ENTRUST
SECURING A WORLD IN MOTION

nCIPHER AN ENTRUST COMPANY

Ponemon INSTITUTE

2020 Global PKI and IoT Trends Study

Sponsored by nCipher,
an Entrust company

Independently conducted
by Ponemon Institute LLC

01 INTRODUCTION

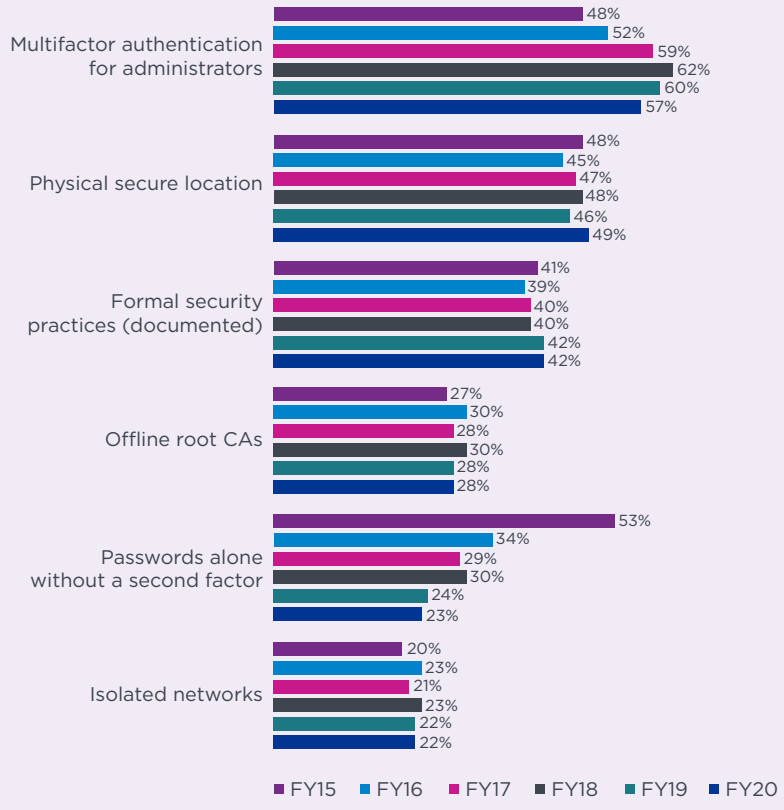
Ponemon Institute is pleased to present the findings of the *2020 Global PKI and IoT Trends Study*, sponsored by nCipher.

According to the findings, digital certificate use is growing rapidly for cloud applications and user authentication. Additionally, the rapid growth in the use of IoT devices[1] is having an impact on the use of PKI technologies and there is realization that PKI provides important core authentication technologies for the IoT.

The PKI research is part of a larger study published in April 2020 involving 6,157 respondents in 17 countries.[2] In this report, Ponemon Institute presents the findings based on a survey of 1,934 IT and IT security who are involved in their organizations' enterprise PKI in the following 17 countries: Australia, Brazil, France, Germany, Hong Kong, India, Japan, Mexico, Middle East (which is a combination of respondents located in Saudi Arabia and the United Arab Emirates), Netherlands, Russian Federation, Southeast Asia (which is a combination of respondents from Indonesia, Malaysia, Philippines, Thailand, and Vietnam), South Korea, Sweden, Taiwan, United Kingdom, and the United States.

Figure 1 shows the primary practices organizations take to secure PKI and Certificate Authorities (CAs). Most companies represented in this study are using multifactor authentication for administrators (57 percent of respondents).

Figure 1. Practices used to secure PKI and Certificate Authorities



[1] IDC predicts by 2025 there will be 41.6 billion IoT devices connected to businesses and these "things" will generate 79.4 zettabytes of data.

[2] See: 2020 Global Encryption Trends (sponsored by nCipher), Ponemon Institute, April 2020.

Similarly, dependency on passwords has declined from 53 percent of respondents in 2015 to 23 percent of respondents in this year's study. Usage of Hardware Security Modules, most prevalent with offline root CAs and issuing CAs, decreased slightly to 39 percent of respondents from 42 percent of respondents in 2019, however they remain the most prevalent method of PKI private key protection.

The report tabulates the responses to the survey and draws some limited conclusions as to how best practices are reflected in observed practices, as well as the influence of cloud computing, the Internet of Things, and other important industry trends. All participants in this research are either involved in the management of their organizations' enterprise PKI or in developing and/or managing applications that depend upon credentials controlled by their organizations' PKI.

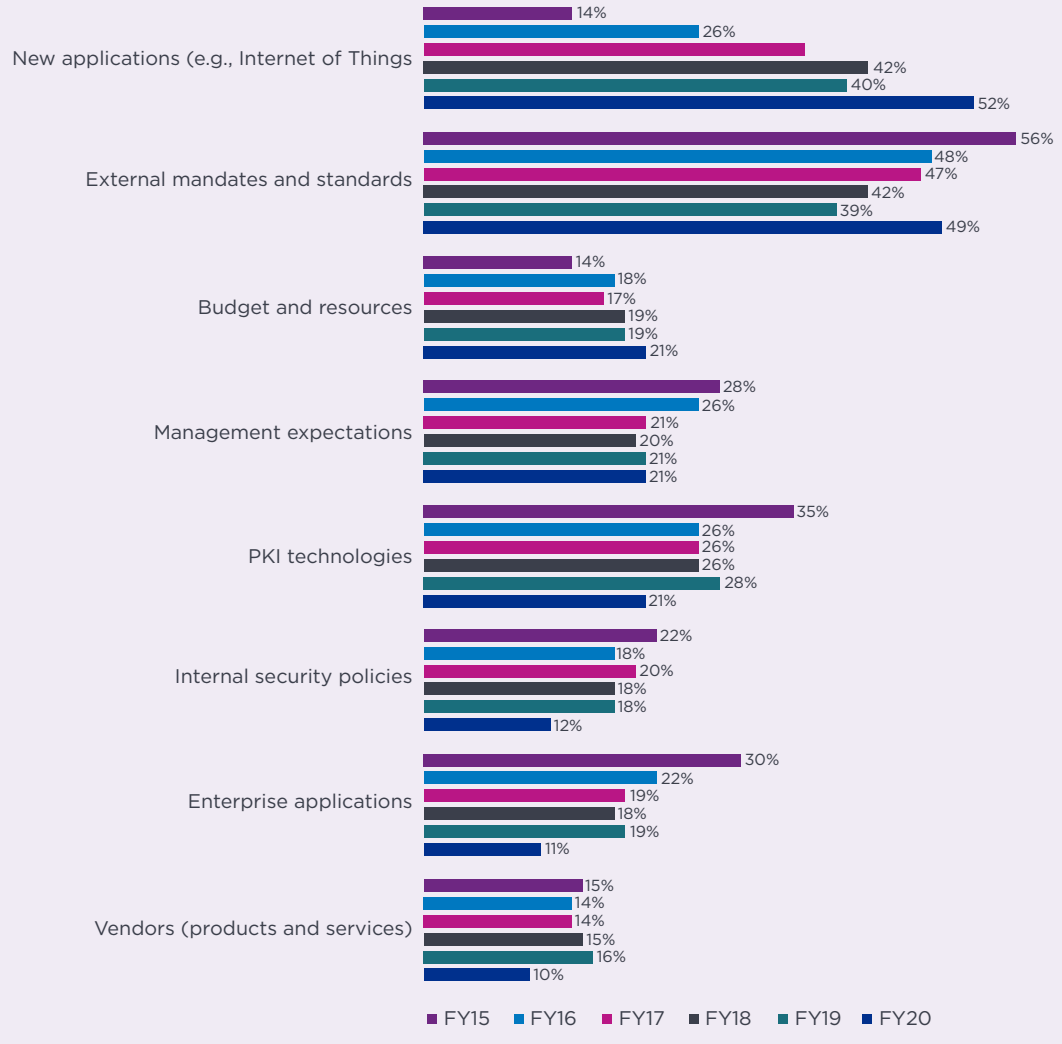
02 KEY FINDINGS

In this section of the report we provide an analysis of the global PKI results over a six-year period.

The pain of managing IoT keys

New applications such as IoT devices continue to drive the most change and uncertainty. According to Figure 2, 52 percent of respondents say the new applications such as the Internet of Things will drive change and this is a significant increase from 40 percent of respondents in 2019. The influence of changing PKI technologies and enterprise applications decreased significantly since 2015.

