ENTRUST

True confidence in your security comes from awareness.

2022 GLOBAL PKI AND IoT TRENDS STUDY

Find out how organizations are using PKI and if they're prepared for what's possible.

Executive Summary

Ponemon INSTITUTE

Things become smart when they connect —
to the internet, other devices, platforms, and people. But all those connections need to be secured, and organizations need to prioritize that security.

With new use cases like IoT and cloud leading the deployment of PKI, and the continued rise of machine identities, there is no longer a security perimeter, and the IT landscape has become more complex.

Looking at this year’s **2022 Global PKI and IoT Trends Study**, we see that without the right resources to secure those connections, many organizations are struggling to achieve PKI maturity so they can take advantage.

Ponemon Institute is pleased to present the findings of the *2022 Global PKI and IoT Trends Study*, sponsored by Entrust.

According to the findings, while PKI is considered a strategic part of the core IT backbone, the challenges in achieving PKI maturity continue to be insufficient resources and the shortage of skilled IT and IT security practitioners. Another growing challenge is the lack of visibility of the applications that will depend upon PKI.

The PKI research is part of a larger study published earlier this year involving 6,264 respondents in 17 countries.[1]

In this report, Ponemon Institute presents the findings based on a survey of 2,505 IT and IT security professionals who are involved in their organizations' enterprise PKI in 17 countries including Australia, Brazil, France, Germany, Hong Kong, Japan, Korea, Mexico, Middle East, Netherlands, Southeast Asia, Spain, Sweden, the United Kingdom, and the United States.

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. The IT manager, IT security manager, and CIO are most responsible for their organizations' PKI strategy.

[1] See: **2022 Global Encryption Trends & Key Management Study** (sponsored by Entrust), Ponemon Institute, April 2022.

Summary of Key Findings and Takeaways

As organizations plan the evolution of their PKI, new applications such as IoT devices and external mandates and standards continue to drive the most change and uncertainty. Thirty-three percent of respondents say new applications such as the IoT (a decrease from 41 percent in 2021) and 30 percent of respondents say external mandates and standards (a decrease from 37 percent in 2021) will drive change. Enterprise applications as a change agent have increased from 17 percent of respondents to 23 percent of respondents).

Cloud-based services and IoT continue to be the most important trends driving the deployment of applications using PKI. There is growing recognition that PKI provides important core authentication technology in the IoT. Cloud-based services is the number one trend driving deployment of applications using PKI (49 percent of respondents). Respondents who say IoT is the most important trend driving the deployment of applications using PKI has remained virtually unchanged (47 percent of respondents) since 2020.

Scalability to millions of managed certificates continues to be the most important PKI capability for IoT employments. While scalability is the most important capability, it has decreased in importance from 53 percent of respondents in 2018 to 39 percent of respondents in 2020. The ability to sign firmware for IoT devices has increased from 27 percent of respondents in 2021 to 33 percent of respondents in 2022.

Hardware security modules (HSMs) continue to be most often used to manage the private keys for their root/policy/issuing CAs (37 percent of respondents). Twenty-six percent of respondents say removable media for CA/root keys and 24 percent of respondents say smart cards are used. Thirty-eight percent of respondents say they have PKI specialists on staff who are involved in their organizations' enterprise PKI, a decrease from 41 percent of respondents in 2021.

Of the 37 percent of organizations in this study that use HSMs to secure PKI, they are used across the entire architecture of the PKI. HSMs deployed in offline roots has declined from 49 percent of respondents in 2018 to 27 percent of respondents in 2022.

Insufficient resources, lack of skills, and no clear ownership are the top three challenges to enabling applications to use PKI. The challenge of not having sufficient resources has increased significantly from 51 percent of respondents in 2021 to 64 percent of respondents in 2022. Other challenges are insufficient skills (52 percent) and no clear ownership (52 percent of respondents). The lack of visibility of the applications that will depend upon PKI increased from 34 percent of respondents in 2021 to 48 percent of respondents in this year's research.

