THALES

Ponemon INSTITUTE

2017 PKI GLOBAL TRENDS STUDY

October 2017

TABLE OF CONTENTS

Sponsored by Thales eSecurity

INDEPENDENTLY CONDUCTED BY PONEMON INSTITUTE LLC

PART 1. EXECUTIVE SUMMARY

The rise of the Internet of Things (IoT) in the enterprise and its impact on how organizations design and build their public key infrastructure (PKI) is a key theme in this year's study. Specifically, IoT is the fastest trend driving the deployment of applications using PKI.

While external mandates and standards and enterprise applications have declined in companies' concerns about change and uncertainty, in the past three years the focus on how new applications such as IoT will affect PKI uncertainty has increased significantly.

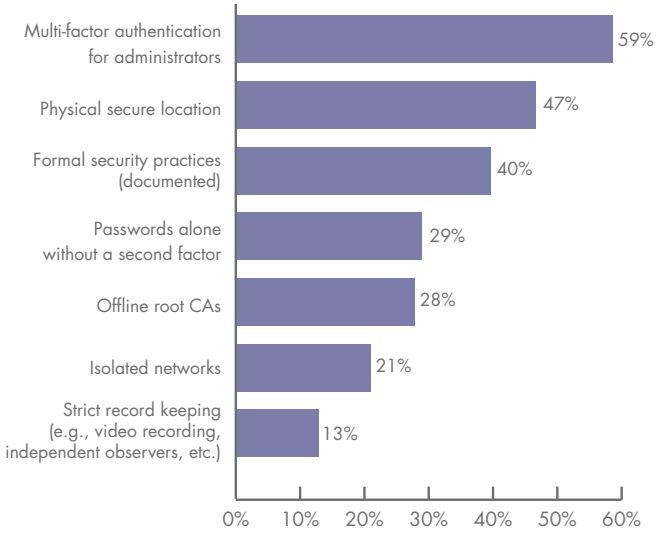
On average, companies today are using their PKI to support over *eight* different applications. Yet the findings of this study indicate a general lack of clear ownership of PKIs, as well as a lack of resources and skills to properly support them. Current approaches to PKI are fragmented and do not always incorporate best practices, indicating a need for many organizations to apply increased effort to securing their PKI as an important part of creating a foundation of trust.[1]

Ponemon Institute is pleased to present the findings of the *2017 PKI Global Trends Study*, sponsored by Thales eSecurity. This report summarizes the third annual results of a survey completed by 1,510 IT and IT security practitioners in the following 11 countries: the United States, the United Kingdom, Germany, France, Australia, Japan, Brazil, Russian Federation, India, Mexico and Arabia. The report tabulates the responses to the survey and draws some limited conclusions as to how best practices are reflected in observed practices, and the influence of cloud computing, the Internet of Things, and other important industry trends.

This work is part of a larger study published in April 2017 involving 4,802 respondents in 11 countries.[2] The purpose of this research is to better understand the use of PKI in organizations. 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.

Figure 1 shows the primary practices organizations take to secure PKI and Certificate Authorities (CAs). The top two are multifactor authentication for administrators and a secure physical location (59 percent and 47 percent of respondents, respectively).

Figure 1. Practices used to secure PKI and Certificate Authorities



[1] Best practices for designing, fielding and maintaining a PKI can be derived from various public documents, for example the Webtrust standards (http://www.webtrust.org/item64428.aspx) and NIST Publication 800-57 Parts 1-3.

[2] See: *2017 Global Encryption Trends Study* (sponsored by Thales eSecurity), Ponemon Institute, April 2017.

Other key findings include the following:

PKI changes and uncertainty due to new applications, such as the IoT, increased dramatically since 2015. Respondents who are concerned about the impact of the IoT on PKI increased from 14 percent to 36 percent.

IoT is growing as an important trend driving the deployment of applications using PKI. While the most important trend driving the deployment of applications that make use of PKI continues to be cloud-based services (54 percent of respondents), IoT increased from 21 percent to 40 percent of respondents over the past three years.

In the next two years, an average of 43 percent of IoT devices in use will rely primarily on digital certificates for identification and authentication.

How are private keys for root/policy/issuing CAs managed? Hardware security modules (HSMs) are used by 36% of respondents to manage the private keys for root/policy/issuing CAs.

The challenge of dealing with a lack of visibility of the security capabilities of existing PKI grows. The lack of visibility of the security capabilities of an existing PKI has increased from 19 percent in 2015 to 28 percent of respondents in this year's research.

The main PKI deployment challenge continues to be the lack of clear ownership of the PKI function. Sixty-nine percent of respondents believe there is no one function responsible for managing PKI, a slight increase from 2015.

FIPS 140 and Common Criteria are the most important security certifications when deploying PKI infrastructure and PKI-based applications. Sixty-five percent say FIPS 140 is most important and this is closely followed by Common Criteria (64 percent of respondents) when deploying PKI.

SSL certificates for public facing websites and services increase the use of PKI credentials significantly. Applications most often using PKI credentials are SSL certificates for public facing websites and services (84 percent of respondents).

"IN THE NEXT TWO YEARS, AN AVERAGE OF 43 PERCENT OF IoT DEVICES IN USE WILL RELY PRIMARILY ON DIGITAL CERTIFICATES FOR IDENTIFICATION AND AUTHENTICATION."

PART 2. KEY FINDINGS

In this section of the report we provide an analysis of the global results. The complete audited findings are presented in the Appendix of this report. The results are grouped into three categories:

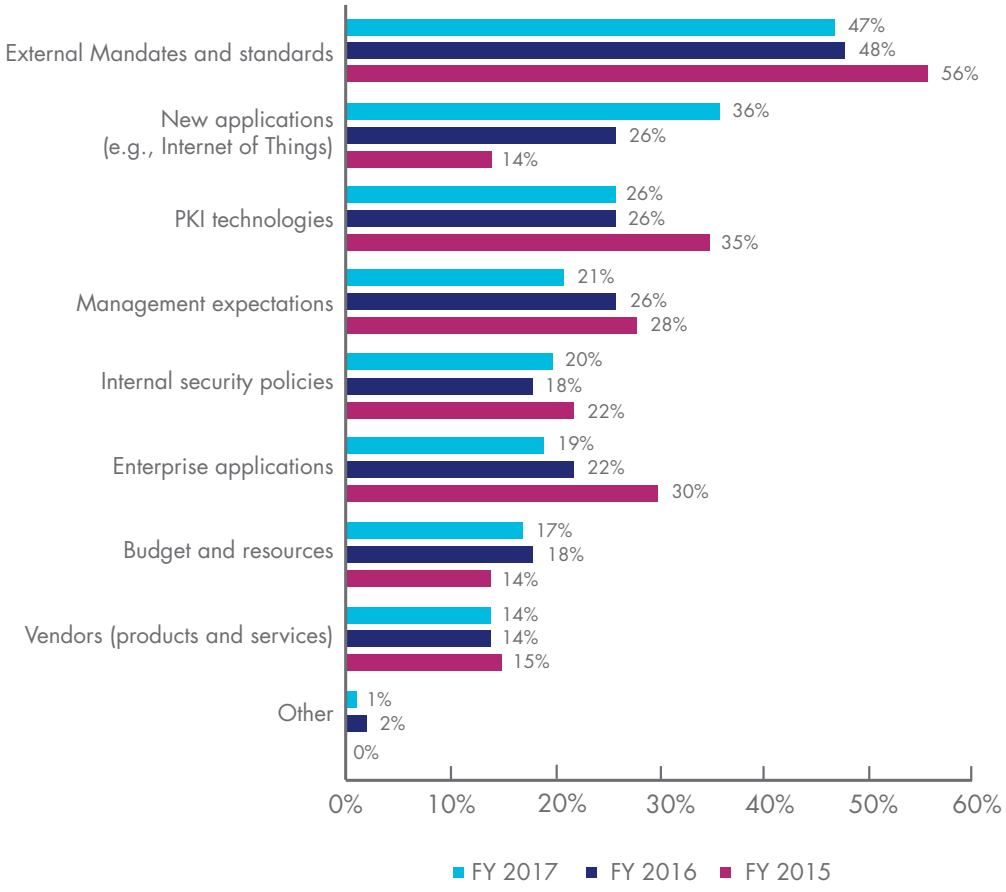
- The increasing influence of the IoT in PKI planning
- Trends in PKI maturity
- Trends in PKI challenges

The increasing influence of the IoT in PKI planning

PKI changes and uncertainty due to new applications, such as the IoT, increased dramatically since 2015. According to Figure 2, since 2015 respondents who are concerned about the impact of the IoT on PKI increased from 14 percent to 36 percent. In contrast, external mandates and standards and enterprise applications saw a decrease in concerns about change (from 47 percent and 19 percent in 2015, respectively).