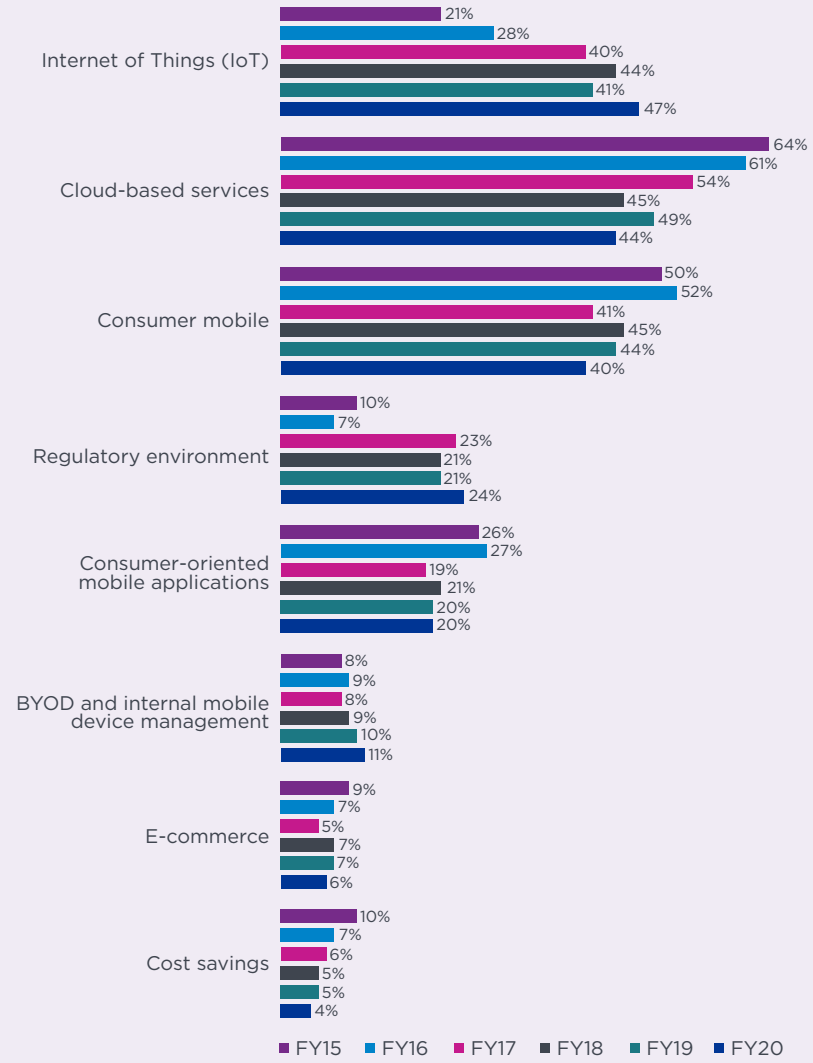
Figure 2. Areas expected to experience the most change and uncertainty
Consolidated view; two responses permitted



While driving change and uncertainty, the IoT is also becoming a major driver for the use of PKI. There is growing recognition that PKI provides important core authentication technology in the IoT. Since 2015, respondents who say IoT is the most important trend driving the deployment of applications using PKI has increased significantly from 21 percent of respondents in 2015 to 47 percent in 2020. In contrast, cloud-based services decreased from 64 percent of respondents in 2015 to 44 percent of respondents in 2020 (Figure 3). This should define the challenges facing PKI vendors and administrators alike as they adapt the technology to these new realities.

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

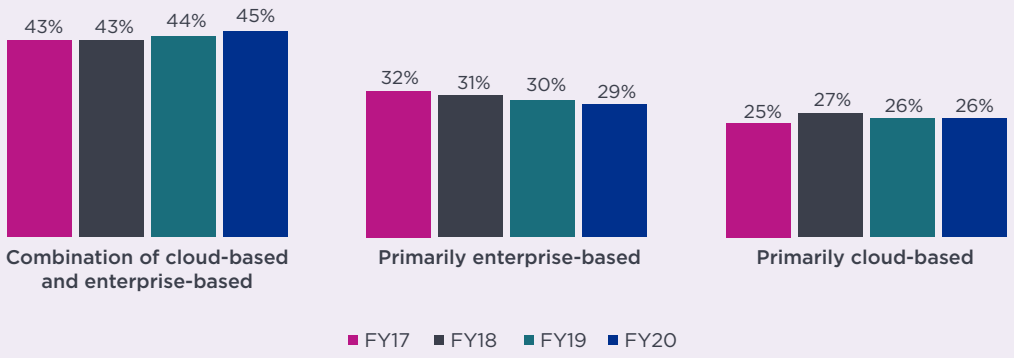
Consolidated view; two responses permitted



> «...the rapid growth in the use of IoT devices is having an impact on the use of PKI technologies and there is realization that PKI provides important core authentication technologies for the IoT.»

In the next two years, an average of 41 percent of IoT devices in use will rely primarily on digital certificates for identification and authentication. As shown in Figure 4, 45 percent of respondents believe that as the IoT continues to grow supporting PKI deployments for IoT device credentialing will be a combination of cloud-based and enterprise-based.

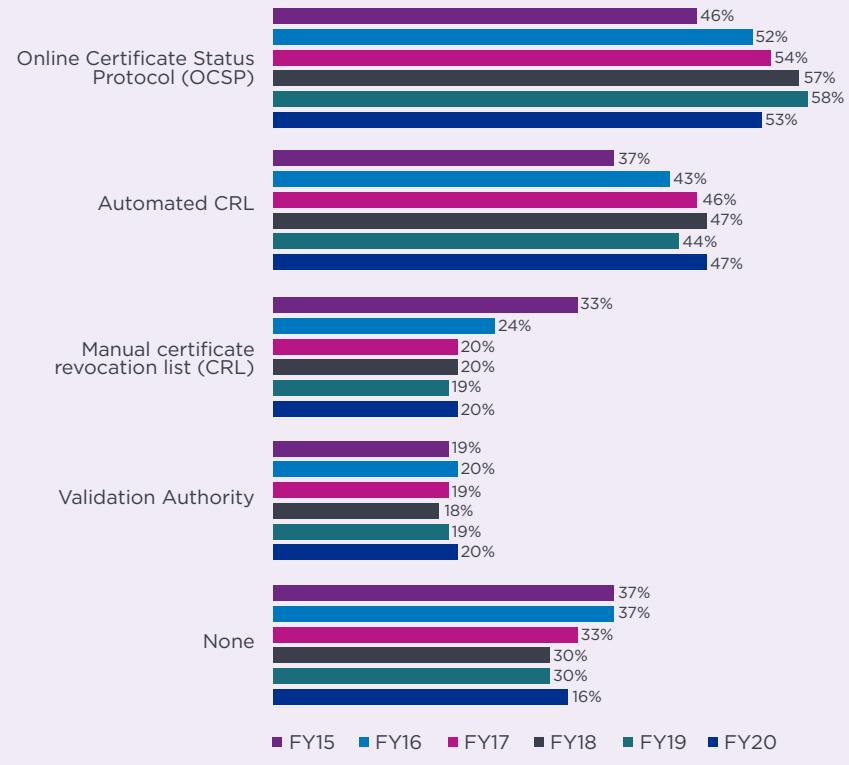
Figure 4. What supporting PKI deployments for IoT device credentialing will be as the IoT continues to grow?



Trends in PKI Maturity

According to Figure 5, the certificate revocation technique most often deployed continues to be online certificate status protocol (OCSP), according to 53 percent of respondents (an increase from 46 percent of respondents since the 2015 study). The next most popular technique is the use of automated certificate revocation list (CRL), according to 47 percent of respondents.

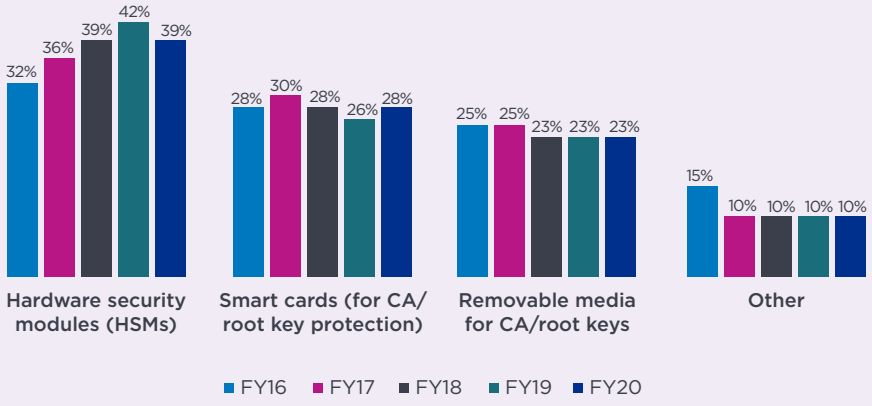
Figure 5. The certificate revocation techniques used in enterprises
Consolidated view; more than one response permitted



Similar to last year, 32 percent of respondents say they do not deploy a certificate revocation technique. There are many possible explanations for this high percentage – use of alternate means to remove users/devices, use of short lifespan certificates, closed systems, etc.