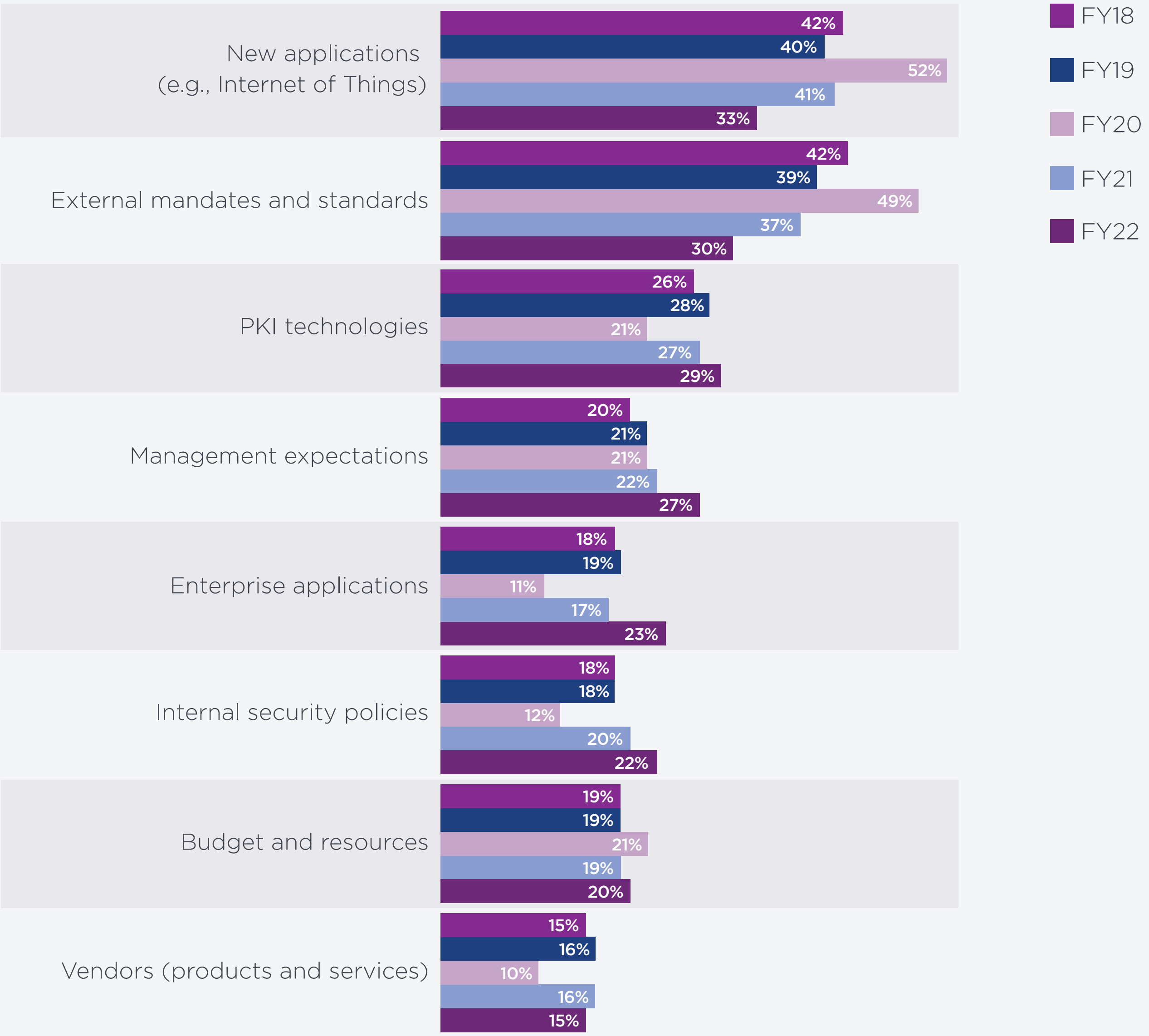
Organizations with internal CAs use an average of 6.8 separate CAs, managing an average of 52,022 internal or externally acquired certificates. An average of 8.4 distinct applications, such as email and network authentication, are managed by an organization's PKI. This indicates that the PKI is at the core of the enterprise IT backbone. Not only the number of applications dependent upon the PKI but the nature of them indicates that PKI is a strategic part of the core IT backbone.

DETAILED FINDINGS

Trends in managing IoT

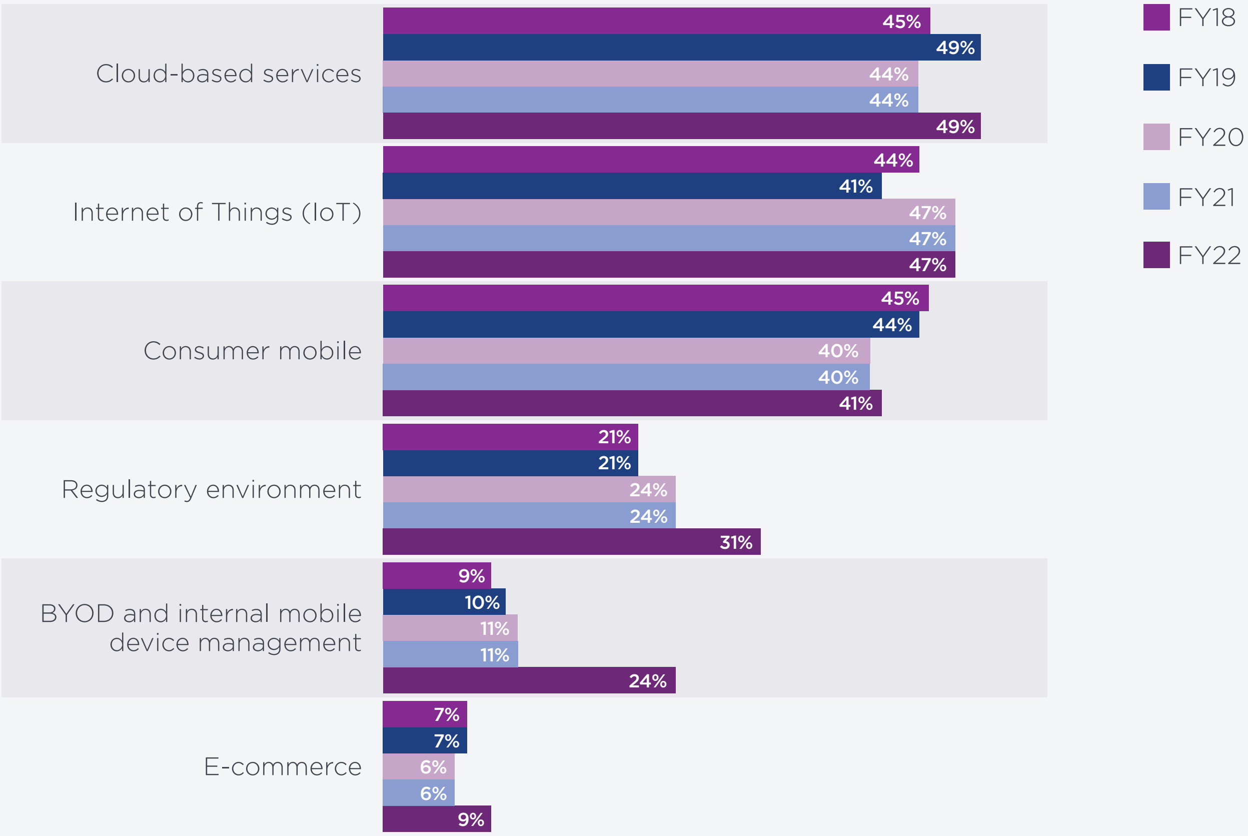
As organizations plan the evolution of their PKI, new applications such as IoT devices and external mandates and standards continue to drive the most change and uncertainty. According to Figure 1, 33 percent of respondents say new applications such as the IoT (a decrease from 41 percent in 2021) and 30 percent of respondents say external mandates and standards (a decrease from 37 percent in 2021) will drive change. Enterprise applications as a change agent for PKI have increased from 17 percent of respondents to 23 percent of respondents.