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

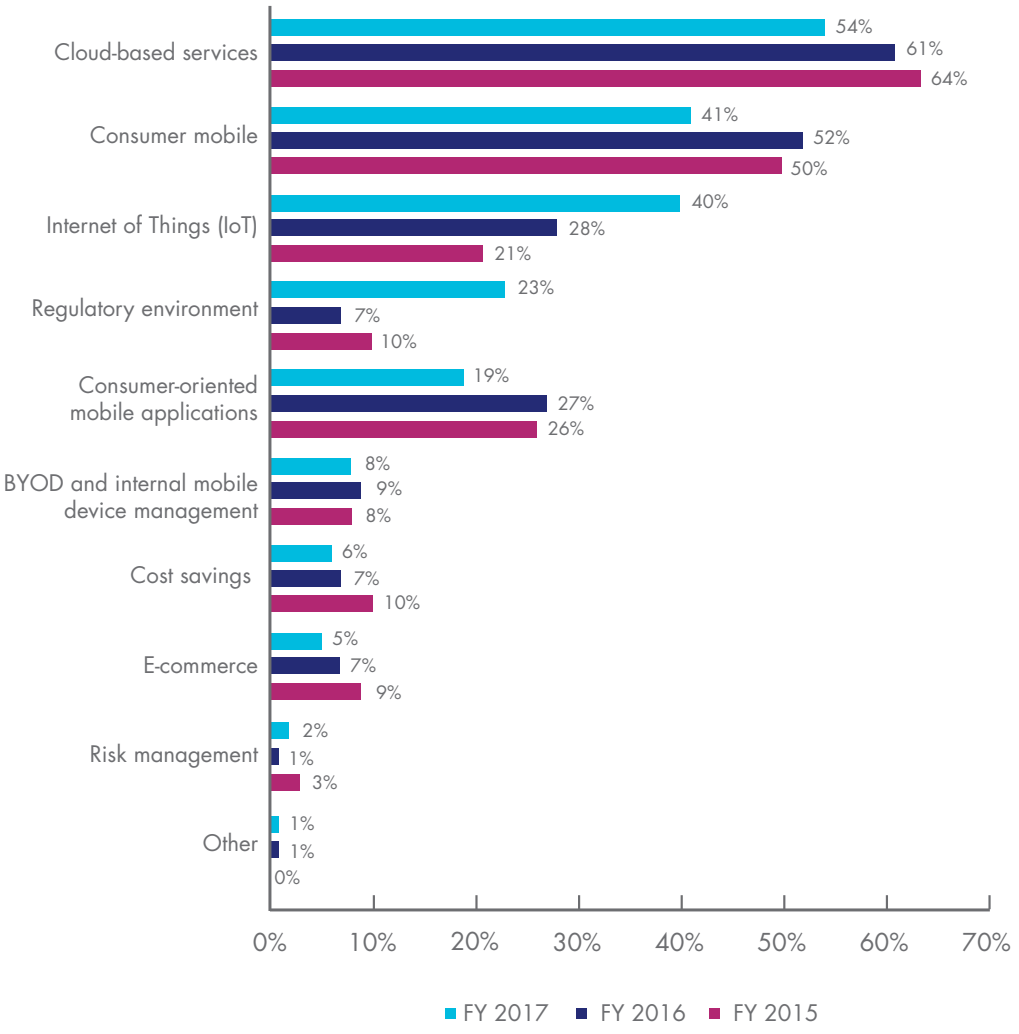
Consolidated view; two responses permitted



IoT is growing as an important trend driving the deployment of applications using PKI. While the most important trend driving the deployment of applications that make use of PKI continues to be cloud-based services (54 percent of respondents), IoT increased from 21 percent to 40 percent of respondents over the past three years (Figure 3). The regulatory environment also has increased significantly from 7 percent of respondents last year to 23 percent of respondents in this year's research.

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

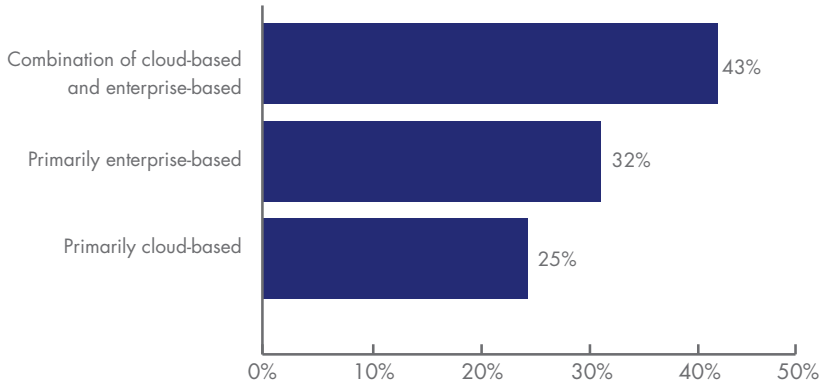
Consolidated view; two responses permitted



"IoT IS GROWING AS AN IMPORTANT TREND DRIVING THE DEPLOYMENT OF APPLICATIONS USING PKI."

In the next two years, an average of 43 percent of IoT devices in use will rely primarily on digital certificates for identification and authentication. Also, as shown in Figure 4, 43 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. How will PKI be deployed for IoT device credentialing as the IoT continues to grow?



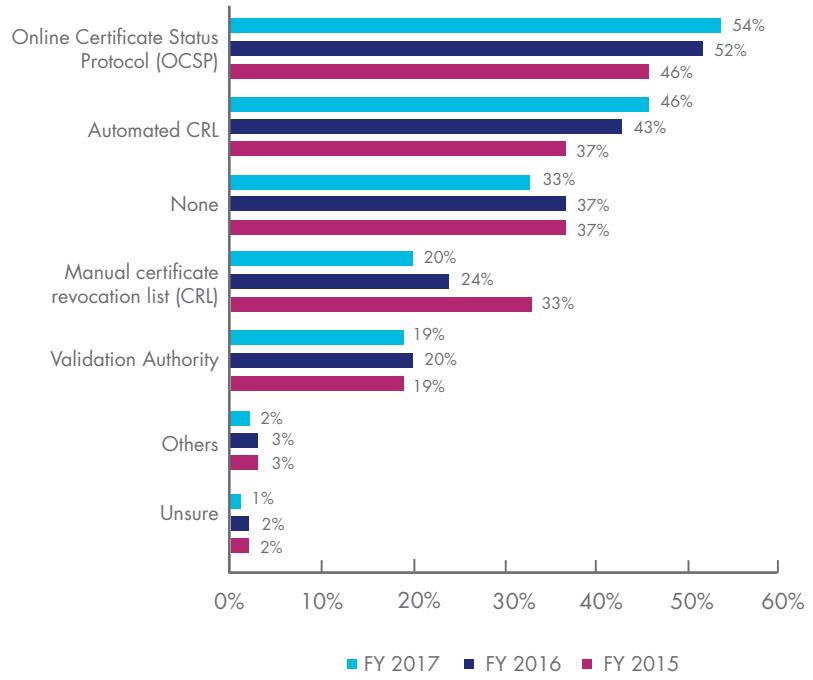
Trends in PKI maturity

The use of manual CRLs is decreasing. According to Figure 5, the certificate revocation technique most often deployed continues to be online certificate status protocol (OCSP), according to 54 percent of respondents (a slight increase from 52 percent of respondents in 2016).

Forty-six percent of respondents say their organizations use automated certificate revocation (CRL), an increase from 37 percent in 2015. Along with the increase in automated methods of revocation, the use of of manual certificate revocation continues to decrease (from 33 percent of respondents in 2015 to 20 percent of respondents in this year's research).

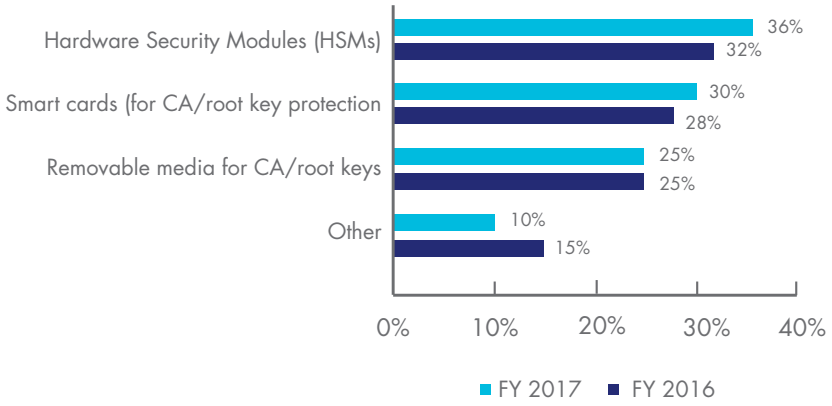
Figure 5. The certificate revocation techniques used in enterprises

Consolidated view; more than one response permitted



Hardware security modules (HSMs) are increasingly used to manage the private keys for root/policy/issuing CAs, as shown in Figure 6. Thirty percent of respondents say smart cards are used. Forty-three percent of respondents say they have PKI specialists on staff to manage private keys.