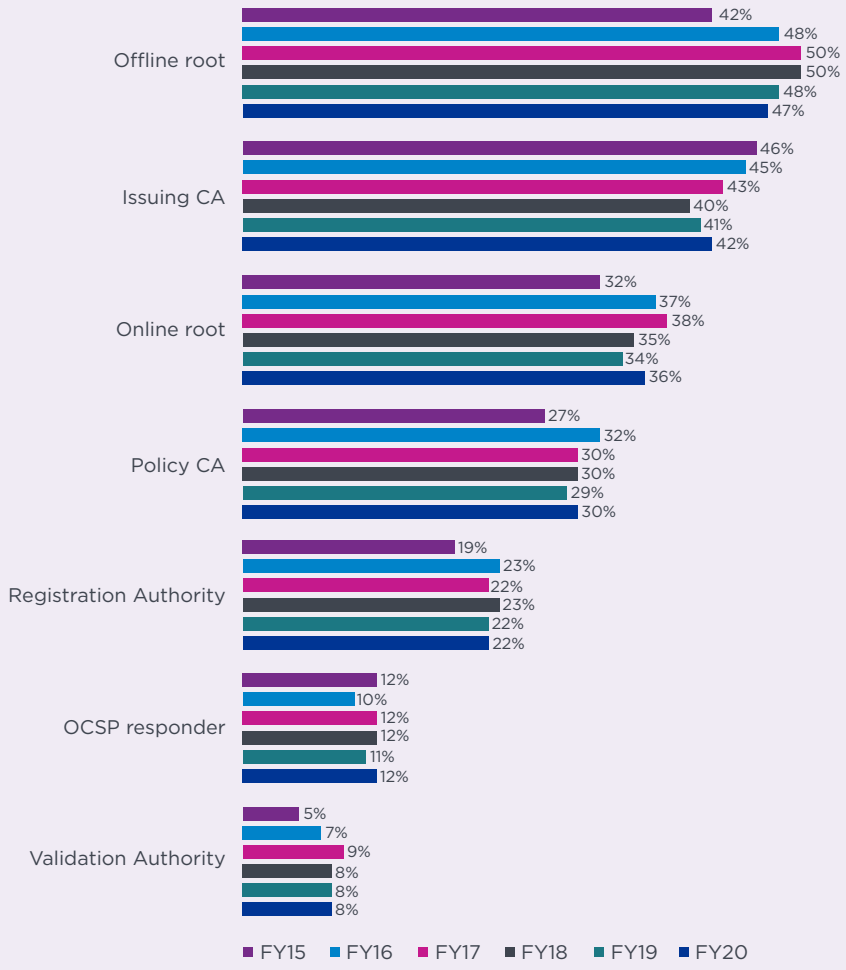
Hardware security modules (HSMs) are most often used to manage the private keys for their root/policy/issuing CAs, as shown in Figure 6. Twenty-eight percent of respondents say smart cards are used. Forty-five percent of respondents say they have PKI specialists on staff who are involved in their organizations' enterprise PKI.

Figure 6. How do you manage the private keys for your root/policy/issuing CAs?



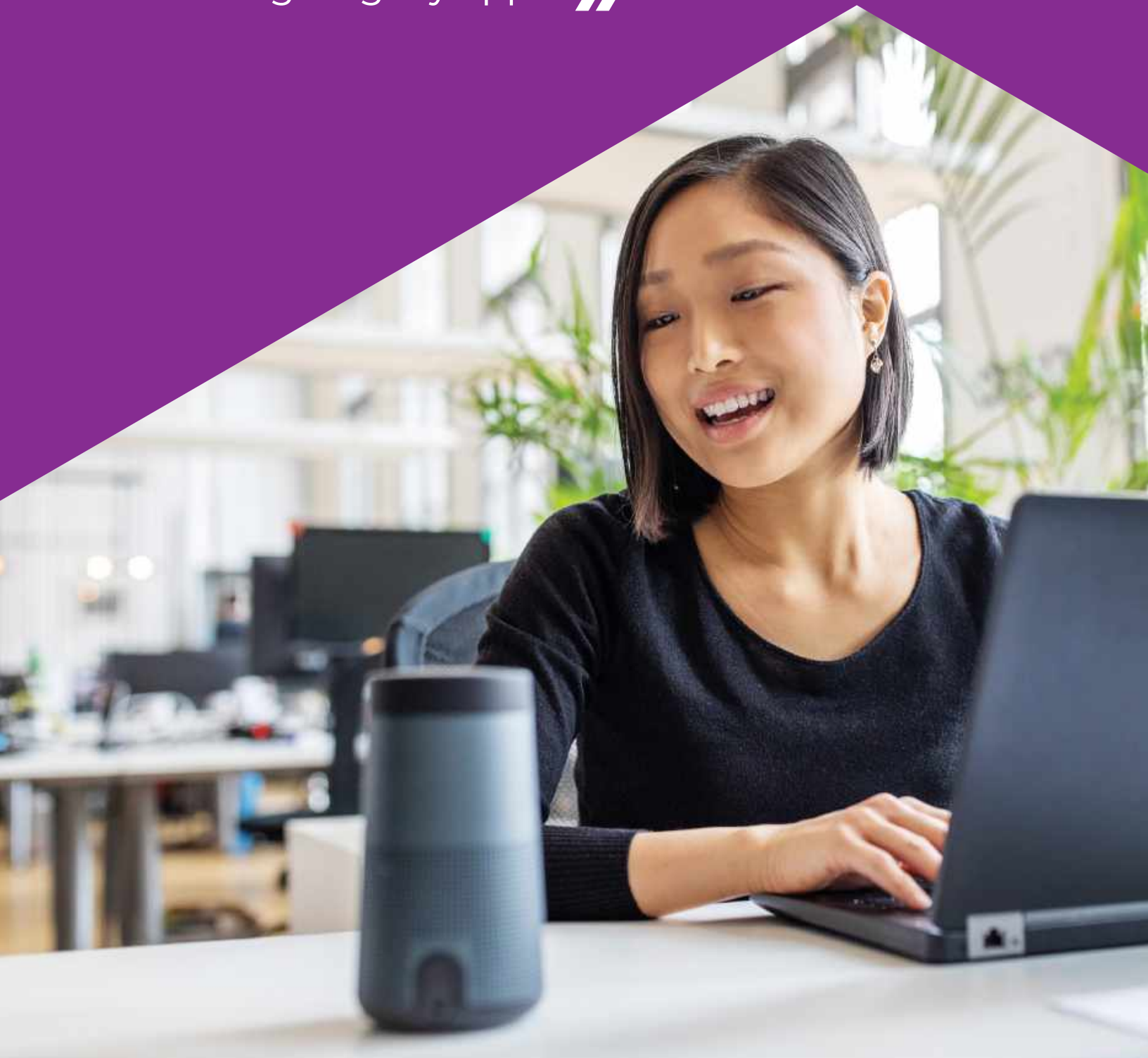
Of the 39 percent of organizations in this study that use HSMs to secure PKI, they are used across the entire architecture of the PKI as shown in Figure 7. As an example of best practice, NIST calls to "Ensure that Cryptographic modules for CAs, Key Recovery Servers, and OCSP responders are hardware modules validated as meeting FIPS 140-2 Level 3 or higher" (NIST Special Publication 800-57 Part 3). Yet, only 12 percent of our respondents indicate the presence of HSMs in their OCSP installations. This is a significant gap between best practices and observed practices.

Figure 7. Where HSMs are deployed to secure PKI
Consolidated view; more than one response permitted



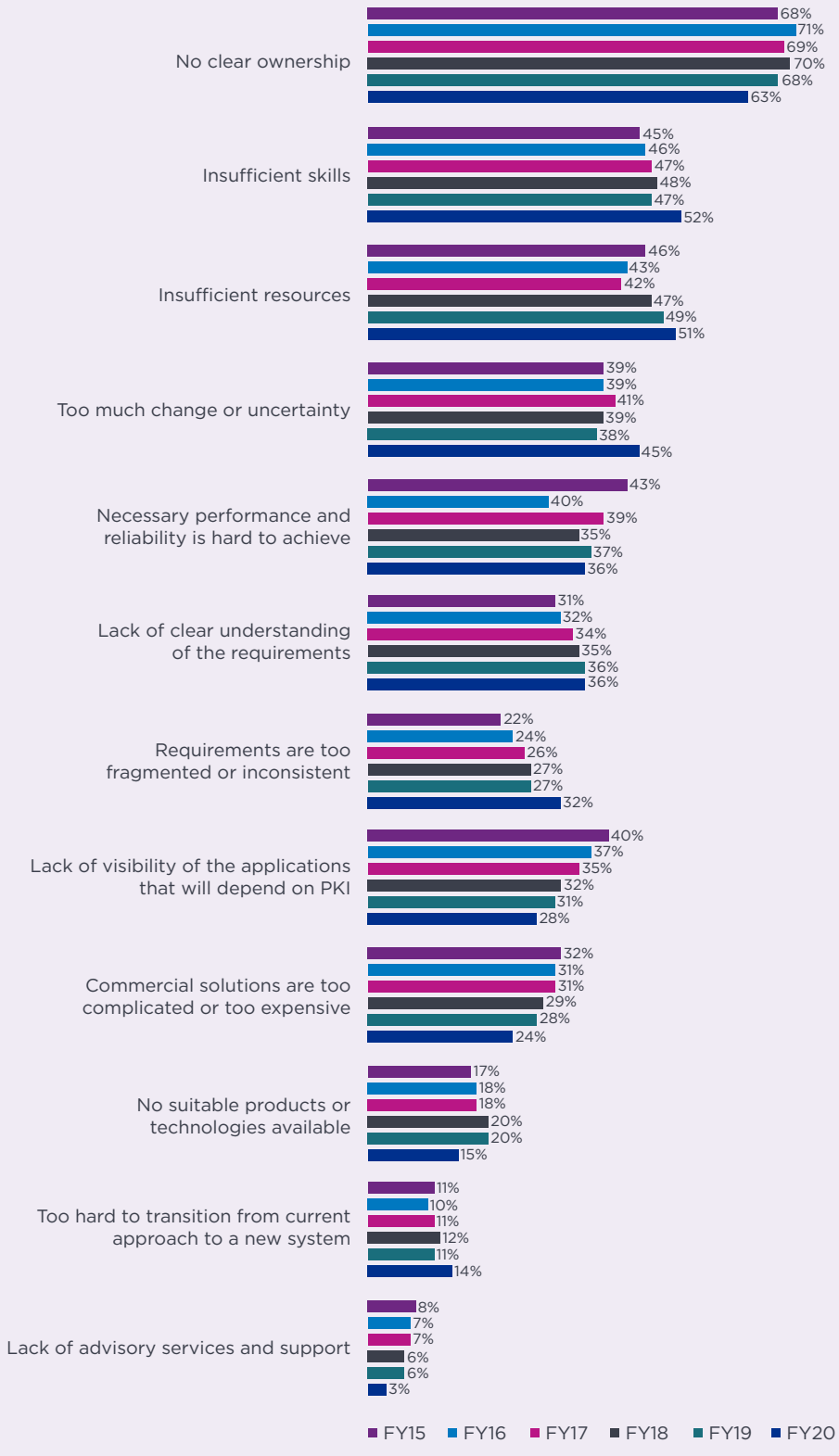
> In the next two years, an average of 41 percent of IoT devices in use will rely primarily on digital certificates for identification and authentication.