Figure 1. **As organizations plan the evolution of their PKI, what areas are expected to experience the most change and uncertainty?** (Consolidated view — two responses permitted)



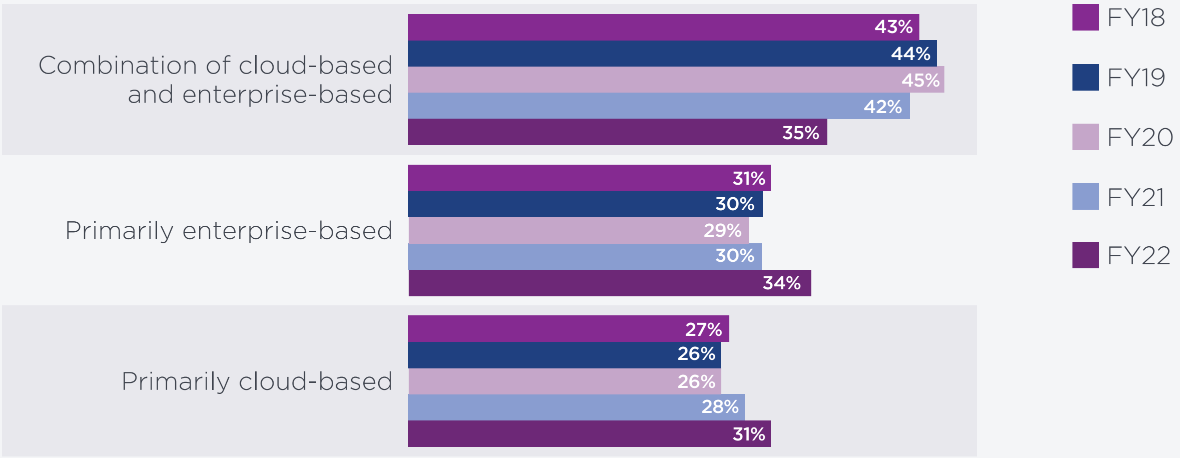
Cloud-based services and IoT continue to be the most important trends driving the deployment of applications using PKI. There is growing recognition that PKI provides important core authentication technology in the IoT. As shown in Figure 2, cloud-based services is the number one trend driving deployment of applications using PKI (49 percent of respondents). Respondents who say IoT is the most important trend driving the deployment of applications using PKI has remained virtually unchanged (47 percent of respondents) since 2020.

Figure 2. **The most important trends driving the deployment of applications using PKI**
(Consolidated view — two responses permitted)



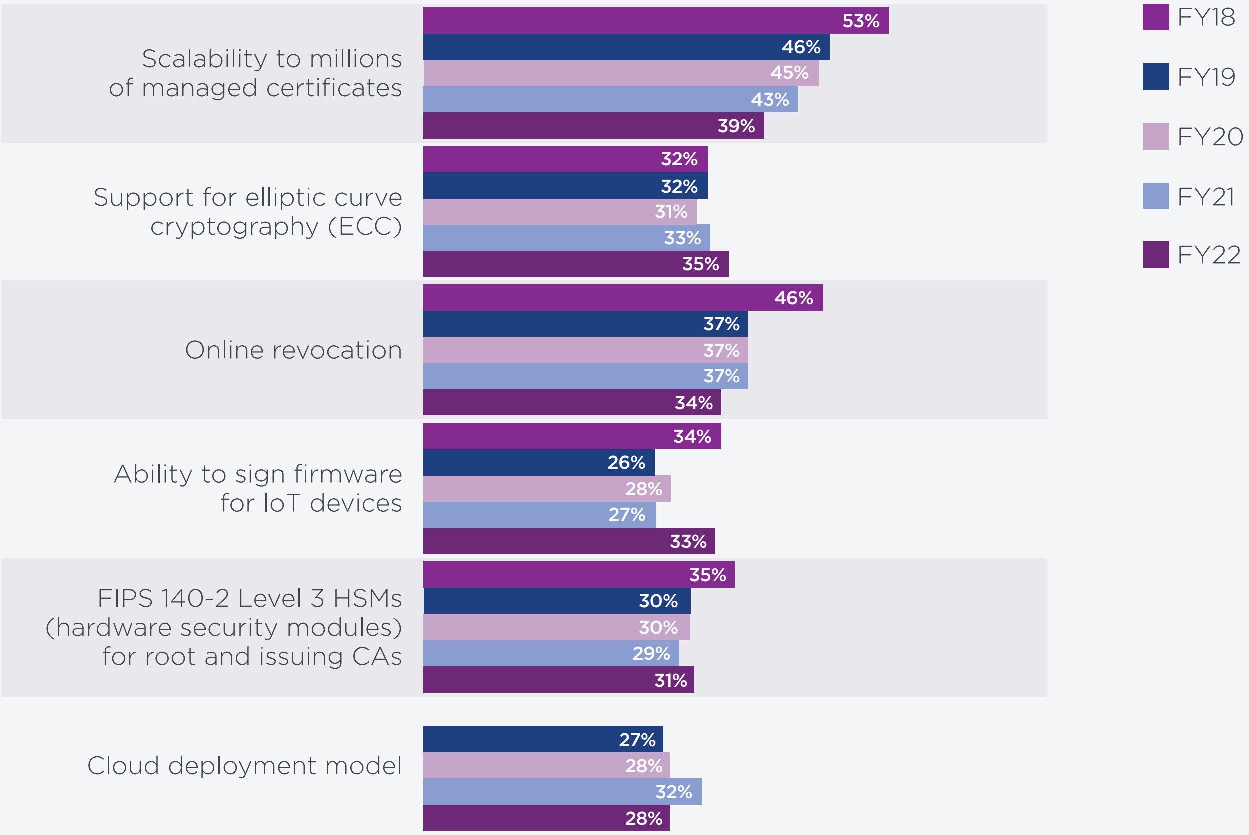
In the next two years, an average of 44 percent of IoT devices in use will rely primarily on digital certificates for identification and authentication. As shown in Figure 3, 35 percent of respondents believe that as the IoT continues to grow supporting PKI deployments for IoT device credentialing will be a combination of cloud-based and enterprise-based. However, this has decreased from 42 percent of respondents in 2021.