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



Of the 36 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

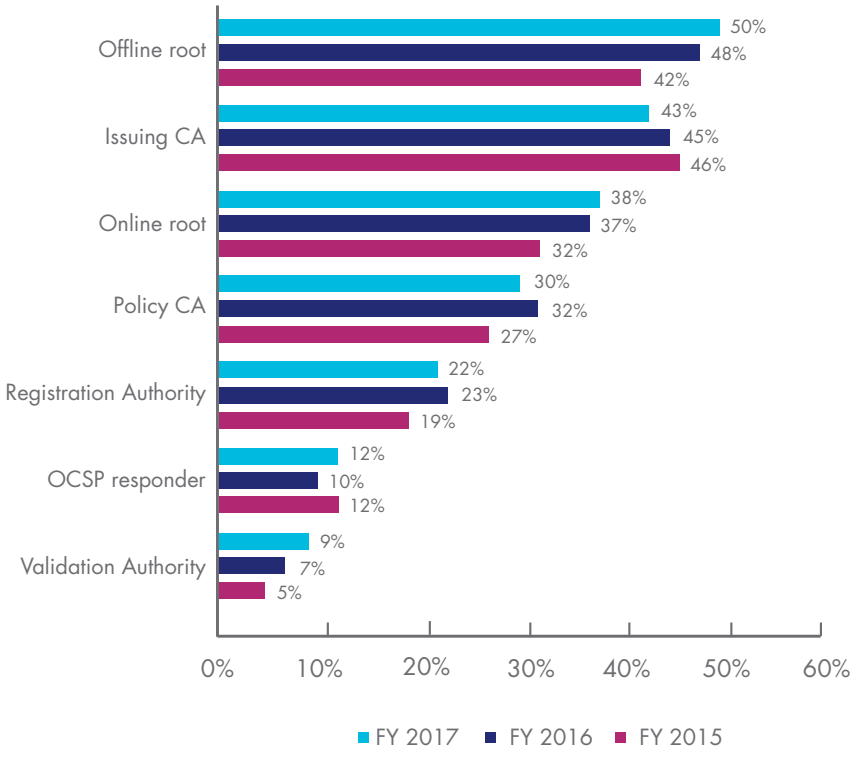
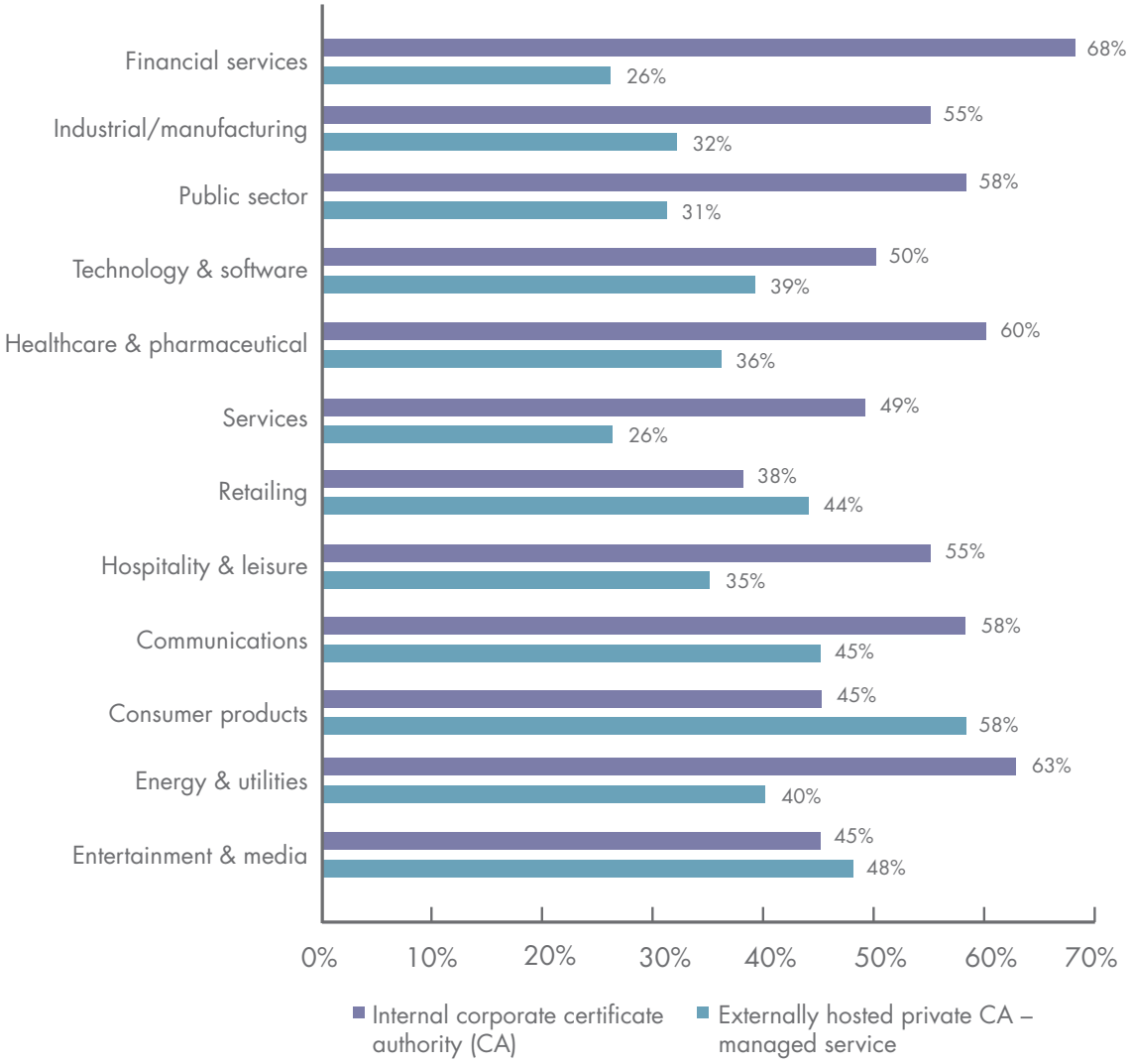


Figure 8 shows the percentage of respondents who say their organizations deploy an internal certificate authority or an externally hosted private certificate authority by 12 industry sectors.

As can be clearly seen, there are differences across industry sectors. Financial service, health and pharmaceutical and energy/utilities are most likely to deploy an internal corporate certificate authority. In contrast, consumer products, entertainment and media, communication and retail companies are most likely to deploy an externally hosted private CA.

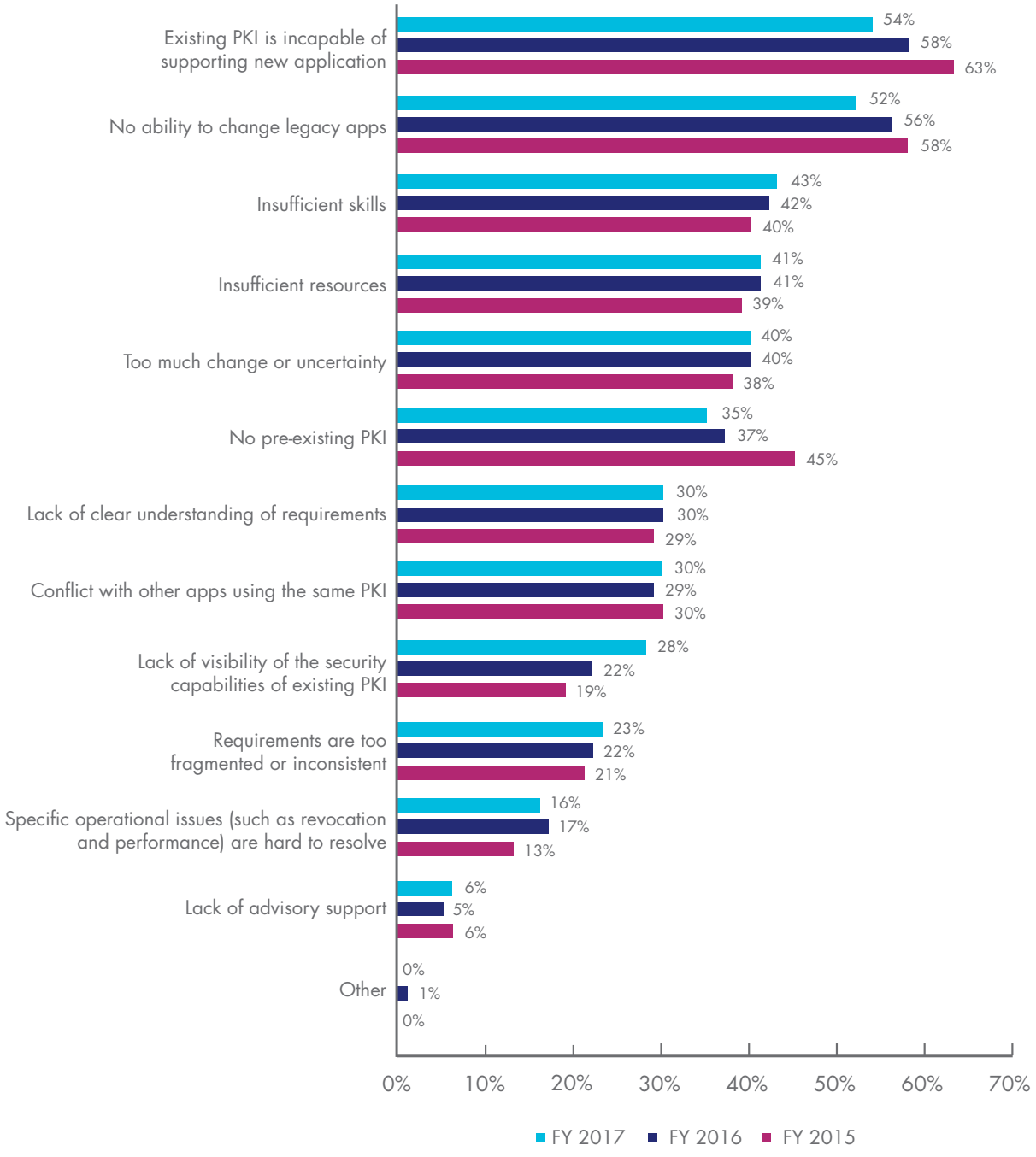
Figure 8. Percentage of companies that deploy internal or external certification authorities by industry sector



The challenge of dealing with a lack of visibility of the security capabilities of existing PKI grows. As shown in Figure 9, the lack of visibility of the security capabilities of existing PKI has increased from 19 percent in 2015 to 28 percent of respondents in this year's research. In contrast, it seems respondents are getting better at dealing with PKIs being incapable of supporting new applications (decrease from 63 percent), the inability to change legacy apps (decrease from 58 percent) and no pre-existing PKI (decrease from 45 percent).