« The primary challenges to enabling applications to utilize PKI are the lack of visibility of the security capabilities of existing PKI, the inability of existing PKI to support new applications and the inability to change legacy apps. »



No clear ownership, insufficient resources and skills are the top three challenges to enabling applications to use PKI. As shown in Figure 8, the most significant challenges are based on organizational issues. These include no clear ownership (63 percent of respondents), insufficient skills (52 percent) and insufficient resources (51 percent).

Figure 8. The challenges in deploying and managing PKI
Consolidated view; four responses permitted

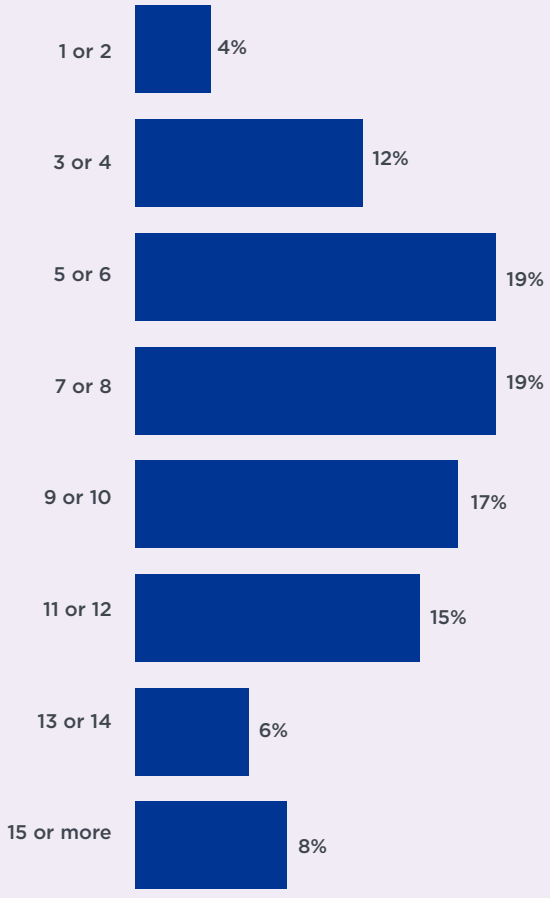


Too much change or uncertainty has increased from 38 percent of respondents in last year's research to 45 percent of respondents in 2020, and requirements that are too fragmented or inconsistent has increased from 22 percent of respondents in 2015 to 32 percent of respondents in 2020.

Trends in PKI challenges

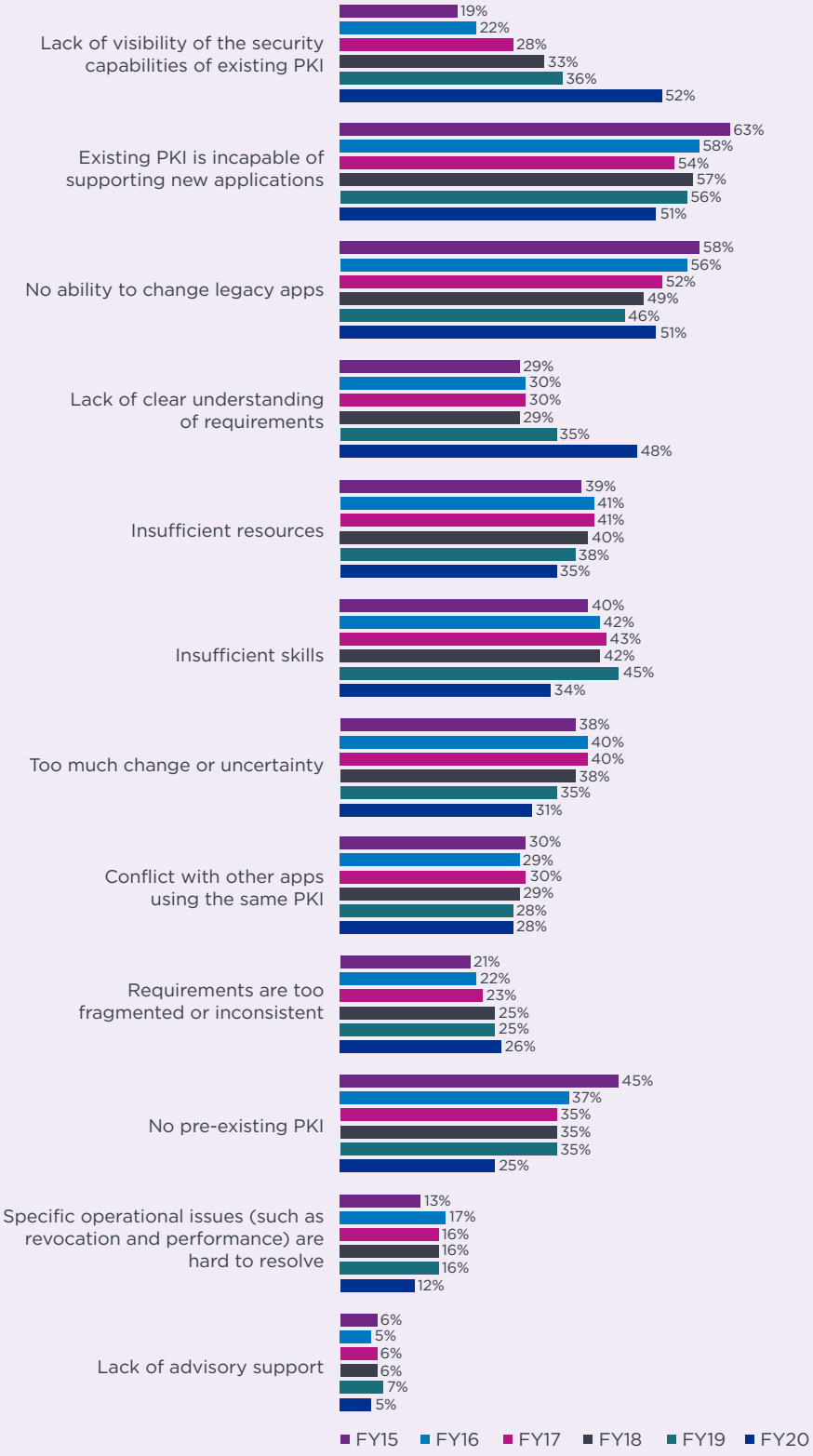
Organizations with internal CAs use an average of 7.2 separate CAs, managing an average of 56,192 internal or externally acquired certificates. As shown in Figure 9, an average of 8.32 distinct applications, such as email and network authentication, are managed by an organization's PKI. This indicates that the PKI is at the core of the enterprise IT backbone. Not only the number of applications dependent upon the PKI but the nature of them indicates that the PKI is a strategic part of the core IT backbone.

Figure 9. How many distinct applications does your PKI manage certificates on behalf of in 2020?
Consolidated view; extrapolated value is 8.32 distinct applications



The primary challenges to enabling applications to utilize PKI are the lack of visibility of the security capabilities of existing PKI, the inability of existing PKI to support new applications and the inability to change legacy apps. As shown in Figure 10, since 2019 the lack of visibility of the security capabilities of existing PKI increased significantly from 36 percent of respondents to 52 percent of respondents.