Figure 3. **As IoT continues to grow, what PKI deployments will support IoT device credentialing?**



Scalability to millions of managed certificates continues to be the most important PKI capability for IoT employments. Figure 4 lists the most important PKI capabilities for IoT deployments. While scalability is the most important, it has decreased in importance from 53 percent of respondents in 2018 to 39 percent of respondents in 2022. The ability to sign firmware for IoT devices has increased from 27 percent of respondents in 2021 to 33 percent of respondents in 2022.

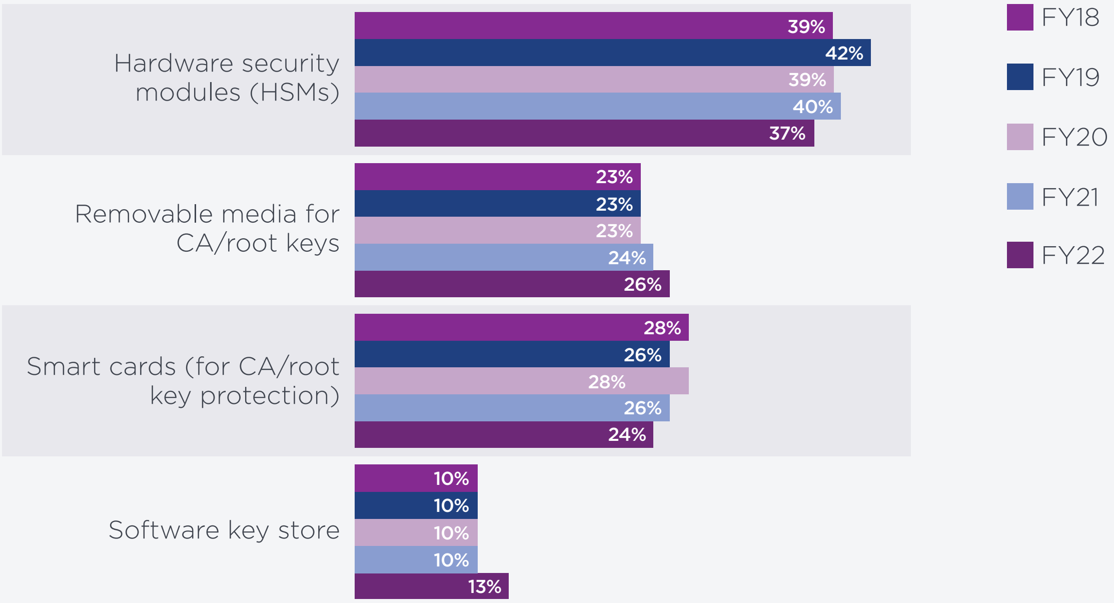
Figure 4. **What are the most important PKI capabilities for IoT deployments?** (Two responses permitted)



Challenges in achieving PKI maturity

Hardware security modules (HSMs) continue to be most often used to manage the private keys for their root/policy/issuing CAs (37 percent of respondents), as shown in Figure 5. Twenty-six percent of respondents say removable media for CA/root keys and 24 percent of respondents say smart cards are used.