Figure 9. The challenges to enable applications to use PKI

Consolidated view; four responses permitted

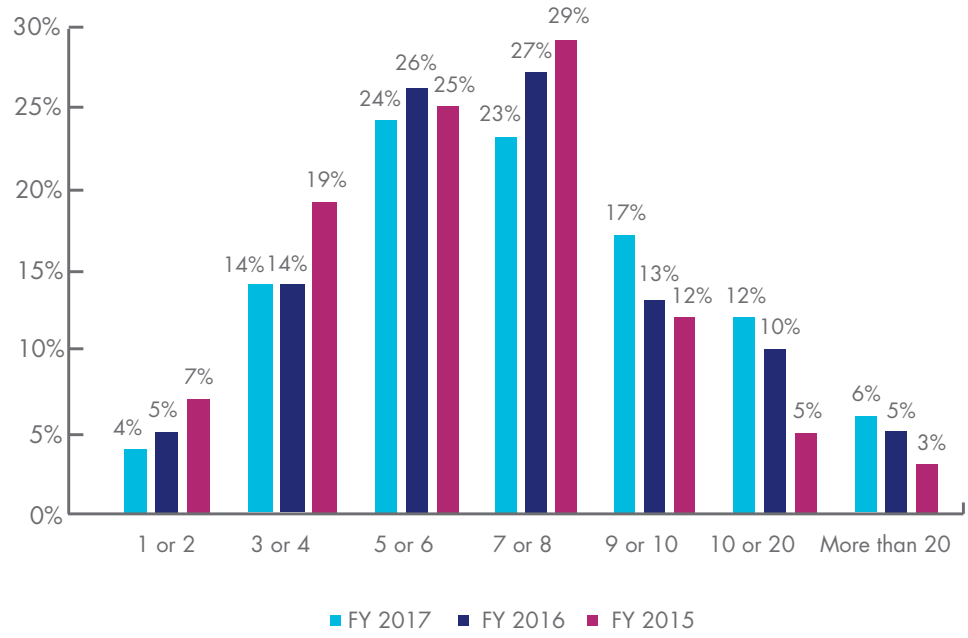


Trends in PKI challenges

Organizations with internal CAs use an average of eight separate CAs, managing an average of 35,488 internal or externally acquired certificates. As shown in Figure 10, an average of over eight 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 are the number of applications dependent upon the PKI increasing, but the nature of them indicates that the PKI is a strategic part of the core IT backbone.

Figure 10. How many distinct applications does your PKI manage certificates on behalf of?

Consolidated view; extrapolated value is 8.47 distinct applications



"NOT ONLY ARE THE NUMBER OF APPLICATIONS DEPENDENT UPON THE PKI INCREASING, BUT THE NATURE OF THEM INDICATES THAT THE PKI IS A STRATEGIC PART OF THE CORE IT BACKBONE."

The main PKI deployment challenge continues to be the lack of clear ownership of the PKI function. As shown in Figure 11, 69 percent of respondents believe there is no one function responsible for managing PKI, a slight increase from 2015. This is not in line with best practices, which assume as a baseline a sufficient degree of staffing and competency to define and maintain the process and procedures on which a modern PKI depends.

Other deployment problems include: insufficient skills (47 percent of respondents), insufficient resources (42 percent of respondents), too much change or uncertainty (41 percent of respondents) and necessary performance and reliability is hard to achieve (39 percent of respondents).

Figure 11. The main challenges deploying and managing PKI

Consolidated view; four responses permitted

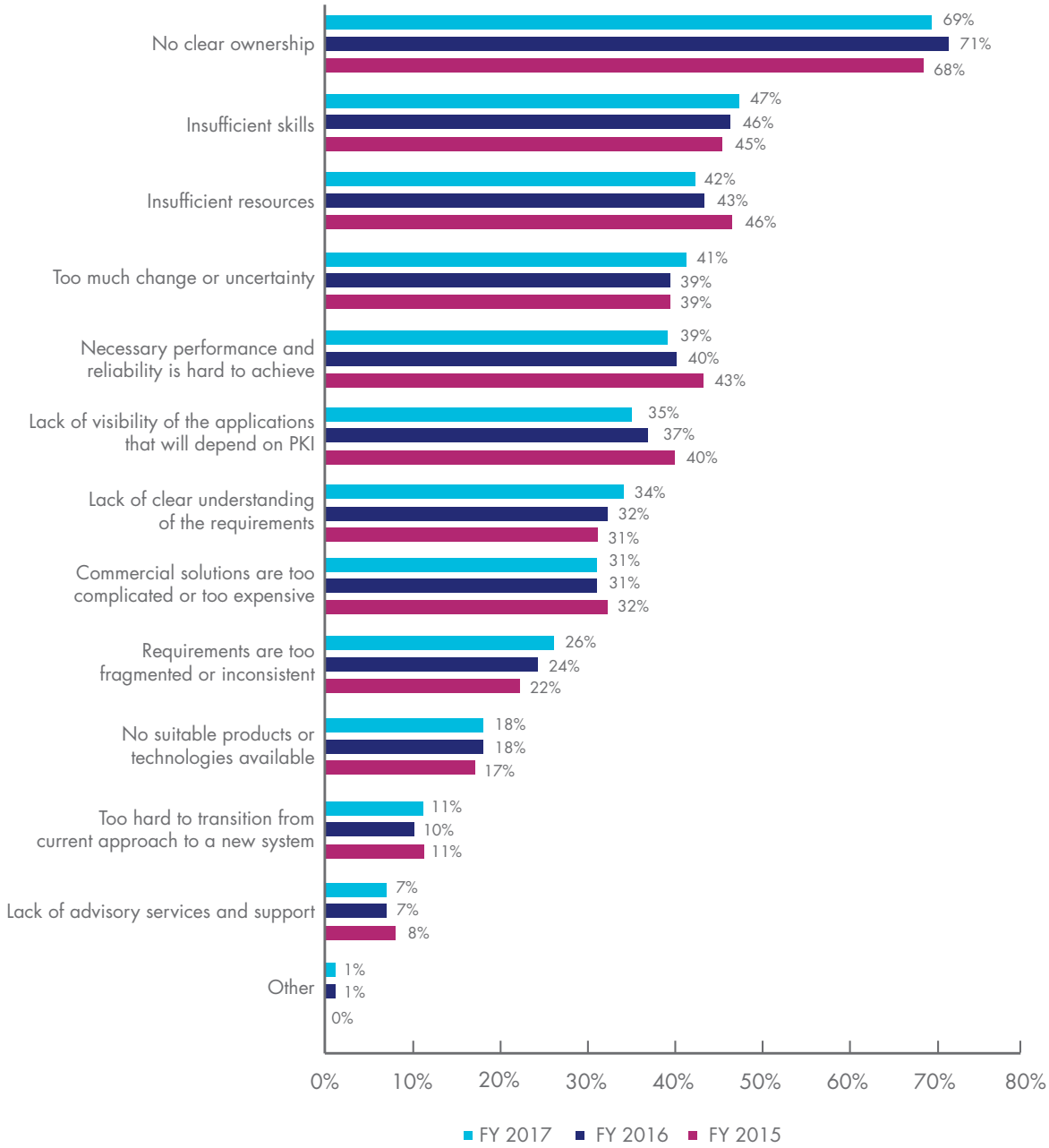
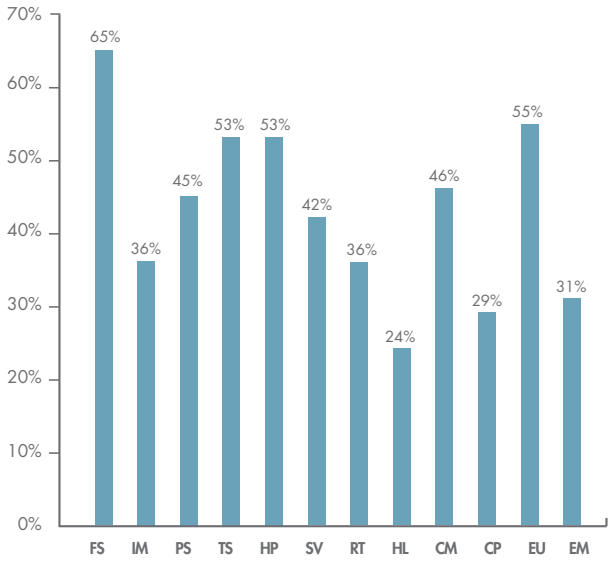


Figure 12 shows the percentage of respondents who say their organizations have PKI specialists on staff. As can be seen, there are significant differences across industry sectors. Specifically, companies in financial services, energy/utilities and health and pharmaceutical are most likely to employ PKI specialists as a fully dedicated role. In contrast, hospitality, consumer products, entertainment and media, communication and retail companies are less likely to employ PKI specialists as a fully dedicated role within the company. Following are the abbreviations used in all industry breakout questions.