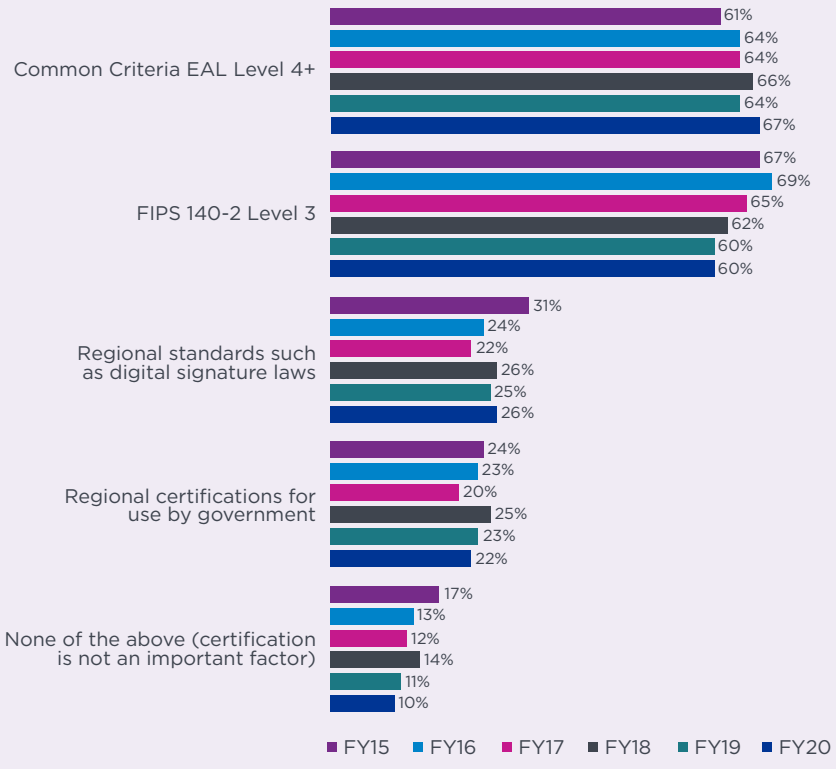
Figure 10. What are the challenges to enable applications to utilize PKI?
Consolidated view; four responses permitted



Also increasing is the inability to change legacy apps (from 46 percent to 51 percent of respondents) and the lack of clear understanding of requirements (from 35 percent to 48 percent of respondents).

Common Criteria EAL Level 4+ is the most important security certification when deploying PKI infrastructure and PKI-based applications. According to Figure 11, 67 percent say Common Criteria followed by 60 percent who say FIPS 140 is the most important when deploying PKI. Twenty-six percent of respondents say regional standards such as digital signature laws are important (a decrease from 31 percent in 2015). In the US, FIPS 140 is the standard called out by NIST in its definition of a "cryptographic module" which is mandatory for most US federal government applications and a best practice in all PKI implementations.

Figure 11. Security certifications important when deploying PKI infrastructure
Consolidated view, more than one response permitted

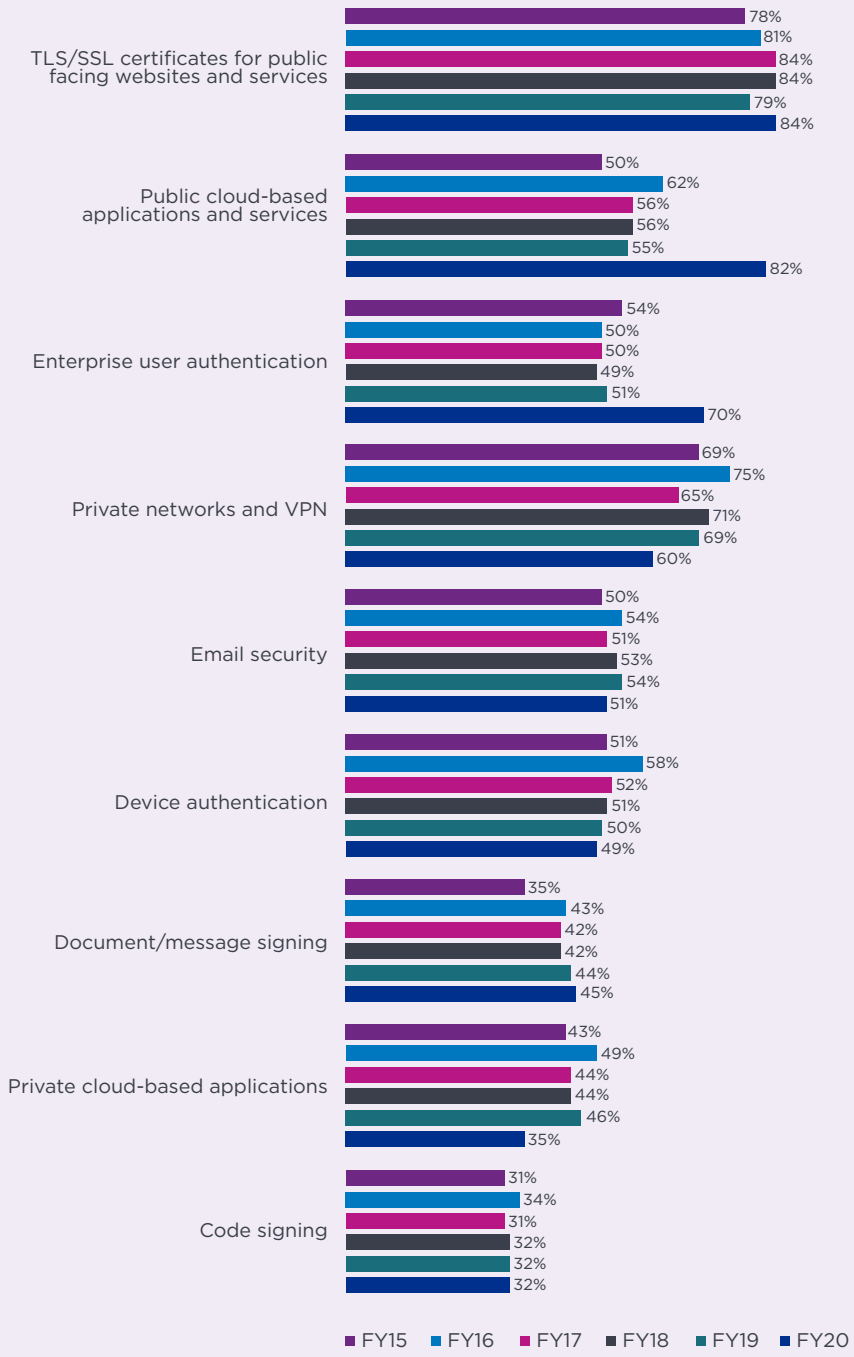


« Common Criteria EAL Level 4+ is the most important security certification when deploying PKI infrastructure and PKI-based applications. »

« The use of PKI credentials for public cloud-based applications and services increased significantly from 55 percent to 82 percent of respondents. »

The use of PKI credentials for public cloud-based applications and services increased significantly from 55 percent to 82 percent of respondents. According to Figure 12, 84 percent of respondents say the application most often using PKI credentials is TLS/SSL certificates for public-facing websites and services. The use of public cloud-based applications and services increased significantly from 55 percent to 82 percent of respondents. Private networks and VPN using PKI credentials decreased from 69 percent in 2019 to 60 percent of respondents in 2020. These are the basic building blocks of the modern enterprise IT system and digital certificates have become much like storage, a commodity component of the system, no longer an exotic add on.

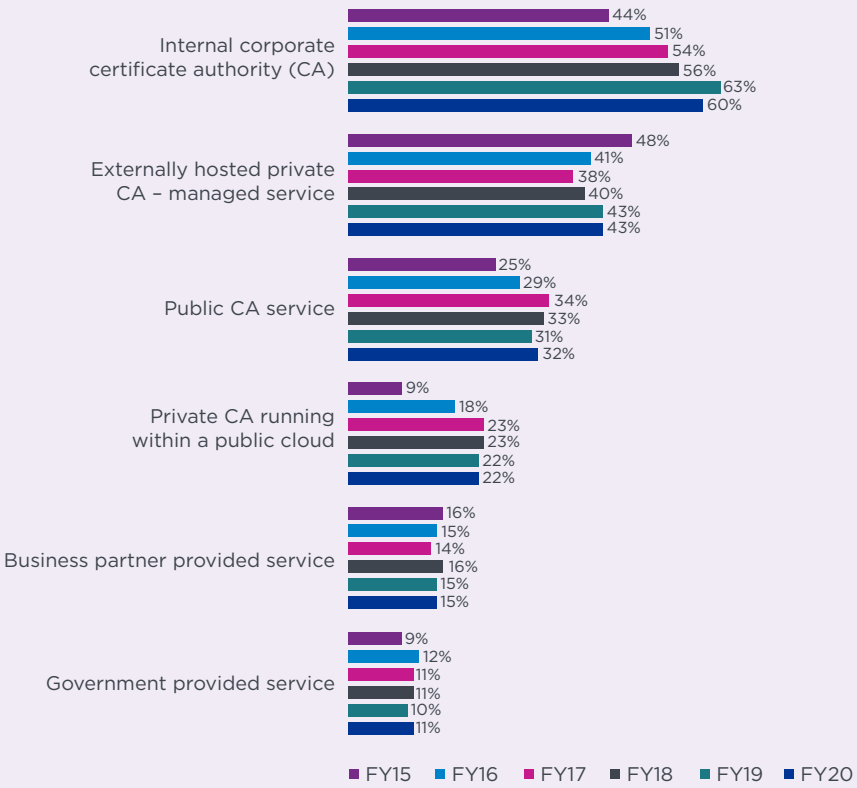
Figure 12. What applications use PKI credentials in organizations?
Consolidated view; more than one response permitted



What are the most popular methods for deploying enterprise PKI? The most cited method for deploying enterprise PKI, according to Figure 13, is through an internal corporate certificate authority (CA) or an externally hosted private CA – managed service, according to 60 percent and 43 percent of respondents, respectively.