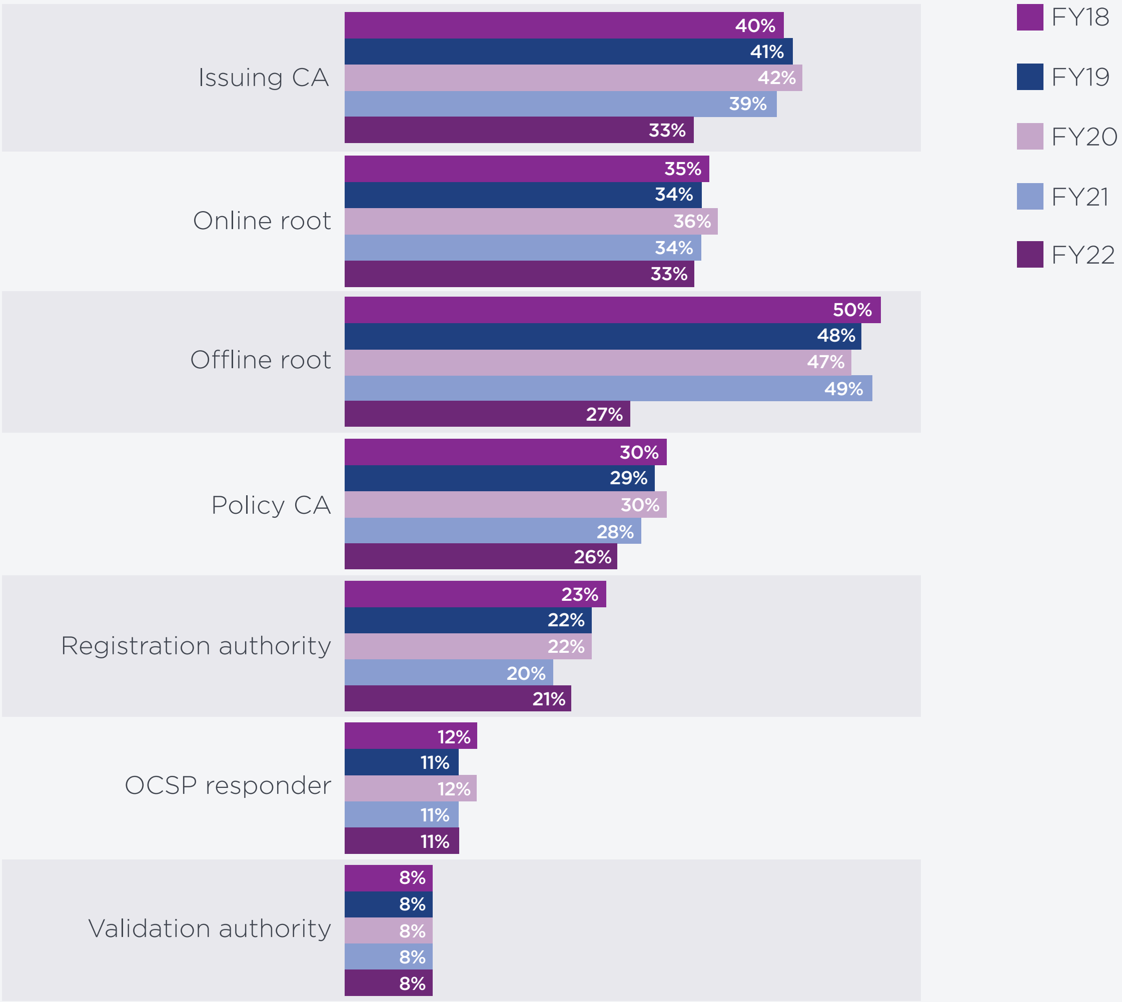
Figure 5. **How do you manage the private keys for your root/policy/issuing CAs?**



Of the 37 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 6. HSMs deployed in offline roots has declined from 49 percent of respondents in 2021 to 27 percent of respondents in 2022.

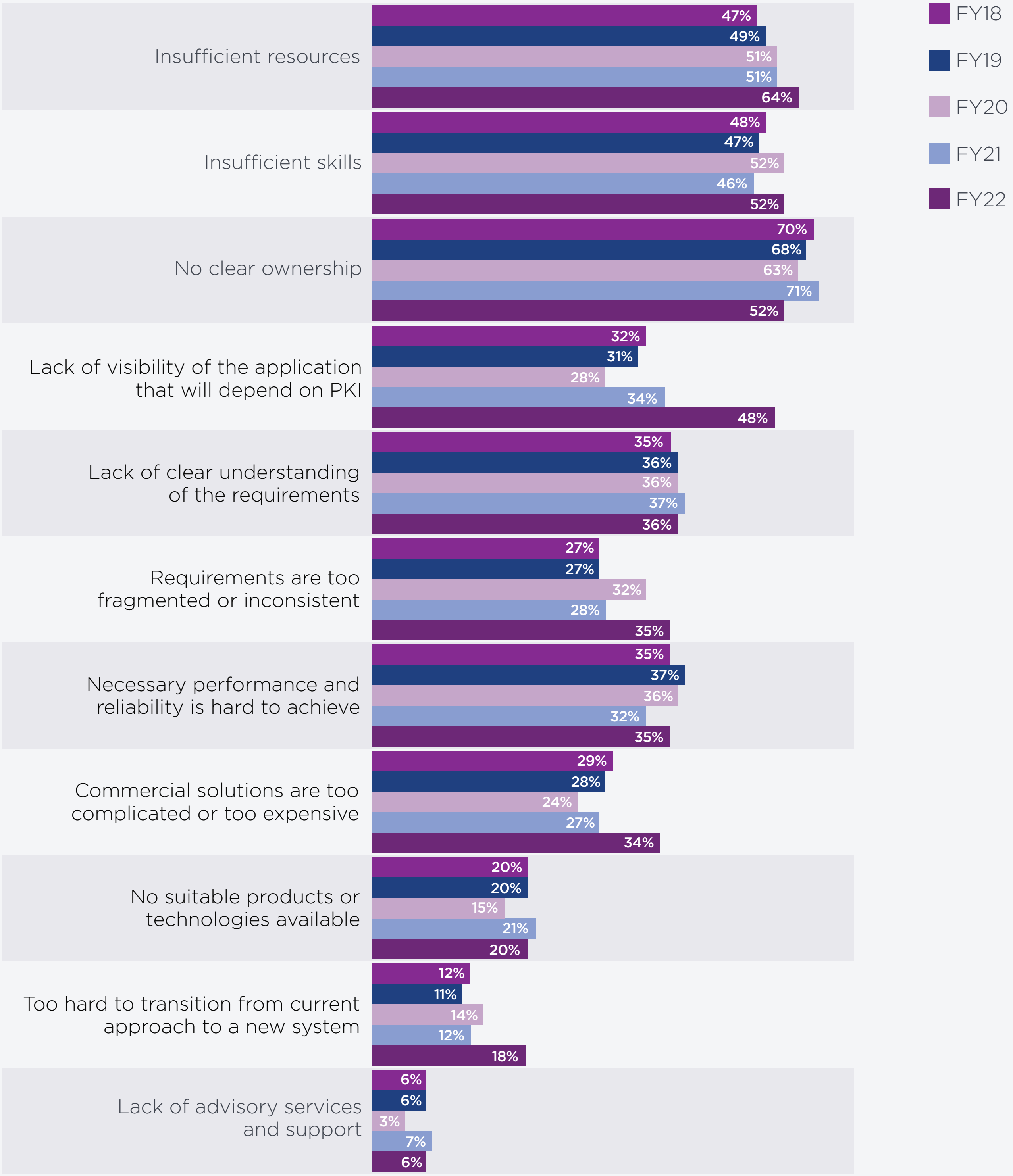
As an example of best practice, NIST calls to "Ensure that Cryptographic modules for CAs, Key Recovery Servers, and OCSP responders are hardware modules validated as meeting FIPS 140-2 Level 3 or higher" (NIST Special Publication 800-57 Part 3). Yet only 11 percent of our respondents indicate the presence of HSMs in their OCSP installations. This is a significant gap between best practices and observed practices.