Industry sectors	Abbreviated
Financial services	FS
Industrial/manufacturing	IM
Public sector	PS
Technology & software	TS
Healthcare & pharmaceutical	HP
Services	SV
Retailing	RT
Hospitality & leisure	HL
Communications	CM
Consumer products	CP
Energy & utilities	EU
Entertainment & media	EM

Figure 12. Percentage of companies that have a PKI specialist on staff

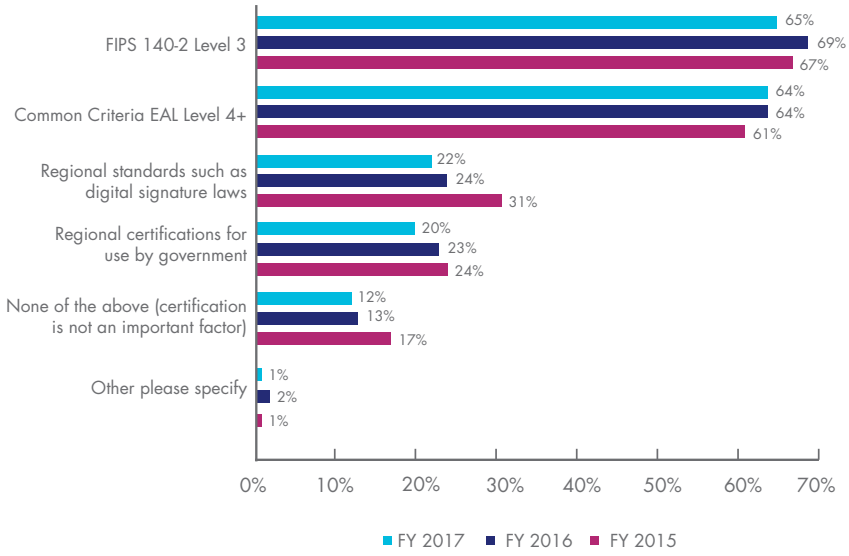
Response = Yes; mean = 43%



FIPS 140 and common criteria are the most important security certification when deploying PKI infrastructure and PKI-based applications. According to Figure 13, 65 percent say FIPS 140 is most important and this is closely followed by Common Criteria (64 percent of respondents) when deploying PKI. Twenty-two percent say it is regional standards such as digital signature laws (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 13. Security certifications important when deploying PKI infrastructure

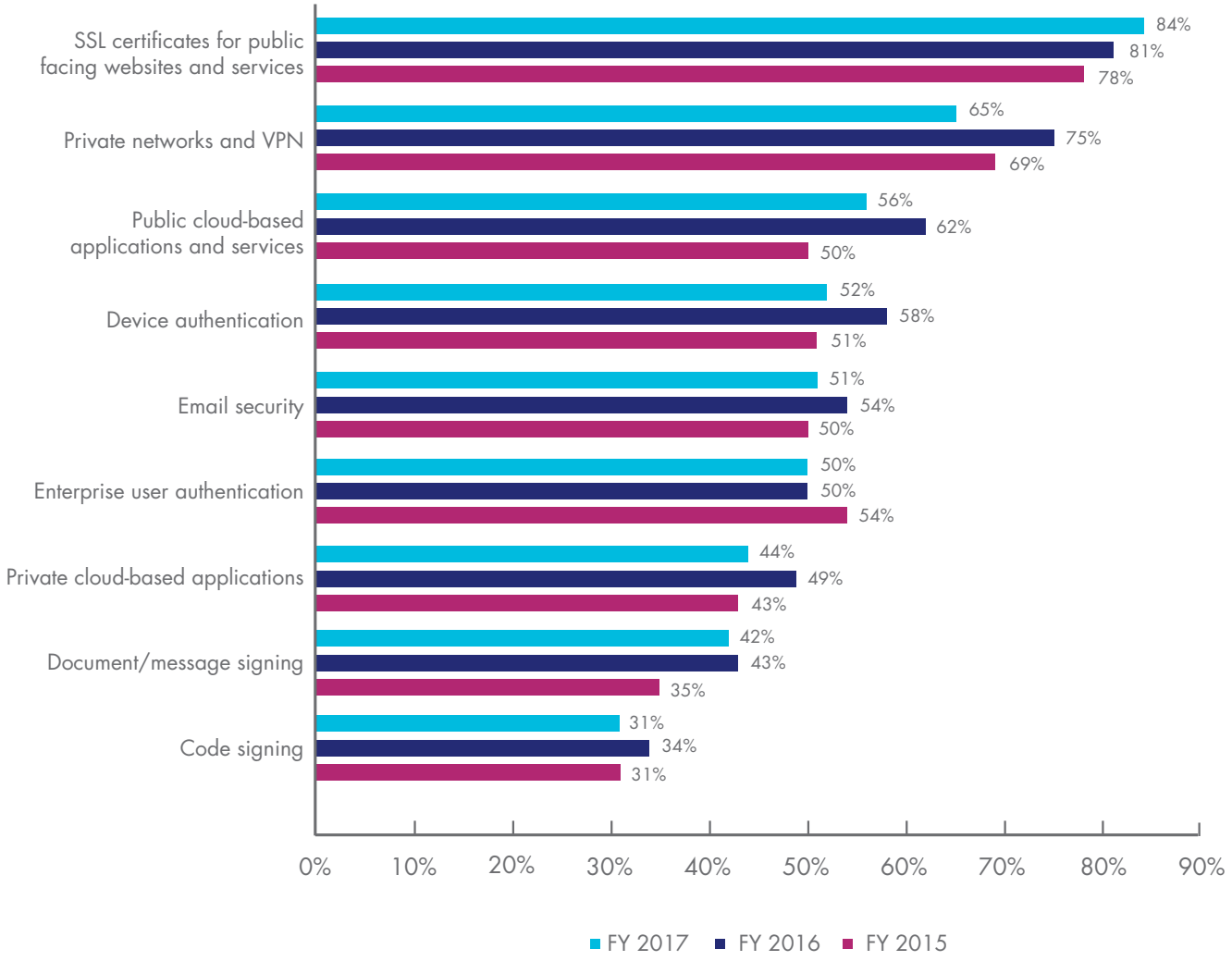
Consolidated view, more than one response permitted



SSL certificates for public facing websites and services increase the use of PKI credentials significantly. According to Figure 14, applications most often using PKI credentials are: SSL certificates for public facing websites and services (84 percent of respondents). Most PKI use by applications has remained relative stable over the three years of the study, however private networks and VPN showed a marked 10 percent decrease from 2016 to 2017. Document/messaging signing applications have increased significantly from 35 percent in 2015 to 42 percent in 2017.

Figure 14. What applications use PKI credentials?

Consolidated view; more than one response permitted

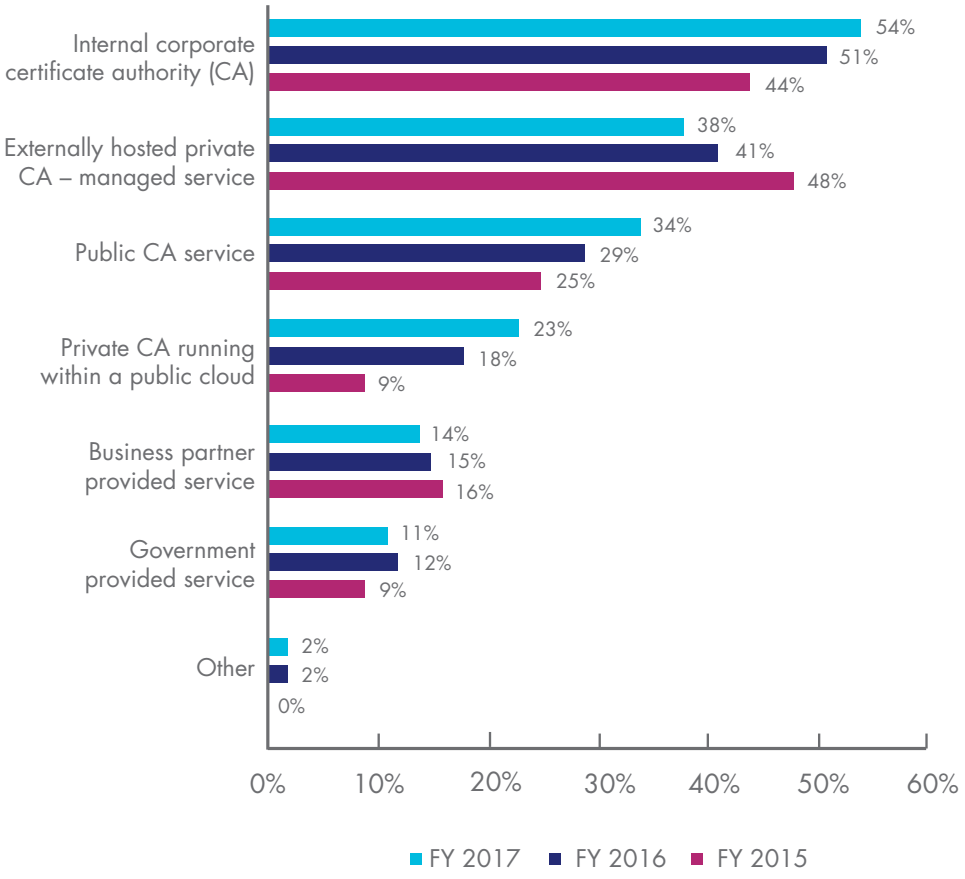


What are the most popular methods for deploying enterprise PKI? Fifty-four percent of respondents say their organizations favor an internal corporate certificate authority (CA), according to Figure 15.

Externally hosted private CA—managed service has decreased from 48 percent of respondents in 2015 to 38 percent of respondents in this year's study. Companies using a private CA running within a public cloud has increased significantly from 9 percent of respondents in 2015 to 23 percent of respondents in 2017.

Figure 15. How is PKI deployed?

Consolidated view; more than one response permitted



"FIFTY-FOUR PERCENT OF RESPONDENTS SAY THEIR ORGANIZATIONS FAVOR AN INTERNAL CORPORATE CERTIFICATE AUTHORITY (CA)."

Global analysis

Figure 16 shows how PKI is deployed within respondents' organizations. As can be seen, 7 of the 11 countries in the survey are more likely to choose internal corporate certificate authority. In contrast, Brazilian, Mexican, Arabian and Russian Federation respondents are more likely to choose external hosted private certificate authorities as a managed service.

Figure 16. How would you describe how your organization's enterprise PKI is deployed?