Externally hosted private CAs, after a decline from 2015 to 2017, have increased in usage. Since 2015, more companies have deployed PKI using a private CA running within a public cloud, an increase from 9 percent to 22 percent of respondents.

Figure 13. How is PKI deployed?
Consolidated view; more than one response permitted

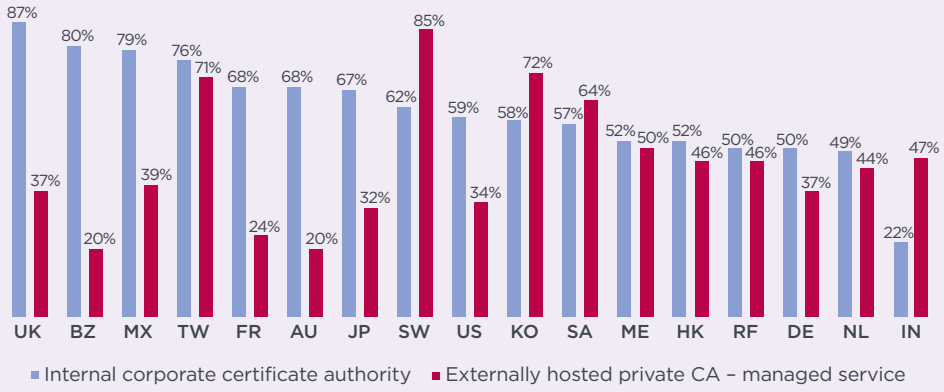


Global Analysis

Figure 14 shows how PKI is deployed within respondents' organizations. As shown, the United Kingdom, Brazil, Mexico and Taiwan are most likely to choose internal corporate certificate authority. In contrast, Sweden, Korea and Southeast Asia respondents are most likely to choose external hosted private certificate authorities as a managed service.

Country	Abbreviated
Australia	AU
Brazil	BZ
France	FR
Germany	DE
Hong Kong	HK
India	IN
Japan	JP
Mexico	MX
Middle East	ME
Netherlands	NL
Russian Federation	RF
Southeast Asia	SA
South Korea	SK
Sweden	SW
Taiwan	TW
United Kingdom	UK
United States	US

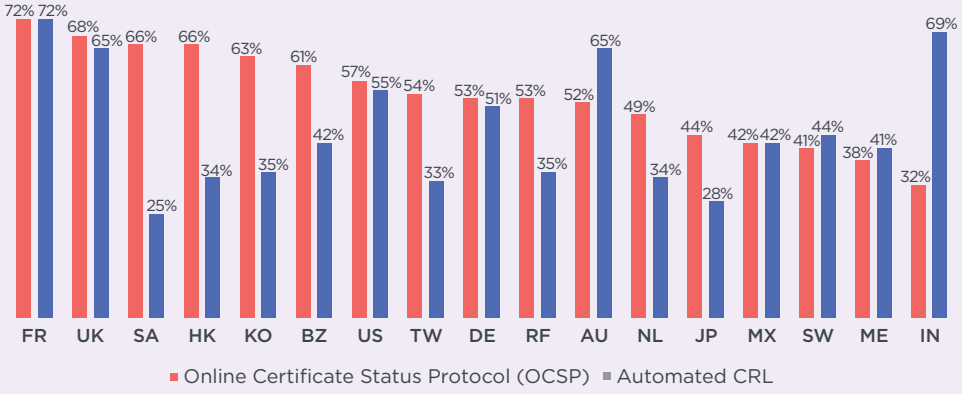
Figure 14. How would you describe how your organization's enterprise PKI is deployed?
Top 2 choices



When asked about the revocation techniques deployed, 32 percent of respondents said none. As shown in Figure 15, of those respondents who say their organizations use a certificate revocation technique, France, the United Kingdom, Southeast Asia and Hong Kong respondents are most likely to use online certificate status protocols (OCSP). France, the United Kingdom and Australia are most likely to use automated CRLs.

As noted above, this implies a true chasm between operational best practices and observed practices. Certificates have a life span. During that life span circumstances change and certificates outlive their purpose. Without a method of revoking certificates, the population of valid, extant certificates simply grows.

Figure 15. Which certificate revocation technique does your organization deploy?
Top 2 choices = OCSP and Automated CRL



We can surmise that there are connections between this observed deviation from best practices and the significant lack of dedicated personnel and skills called out in the study. When something as basic as lack of revocation processes is this common, one has to wonder about the currency of documentation on and processes for managing the average of eight major enterprise applications that are dependent on the PKI.

According to Figure 16, the US and Germany have the most individual CAs deployed within their organizations (9.41 and 8.75, respectively). Mexico and Russian Federation have the least number of individual CAs (5.62 and 5.26, respectively).

Again, this reinforced the penetration of the PKI into the core IT backbone of the modern organization. And, given the stated lack of skilled personnel and organizational clarity, combined with the lack of consistent revocation practices, one has to draw attention to risks to the health and integrity of these CAs and the important core enterprise applications that use their certificates.

> « Externally hosted private CAs, after a decline from 2015 to 2017, have increased in usage. Since 2015, more companies have deployed PKI using a private CA running within a public cloud... »

Figure 16. What best describes the number of individual CAs in your organization?
Extrapolated average values

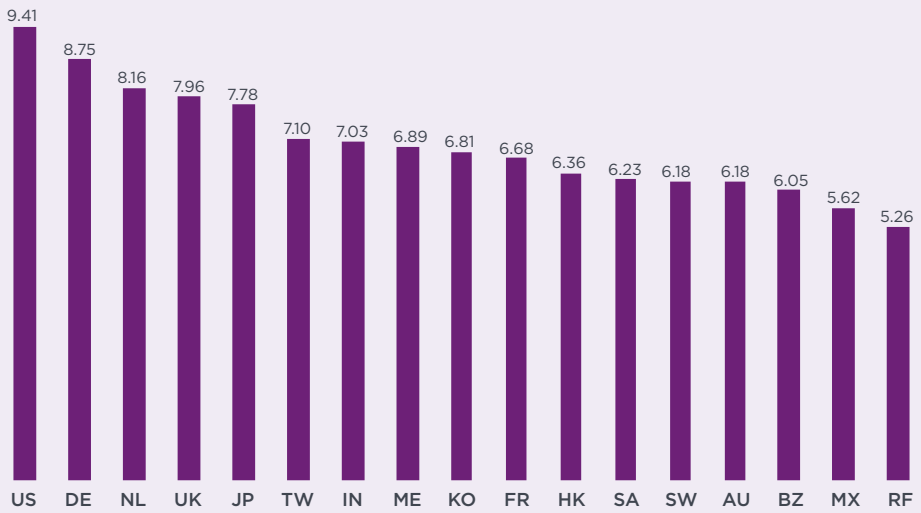
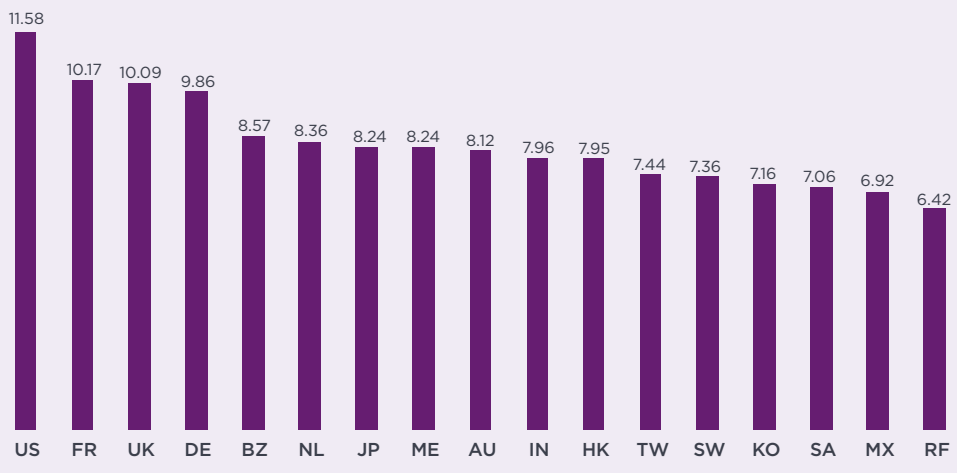


Figure 17 shows the number of distinct applications (e.g., email, network authentication, etc.) for which PKI manages certificates. US at 11.58 has the largest number of distinct applications. Mexico (6.92) and Russia (6.42) have the smallest number of distinct applications, respectively.