Figure 6. **Where HSMs are deployed to secure PKI**
(Consolidated view — more than one response permitted)



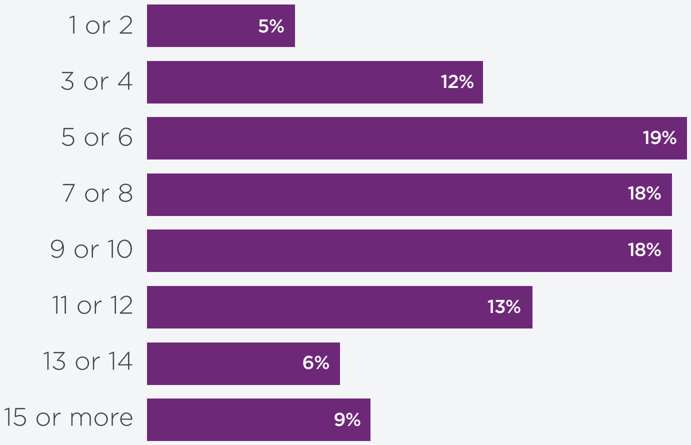
Insufficient resources, lack of skills, and no clear ownership are the top three challenges to enabling applications to use PKI. As shown in Figure 7, the challenge of not having sufficient resources has increased significantly from 51 percent of respondents in 2021 to 64 percent of respondents in 2022. Other challenges are insufficient skills (52 percent) and no clear ownership (52 percent of respondents). The lack of visibility of the applications that will depend upon PKI increased from 34 percent of respondents in 2021 to 48 percent of respondents in this year's research.

Figure 7. **The challenges in deploying and managing PKI** (Consolidated view — four responses permitted)



