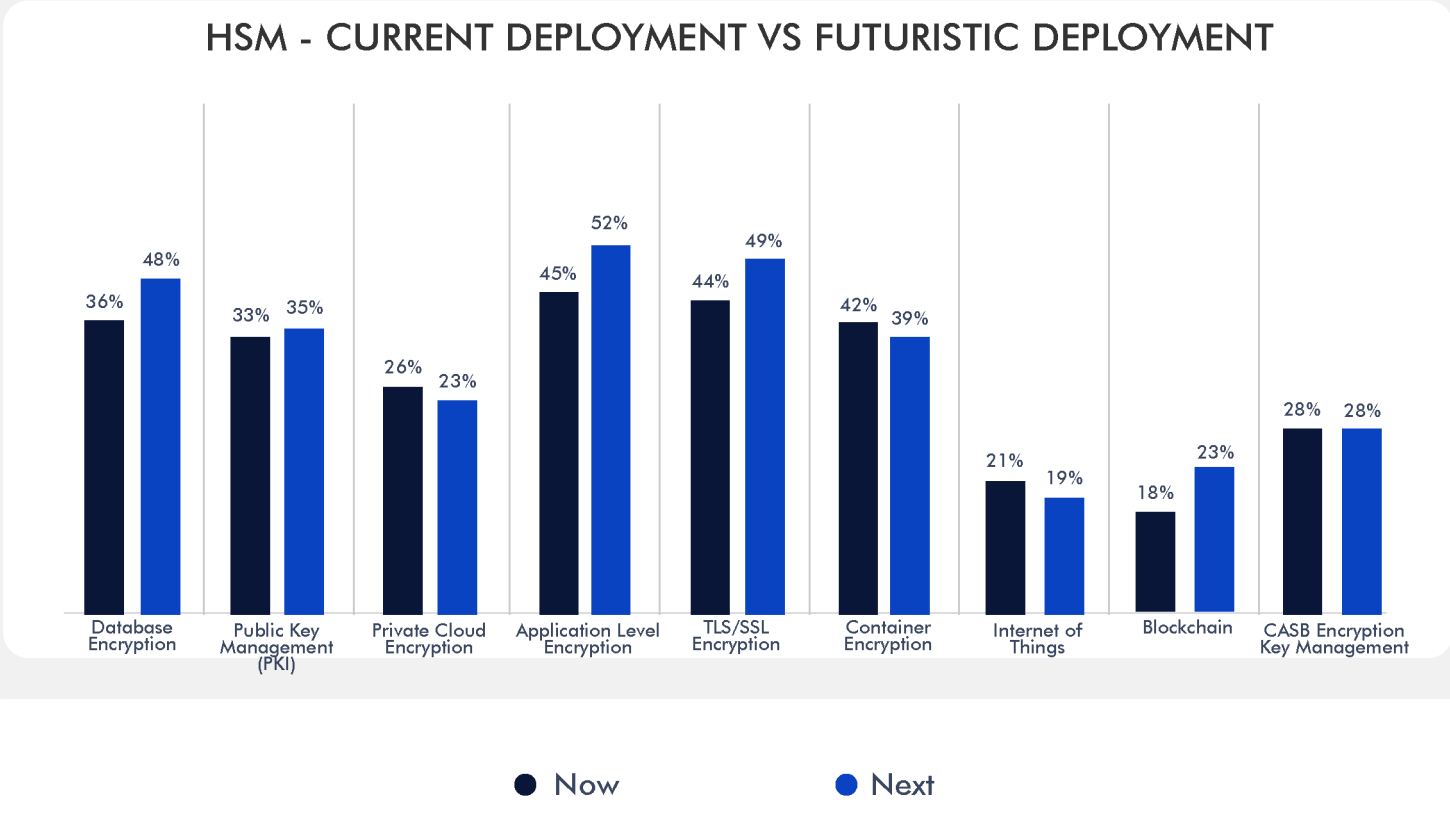
Figure 18 shows the HSMs usage, 61 percent of respondents say their organization has a centralized team that provides cryptography as a service (including HSMs) to multiple applications/teams within their organization (i.e., private cloud model). 41% responded that each individual application owner/team is responsible for their own cryptographic services (including HSMs), indicative of the more traditional individual application-specific approach.

Figure 18. **Organizational Usage Of Hardware & Security Modules**



Important use cases of HSMs by various organizations are summarized in Figure 19. We surveyed the primary purpose or use cases for the current deployment of HSMs versus future use. As can be seen, the top choices are database encryption, application-level encryption, TLS/SSL, followed by container encryption/signing services. This chart shows a significant increase in the use of database encryption 12 months from now which is a good indication for increasing trend of performing data-at-rest encryption. It is significant to note that HSM use for application-level encryption will soon be deployed in 49 percent of the organizations represented in this study. One of the significant observations from the survey's outcome is the preference to increase the usage of HSMs for blockchain technology based applications and decrease in usage for Internet of Things (IoT). Increasing importance for blockchain technology can be attributed to many trending and budding factors such as decentralization and cryptocurrency invasion. It will be interesting to see how these new upcoming technologies impact encryption.

Figure 19. **HSMs - Current Deployment vs Future Deployment**



About **Encryption Consulting**

Strategic Technology Partnerships

We work with the industry's best technology providers and have broad experience deploying, managing, and 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

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 applica tions.

THALES

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

Fortanix

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

KEYFACTOR

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

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

MICRO FOCUS

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

CRYPTOMATHIC

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

gemalto
security to be free

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

FORNETIX

Fornetix Key Orchestration TM is a scalable and flexible solution designed to simplify key management. Granular policy 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

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

PrimeKey

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

UNBOUND
(MATH OVER MATTER)

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

VENAFI

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

utimaco®

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.

protegrity

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.

PrimeFactors
APPLIED DATA PROTECTION

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.

comforte

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

ENCRYPTION CONSULTING
www.encryptionconsulting.com

Why Encryption Consulting LLC?

ENCRYPTION CONSULTING
www.encryptionconsulting.com

Encryption Advisory Services

Encryption is used for securely protecting data from unauthorized access. 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 have 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 environments? 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 securtiy consulting firm providing an array of services in all aspects of data protection.

Contact Us

encryptionconsulting.com

facebook.com/encryptionconsulting

linkedin.com/company/encryptionconsulting

twitter.com/encryptioncons