Figure 17. How many distinct applications does your PKI manage certificates on behalf of?
Extrapolated average values



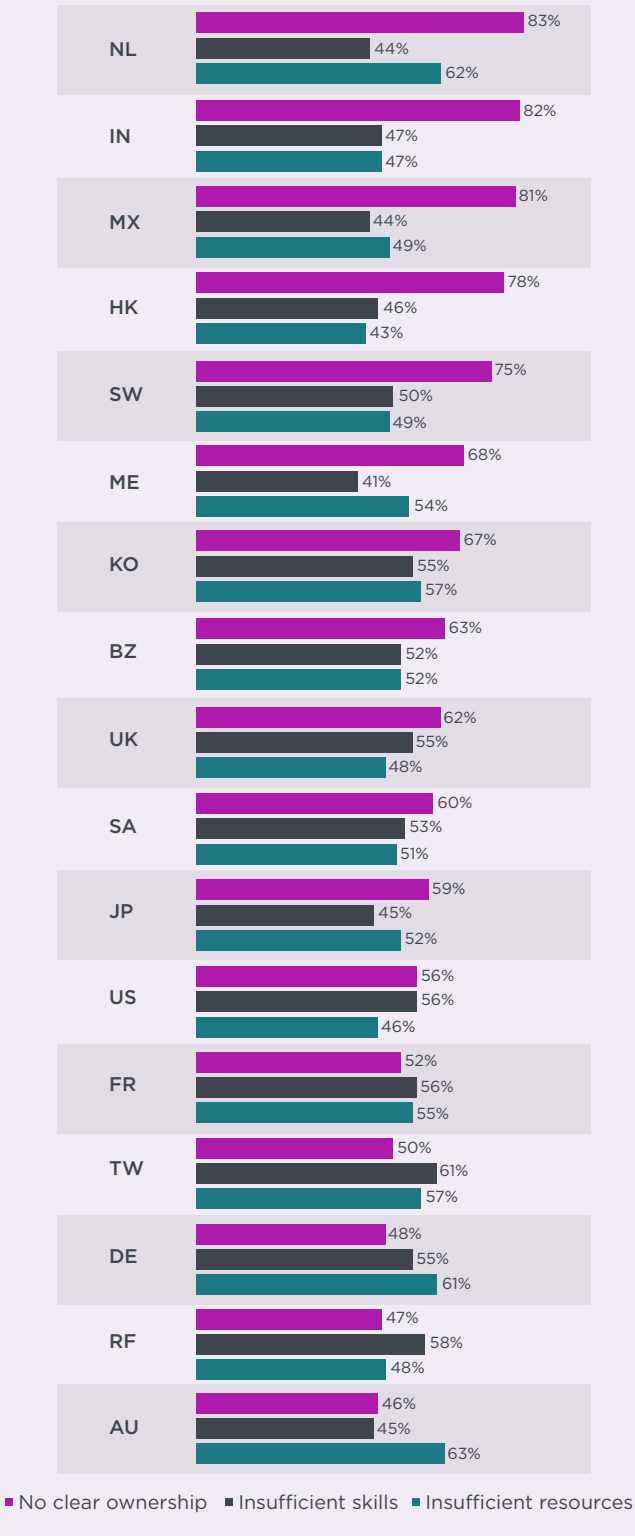
One should note that even in the lowest figures that the average number of applications is just north of 6. Given previous responses, we can extrapolate that these likely include email, SSL certificates, device identification and logon credentials. These are non-trivial applications, the failure of which could pose existential risks to the host organization.

Figure 18 on the following page reports the three most salient challenges in deploying and managing PKI. As shown, the Netherlands, India and Mexico respondents are most likely to say no clear ownership as their most significant challenge. Taiwan and Russian Federation respondents are most likely to say insufficient resources. Australian, the Netherlands and German respondents are most likely to cite insufficient skills as a top three challenge.

There is a consistent theme in these responses. We can see the importance of the PKI growing and its integration with core IT applications. Also, PKI's near-term future is being buffeted by trends towards the cloud, mobility and the IoT. However, globally there is a lack of trained people and tendency towards fuzzy ownership of the PKI.

This is a significant departure from known best practices that require direct lines of responsibility for all PKI dependent applications and clear documentation of the dependencies and risk mitigation strategies. One has to wonder about the condition of required PKI documentation and processes given these high rates of skills and personnel shortages.

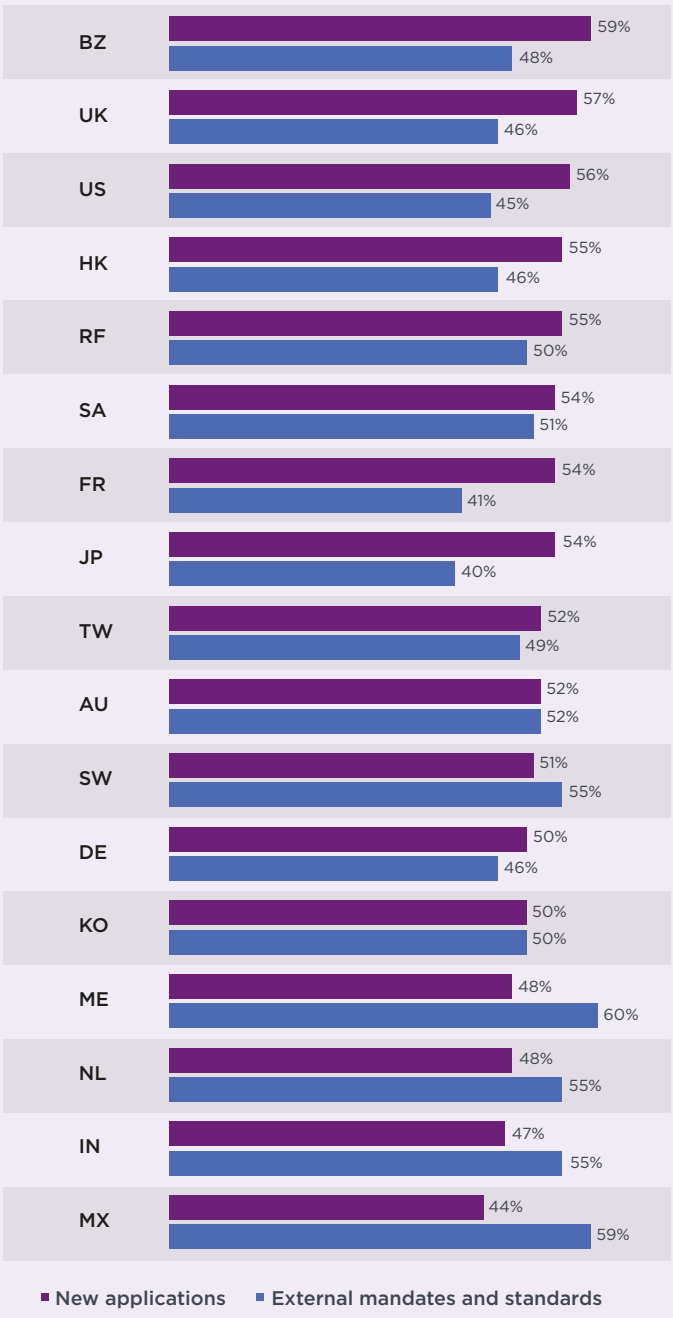
Figure 18. What are the main challenges in deploying and managing PKI?
Top 3 choices



As organizations plan the evolution of their PKI, where are the greatest areas of possible change and uncertainty? Figure 19 provides the top two choices. Accordingly, Brazil, the United Kingdom and United States respondents say new applications such as IoT are driving change and uncertainty. The Middle East and Mexico organizations are more likely to say that external mandates and standards are driving change and uncertainty.