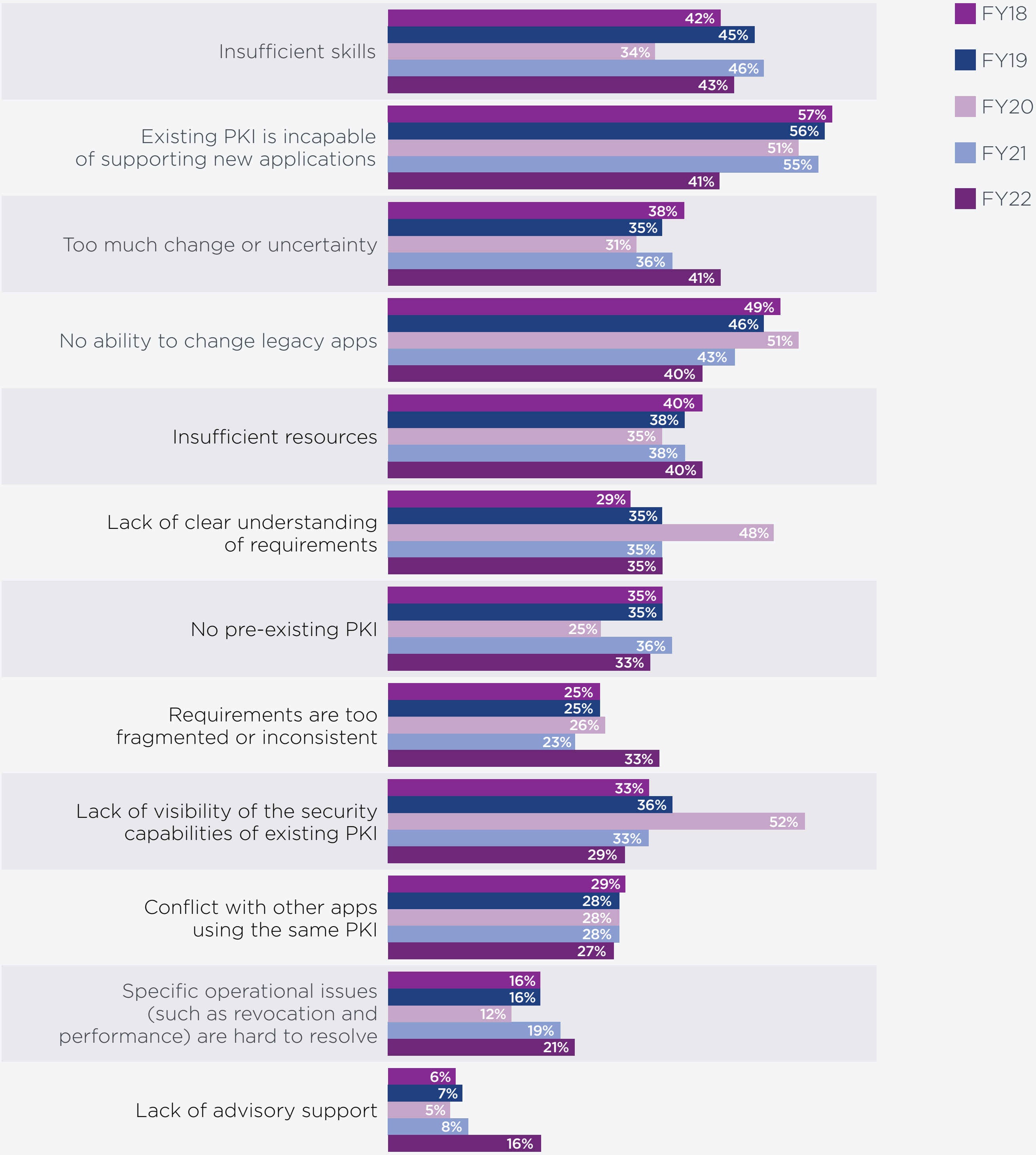
Organizations with internal CAs use an average of 6.8 separate CAs, managing an average of 52,022 internal or externally acquired certificates. As shown in Figure 8, an average of 8.4 distinct applications, such as email and network authentication, are managed by an organization's PKI. This indicates 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 PKI is a strategic part of the core IT backbone.

Figure 8. **How many distinct applications does your PKI manage certificates on behalf of?** (Consolidated view — extrapolated value is 8.4 distinct applications)



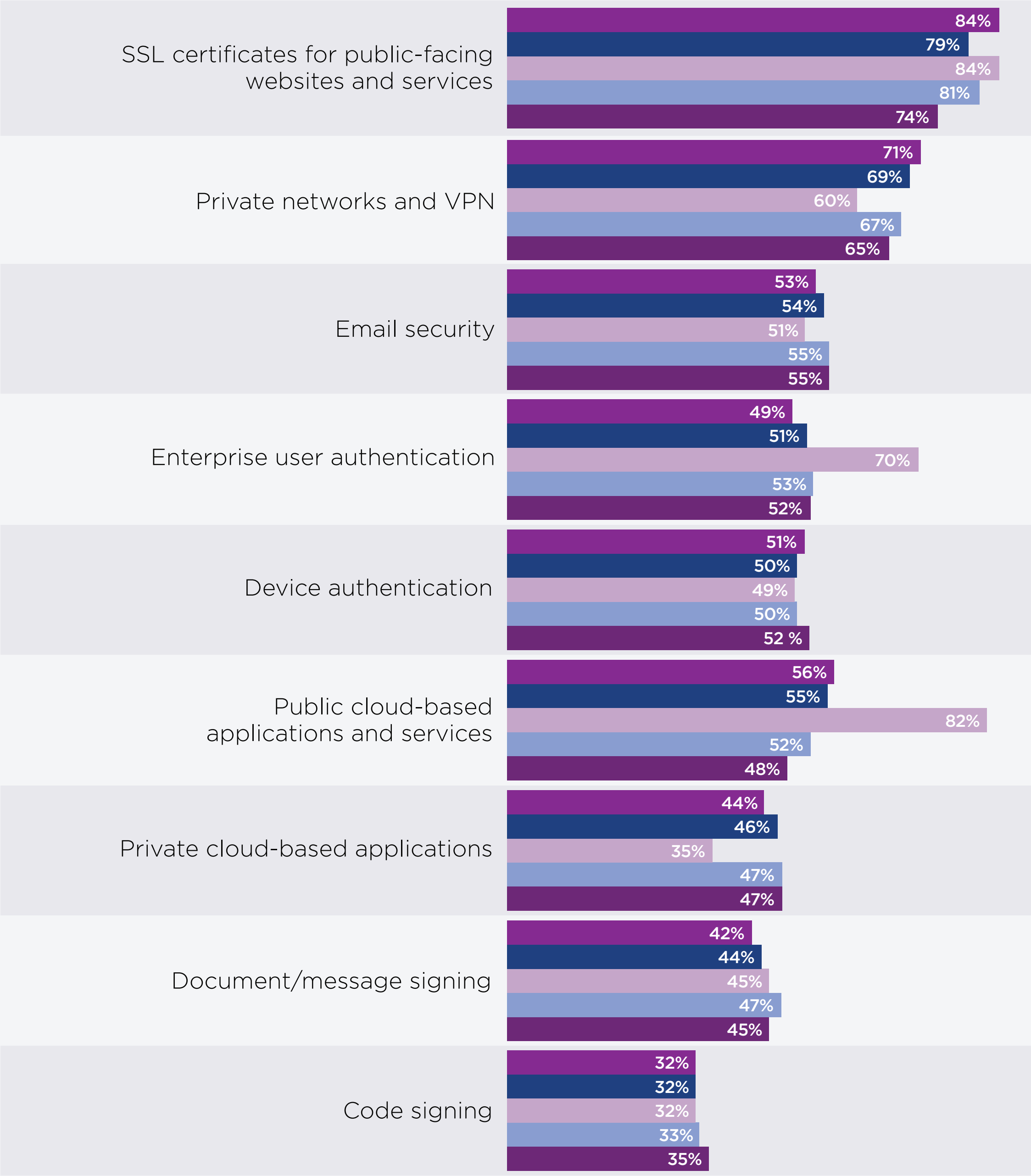
The challenge of PKI supporting new applications has declined significantly since 2021. As shown in Figure 9, the previous number one challenge has been that existing PKI is incapable of supporting new applications. However, that concern has decreased significantly from 55 percent of respondents in 2021 to 41 percent of respondents in 2022. The lack of visibility of the security capabilities of existing PKI also has decreased significantly from 52 percent of respondents in 2020 to 29 percent of respondents in 2022.