Top 2 choices

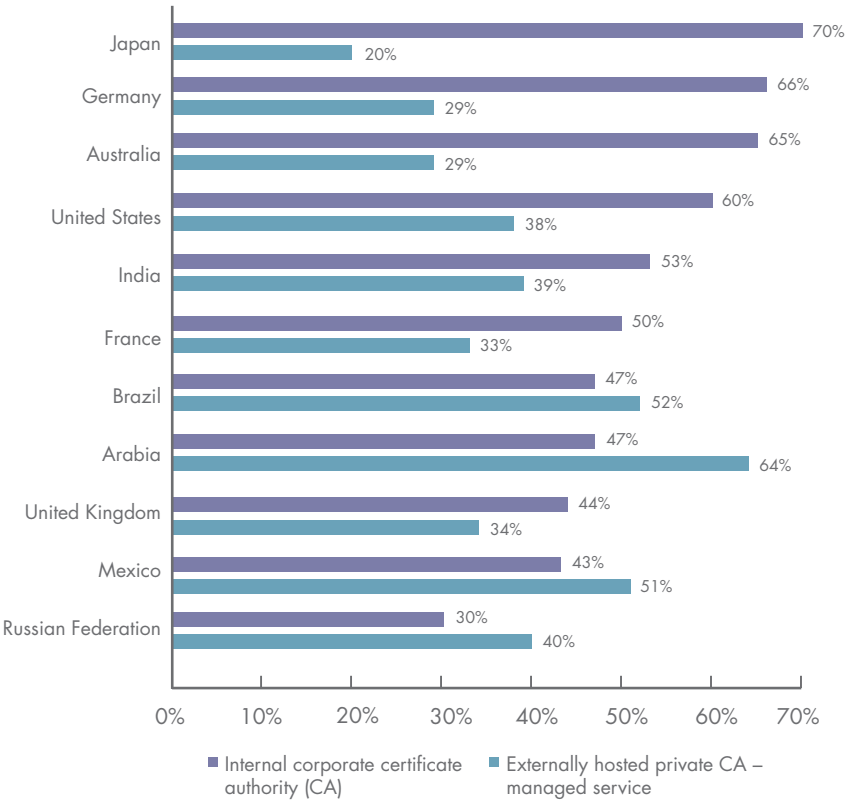


Figure 17 shows the percentage of respondents who say their organization does not deploy a certification revocation technique or process. As can be seen, there are marked differences across industry sectors. Specifically, industrial/manufacturing, public sector and financial service companies are most likely to report their organizations deploy a certification revocation technique. In contrast, services, retail and healthcare/pharma companies are most likely to report their organizations do not deploy a certification revocation technique.

Figure 17. Percentage of companies by industry that do not deploy a certificate revocation technique

Response = none; mean value = 33%

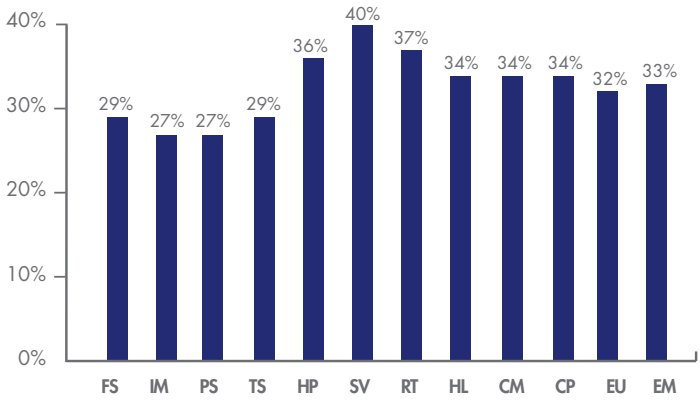
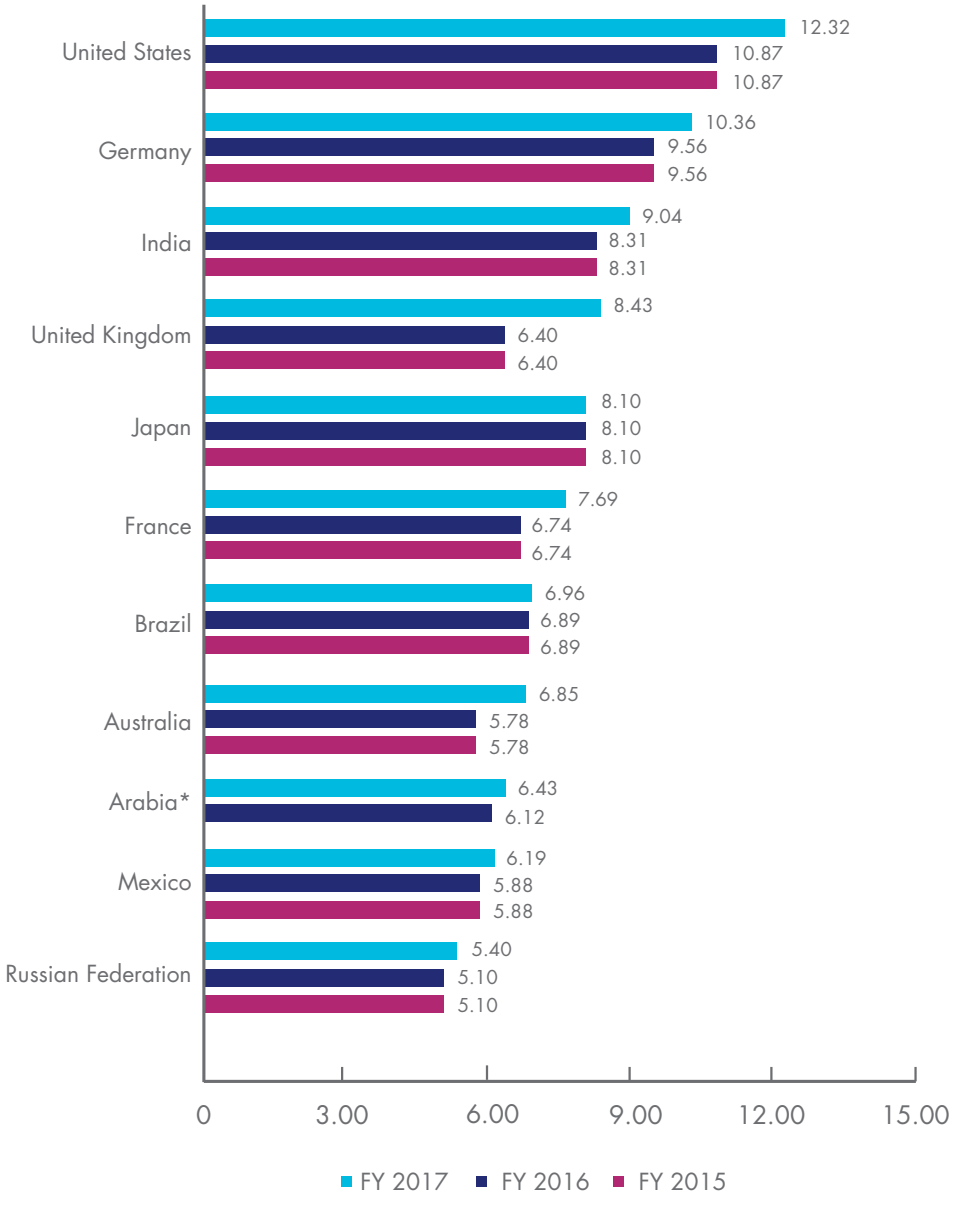


Figure 18 shows the number of distinct applications (e.g., email, network authentication, etc.) for which PKI manages certificates. The US at 12.32 distinct applications has the largest number of distinct applications. Mexico (6.19) and Russia Federation (5.40) have the smallest number of distinct applications, respectively.

One should note that even in the lowest figures that the average number of applications is just north of 5. 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. How many distinct applications does your PKI manage certificates on behalf of?

Extrapolated value



*Arabia was not surveyed in FY 2015

Figure 19 reports the three most salient challenges in deploying and managing PKI. As can be seen, Arabia, Germany, Australia, Japan and Mexico respondents are most likely to say no clear ownership as their most significant challenge. Russian Federation respondents are most likely to say insufficient resources. Arabia and Mexican respondents are most likely to say 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 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 19. What are the main challenges in deploying and managing PKI?