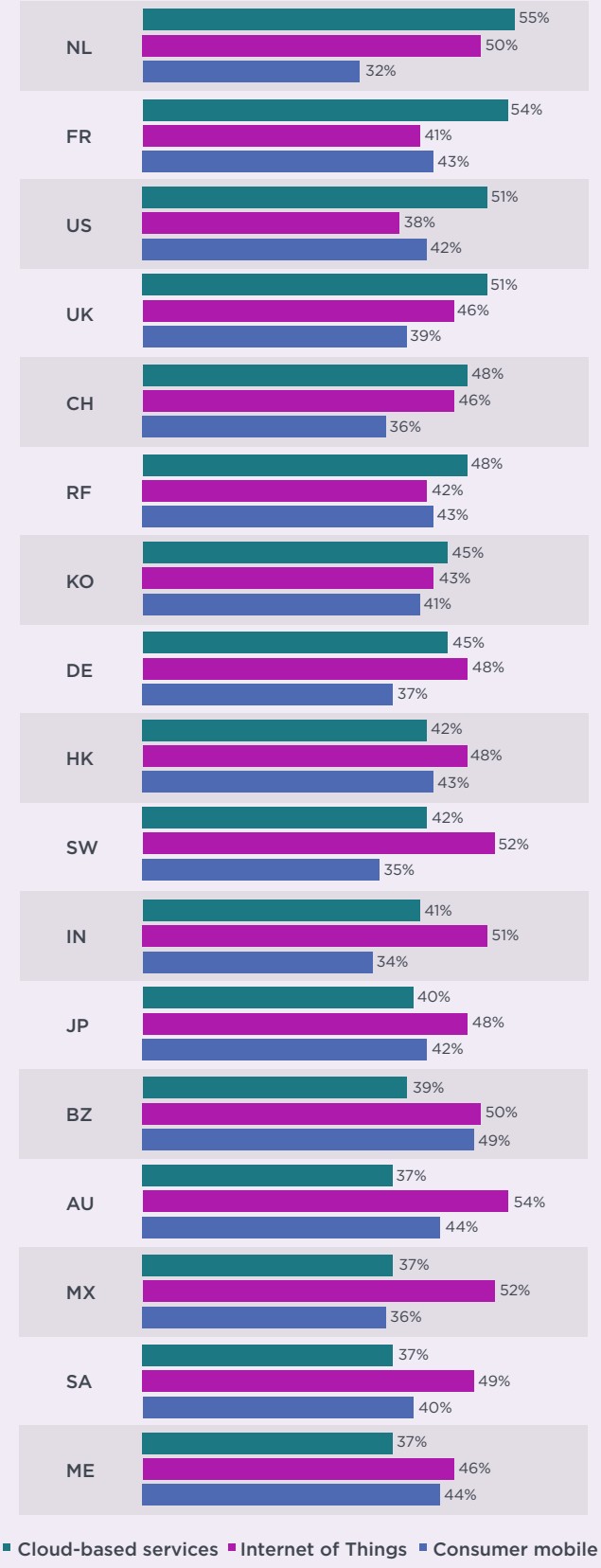
Figure 20 on the following page reports what respondents believe are the most important trends that are driving the deployment of applications that make use of PKI. As can be seen, the Netherlands, France, the United States and United Kingdom are most likely to cite cloud-based services as driving the deployment of applications that make use of PKI.

Figure 19. Where are the greatest areas of change and uncertainty in the evolution of your PKI?
Top 2 choices



Australia, Mexico and Sweden respondents are most likely to see IoT as a driver to PKI adoption. Brazil, Australia and the Middle East are more likely to see consumer mobile as a driver.

Figure 20. What are the most important trends that are driving the deployment of applications that make use of PKI?
Top 3 choices



03 METHODS

Table 1 reports the consolidated sample response for 17 separate country samples. Data collection was started in December 2019 and completed in January 2020. Our consolidated sampling frame of practitioners in all countries consisted of 69,574 individuals who have bona fide credentials in IT or security fields. From this sampling frame, we captured 6,903 returns of which 746 were rejected for reliability issues. From our final consolidated 2020 sample of 6,903, we calculated the PKI subsample to be 1,934.

Table 1. Sample response	Frequency
Sampling frame	169,574
Total returns	6,903
Rejected or screened surveys	746
Overall sample (encryption trends)	6,157
PKI subsample	1,934
Ratio subsample to overall sample	31%

Figure 21 reports the respondent's organizational level within participating organizations. By design, 55 percent of respondents are at or above the supervisory levels and 44 percent of respondents reported their position as associate/staff/technician. Respondents have on average 8.5 years of security experience with approximately 5.6 years of experience in their current position.

Figure 22 identifies the organizational location of respondents in our study. Over half (55 percent) of respondents are located within IT operations. This is followed by security at 20 percent of respondents and lines of business at 9 percent of respondents.

Figure 21. Distribution of respondents according to position level
Country samples are consolidated

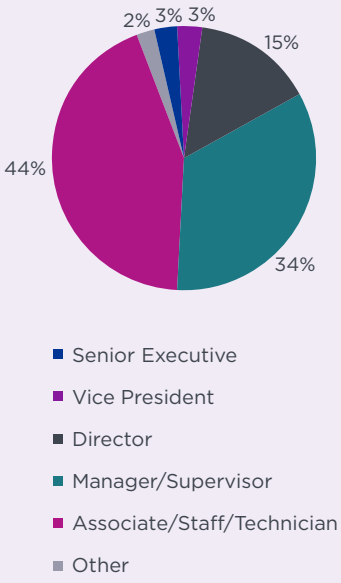


Figure 22. Distribution of respondents according to functional area

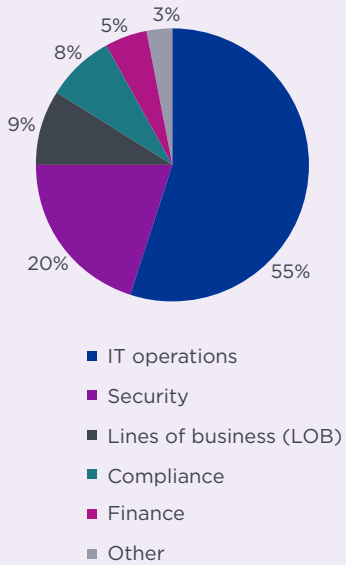


Figure 23 reports the industry classification of respondents' organizations. Fifteen percent of respondents are located in the financial services industry, which includes banking, investment management, insurance, brokerage, payments and credit cards. Twelve percent of respondents are located in manufacturing and industrial organizations and 11 percent of respondents are in service organizations. Another nine percent are located in the technology and software sector.

According to Figure 24, more than half (55 percent) of respondent are located in larger-sized organizations with a global headcount of more than 1,000 employees.

Figure 23. Distribution of respondents according to primary industry classification
Country samples are consolidated

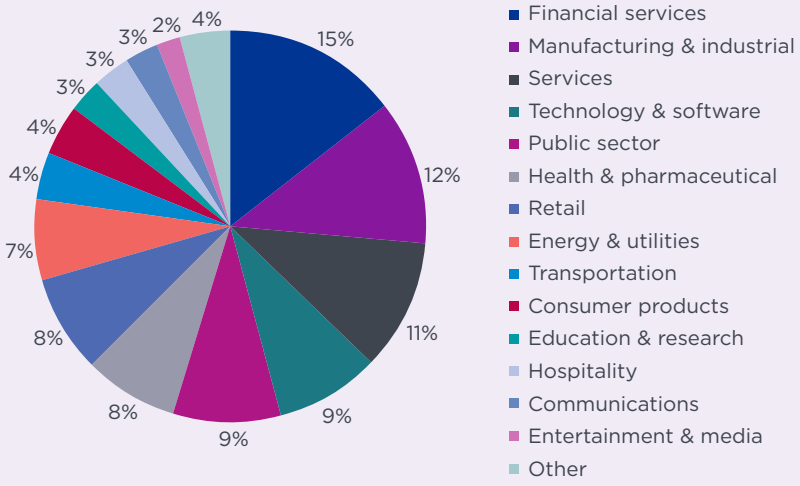
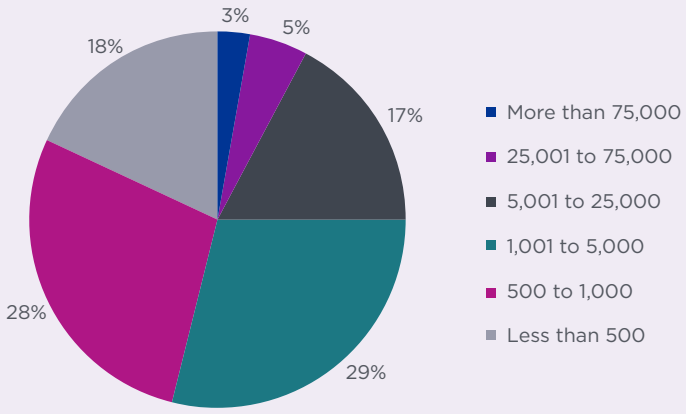


Figure 24. Distribution of respondents according to organizational headcount
Country samples are consolidated



04 LIMITATIONS

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from the presented findings. The following items are specific limitations that are germane to most survey-based research studies.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of IT and IT security practitioners in 17 countries resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the survey.

Sampling-frame bias: The accuracy of survey results is dependent upon the degree to which our sampling frames are representative of individuals who are IT or IT security practitioners within global companies represented in this study.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from respondents. While certain checks and balances were incorporated into our survey evaluation process including sanity checks, there is always the possibility that some respondents did not provide truthful responses.

About Ponemon Institute

The Ponemon Institute© is dedicated to advancing responsible information and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations in a variety of industries.

About nCipher Security

nCipher Security, an Entrust company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity and control to their business critical information and applications. Today's fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency – it also multiplies the security risks. Our cryptographic solutions secure emerging technologies such as cloud, IoT, blockchain, and digital payments and help meet new compliance mandates. We do this using our same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensure the integrity of your data and put you in complete control – today, tomorrow, always. **www.ncipher.com**

About Entrust Corporation

Entrust secures a rapidly changing world by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us. **www.entrust.com**

entrust.com

ncipher.com