Top 3 choices

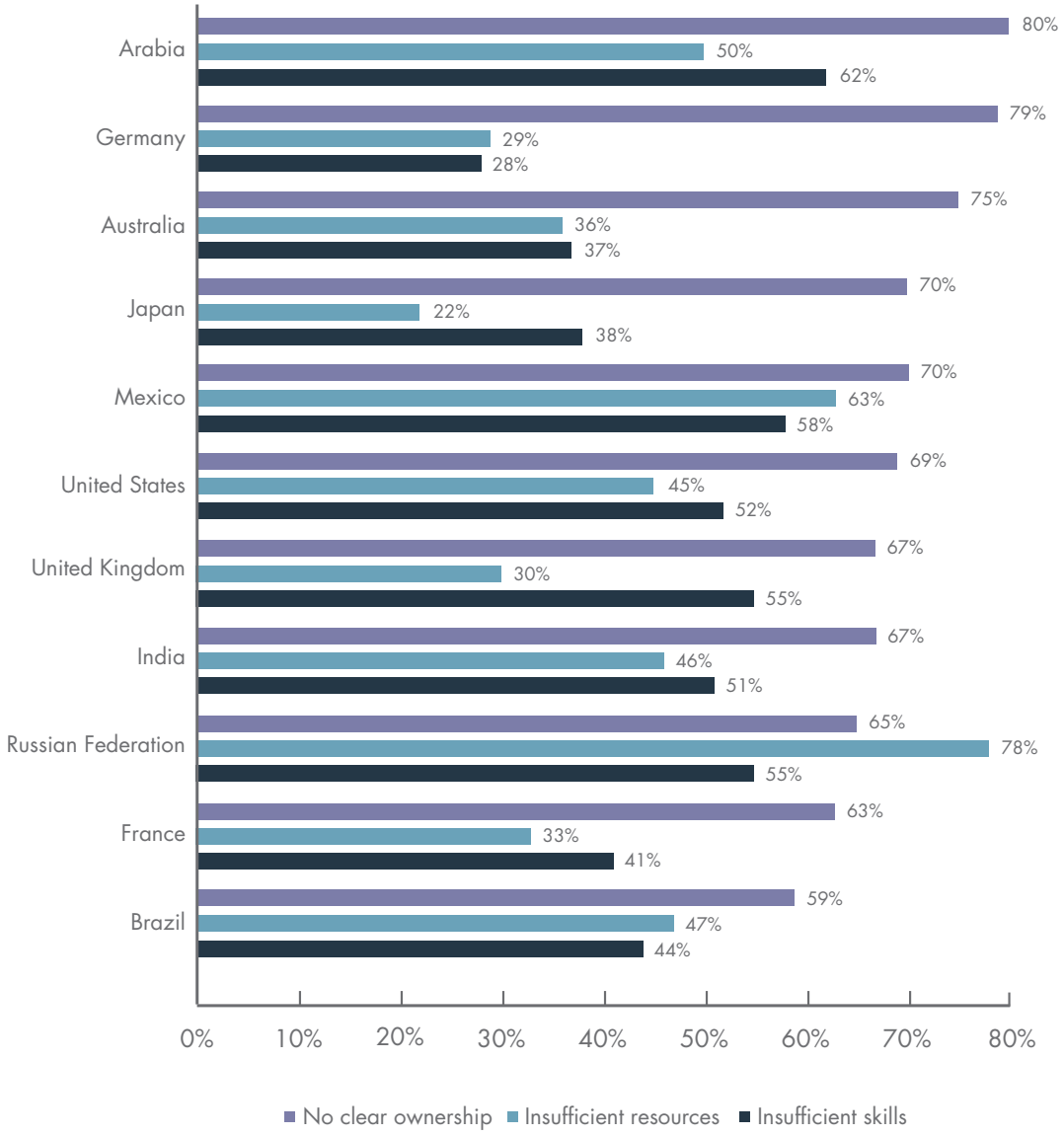
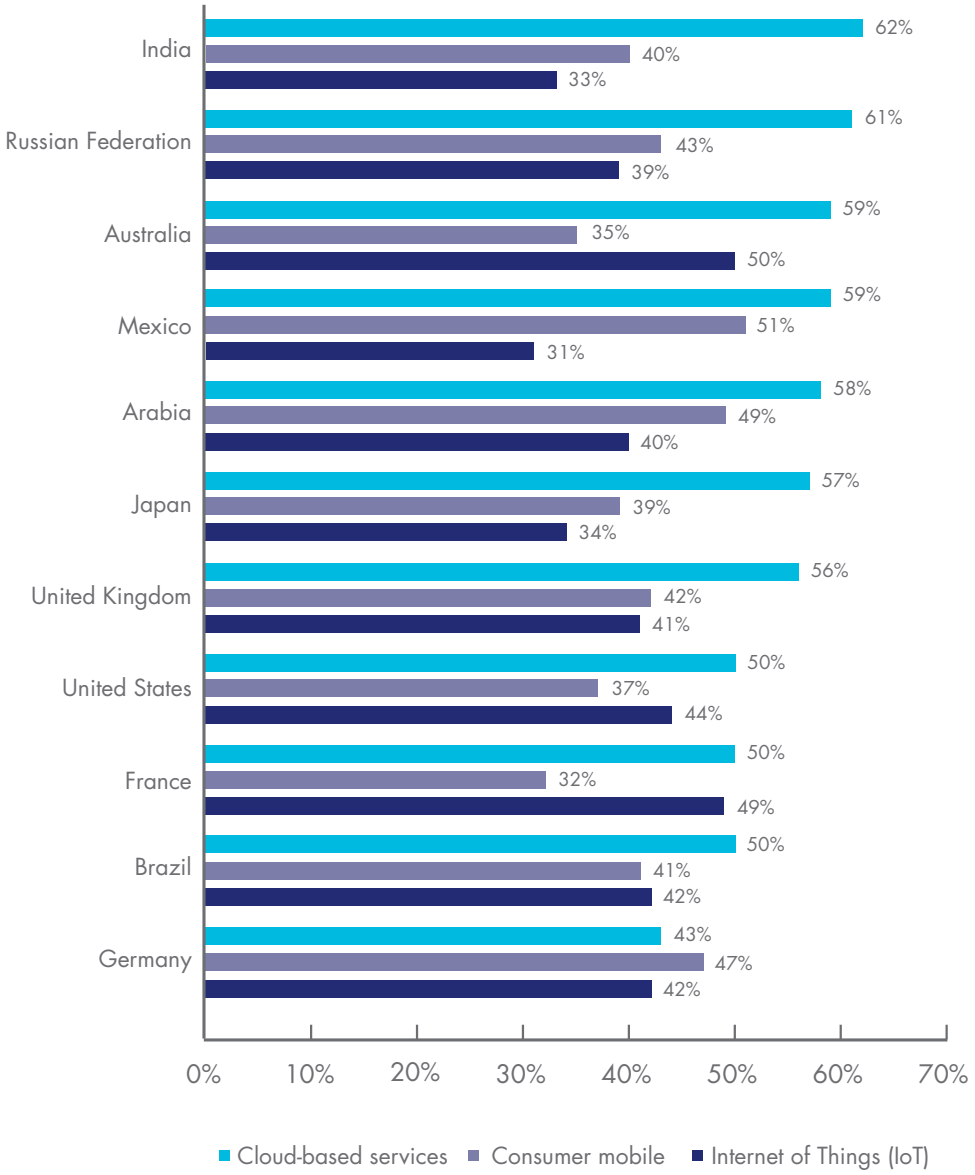


Figure 20 reports what respondents believe are the most important trends that are driving the deployment of applications that make use of PKI. As can be seen, the majority of all respondents, with the exception of German respondents, found that cloud-based services are the most important trend driving application use of PKI technologies. Mexico and Arabia respondents are most likely to see consumer-oriented mobile applications as a driver to PKI adoption. The IoT is beginning to have a significant impact, particularly in the Australia and France.

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

Top 3 choices



PART 3. METHODS

Table 1 reports the consolidated sample response for 11 separate country samples. The sample response for this study conducted over a 49-day period ending in February 2017.

Our consolidated sampling frame of practitioners in all countries consisted of 138,530 individuals who have bona fide credentials in IT or security fields. From this sampling frame, we captured 5,397 returns of which 595 were rejected for reliability issues. From our final consolidated 2017 sample of 4,802, we calculated the PKI subsample to be 1,510.

Table 1. Sample response	Frequency
Sampling FY 2017ame	138,530
Total returns	5,397
Rejected or screened surveys	595
Overall sample (encryption trends)	4,802
PKI subsample	1,510
Ratio subsample to overall sample	31.4%

Figure 21 summarizes the approximate position levels of respondents in our study. As can be seen, more than half of respondents (54 percent) are at or above the supervisory level.

As shown in Figure 22, 59 percent of respondents identified IT operations as their functional area within the organization and 18 percent of respondents are functioning within security.

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

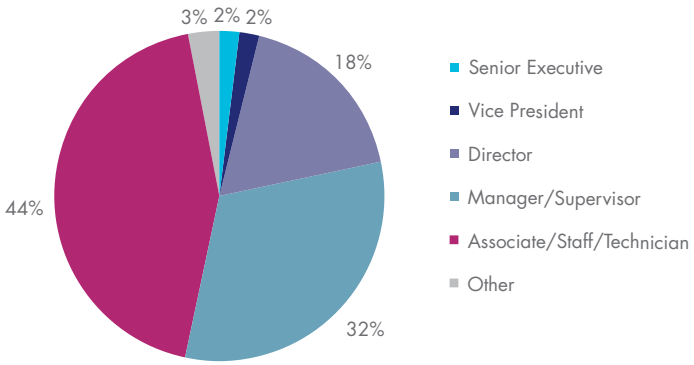


Figure 22. Distribution of respondents according to functional area
Country samples are consolidated

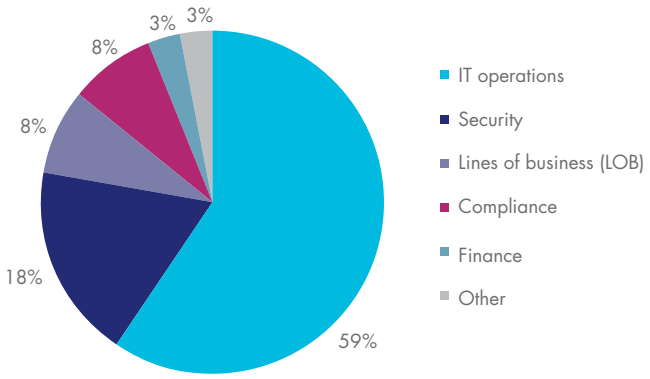


Figure 23 reports the respondents' organizations primary industry segments. As shown, 16 percent of respondents are located in the financial services industry, which includes banking, investment management, insurance, brokerage, payments and credit cards. Eleven percent are located in manufacturing and industrial companies. Another 11 percent are located in service companies.

According to Figure 24, the majority of respondents (65 percent) 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

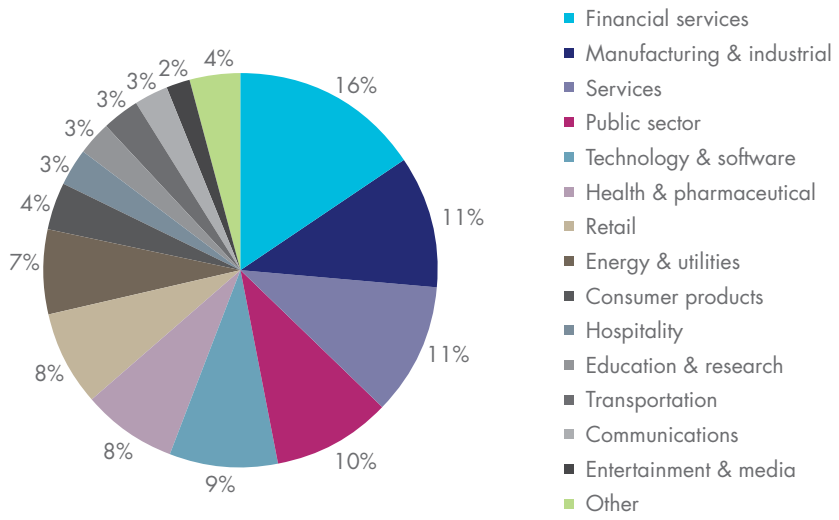
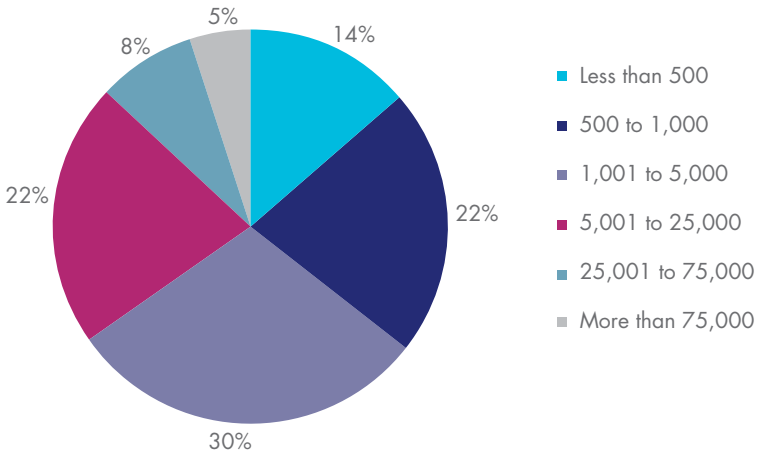


Figure 24. Distribution of respondents according to organizational headcount

Country samples are consolidated



PART 4. 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 11 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.

APPENDIX: DETAILED SURVEY RESULTS

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured over a 49-day period ending February 2017.

2017 Consolidated Survey Response	Total
Sampling frame (11 countries)	138,530
Total returns	5,397
Rejected surveys	595
Overall sample (encryption trends)	4,802
PKI subsample	1,510
Ratio subsample to overall sample	31.4%
PKI subsample weights	100%

Public Key Infrastructure (PKI)

Q1. What best describes your role or involvement in your organization's enterprise PKI?	**FY 2017**
I am involved in the management my organization's PKI	58%
I am involved in developing and/or managing applications that depend upon credentials controlled by my organization's PKI	42%
I am not involved in my organization's PKI or the applications that depend on them (Stop)	0%
My organization does not have an PKI (Stop)	0%
Total	100%

Q2. How would you describe how your organization's enterprise PKI is deployed? Please select all that apply.	**FY 2017**
Internal corporate certificate authority (CA)	54%
Externally hosted private CA – managed service	38%
Public CA service	34%
Private CA running within a public cloud	23%
Business partner provided service	14%
Government provided service	11%
Other (please specify)	2%
None of the above (stop)	0%
Total	176%

Q3. Which certificate revocation technique does your organization deploy? Please select all that apply.	**FY 2017**
Online Certificate Status Protocol (OCSP)	54%
Manual certificate revocation list (CRL)	20%
Automated CRL	46%
Validation Authority	19%
Others (please specify)	2%
None	33%
Unsure	1%
Total	175%

Q4. How many issuing CAs does your PKI support? Those respondents that use an external CA service were removed.	FY 2017
1 or 2	16%
3 or 4	18%
5 or 6	18%
7 or 8	14%
9 or 10	14%
More than 10	22%
Total	100%
Extrapolated value	7.39

Q5. How many certificates does your PKI issue (or have been acquired from an external service)?	FY 2017
Less than 10	2%
10 to100	3%
101 to 1,000	15%
1,001 to 5,000	18%
5,001 to 10,000	18%
10,001 to 50,000	15%
50,001 to 100,000	15%
More than 100,000	15%
Total	100%
Extrapolated value	35,488

Q6. How many distinct applications (e.g., email, network authentication, etc.) does your PKI manage certificates on behalf of?	**FY 2017**
1 or 2	4%
3 or 4	14%
5 or 6	24%
7 or 8	23%
9 or 10	17%
10 or 20	12%
More than 20	6%
Total	100%
Extrapolated value	8.47

Q7. What security controls and best practices do you use to secure the PKI and CA in particular? Please select all that apply.	**FY 2017**
Physical secure location	47%
Isolated networks	21%
Strict record keeping (e.g., video recording, independent observers, etc.)	13%
Formal security practices (documented)	40%
Offline root CAs	28%
Quorums and dual controls	13%
Multifactor authentication for administrators	59%
Passwords alone without a second factor	29%
No special security measures	6%
Other (please specify)	2%
Total	258%

Q8a. Do you have PKI specialists on staff?	FY 2017
Yes	43%
No	27%
Rely on consultants	15%
Rely on service provider	14%
Total	100%

Q8b. How do you manage the private keys for your root/policy/issuing CAs?	FY 2017
Hardware security modules (HSMs)	36%
Smart cards (for CA/root key protection)	30%
Removable media for CA/root keys	25%
Other	10%
Total	100%

Q9. If you use HSMs to secure PKI, where are they deployed? Please select all that apply.	FY 2017
Offline root	50%
Online root	38%
Issuing CA	43%
Policy CA	30%
Registration Authority	22%
OCSP responder	12%
Validation Authority	9%
Total	203%

Q10. What are the main challenges in deploying and managing PKI? Please select 4 top choices.	**FY 2017**
No clear ownership	69%
Insufficient resources	42%
Insufficient skills	47%
Lack of clear understanding of the requirements	34%
Too much change or uncertainty	41%
Requirements are too fragmented or inconsistent	26%
No suitable products or technologies available	18%
Necessary performance and reliability is hard to achieve	39%
Commercial solutions are too complicated or too expensive	31%
Lack of visibility of the applications that will depend on PKI	35%
Lack of advisory services and support	7%
Too hard to transition from current approach to a new system	11%
Other (please specify)	1%
Total	400%

Q11. As you plan the evolution of your PKI, where are the greatest areas of possible change and uncertainty? Please select 2 top choices.	**FY 2017**
PKI technologies	26%
Vendors (products and services)	14%
Enterprise applications	19%
Internal security policies	20%
External mandates and standards	47%
Budget and resources	17%
Management expectations	21%
New applications (e.g., Internet of Things)	36%
Other (please specify)	1%
Total	200%

Q12. In your opinion, which security certifications are important when deploying PKI infrastructure?	FY 2017
Common Criteria EAL Level 4+	64%
FIPS 140-2 Level 3	65%
Regional certifications for use by government	20%
Regional standards such as digital signature laws	22%
Other please specify	1%
None of the above (certification is not an important factor)	12%
Total	184%

Q13. What applications use PKI credentials in your organization?	FY 2017
SSL certificates for public facing websites and services	84%
Private networks and VPN	65%
Email security	51%
Enterprise user authentication	50%
Device authentication	52%
Document/message signing	42%
Code signing	31%
Public cloud-based applications and services	56%
Private cloud-based applications	44%
Other (please specify)	1%
None of the above	4%
Total	479%

Q14. In your opinion, what are the most important trends that are driving the deployment of applications that make use of PKI? Please select 2 top choices.	**FY 2017**
Consumer mobile	41%
Cloud-based services	54%
BYOD and internal mobile device management	8%
Internet of Things (IoT)	40%
Regulatory environment	23%
Consumer-oriented mobile applications	19%
E-commerce	5%
Risk management	2%
Cost savings	6%
Other (please specify)	1%
Total	200%

Q15. What are the challenges to enable applications to utilize PKI? Please select 4 top choices.	**FY 2017**
No pre-existing PKI	35%
Existing PKI is incapable of supporting new applications	54%
Insufficient resources	41%
Insufficient skills	43%
Lack of clear understanding of requirements	30%
Too much change or uncertainty	40%
Requirements are too fragmented or inconsistent	23%
No ability to change legacy apps	52%
Lack of visibility of the security capabilities of existing PKI	28%
Conflict with other apps using the same PKI	30%
Specific operational issues (such as revocation and performance) are hard to resolve	16%
Lack of advisory support	6%
Other (please specify)	0%
Total	400%

Q16. Do you believe that the Internet of Things continues to grow, that supporting PKI deployments for IoT device credentialing will be:	FY 2017
Primarily cloud-based	25%
Primarily enterprise-based	32%
Combination of cloud-based and enterprise-based	43%
Total	100%

Q17. What percentage of IoT devices that will likely be used by your organization in the next two years do you believe will rely primarily on digital certificates for identification/authentication?	FY 2017
Less than 10%	11%
10% to 25%	19%
26% to 50%	36%
51% to 75%	22%
76% to 100%	13%
Total	100%
Extrapolated value	43%

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 Thales eSecurity

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premise, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and, with the internet of things (IoT), even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property, and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged-user control and high-assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

About Thales

Thales is a global technology leader for the Aerospace, Transport, Defence and Security markets. With 64,000 employees in 56 countries, Thales reported sales of €14.9 billion in 2016. With over 25,000 engineers and researchers, Thales has a unique capability to design and deploy equipment, systems and services to meet the most complex security requirements. Its exceptional international footprint allows it to work closely with its customer all over the world.

THALES

www.thalesesecurity.com