Figure 9. **What are the challenges to enable applications to utilize PKI?**
(Consolidated view — four responses permitted)



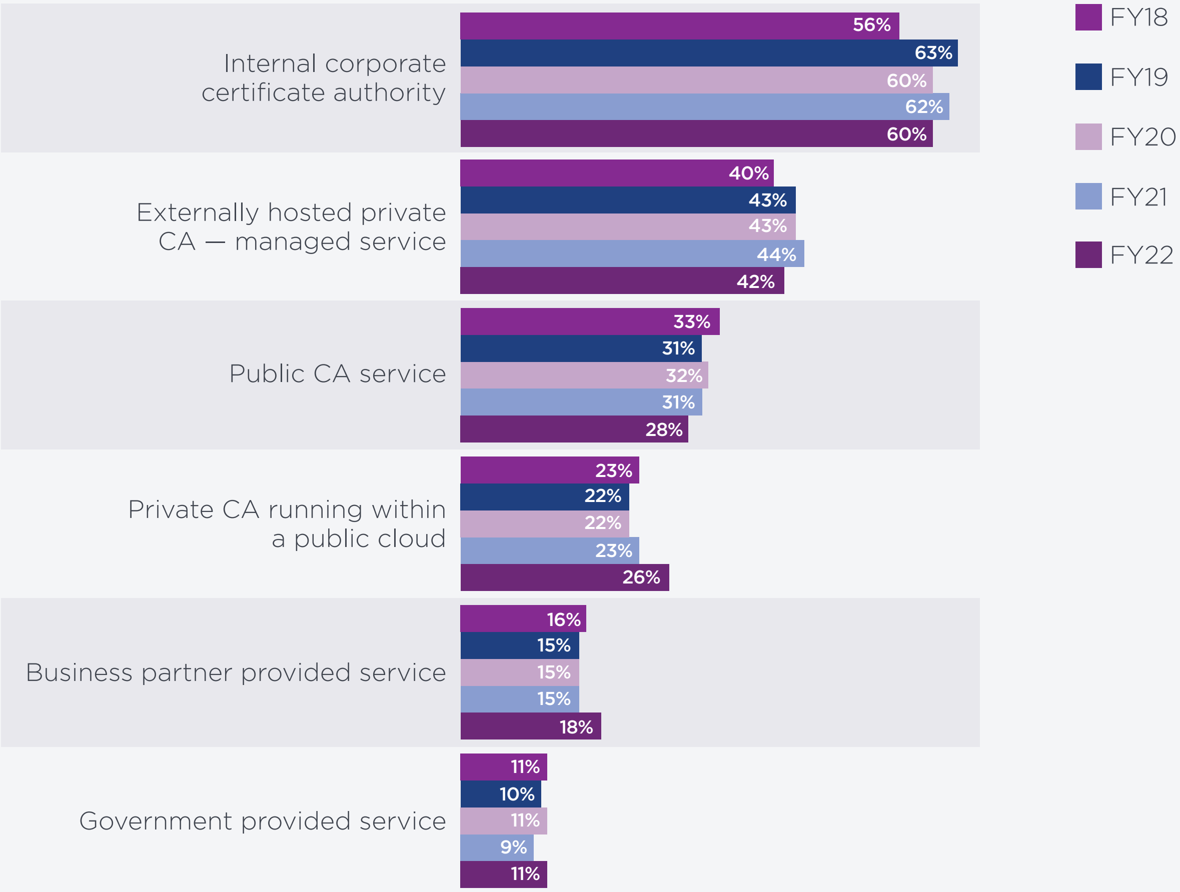
SSL certificates for public-facing websites and services are most often using PKI credentials. According to Figure 10, 74 percent of respondents say the application most often using PKI credentials is SSL certificates for public-facing websites and services. However, enterprise user authentication has decreased significantly from 70 percent of respondents in 2020 to 52 percent of respondents in 2022, and the use of public cloud-based applications and services has decreased significantly from 82 percent in 2020 to 48 percent of respondents in 2022.

Figure 10. **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 11, is through an internal corporate certificate authority (CA) or an externally hosted private CA — managed service, according to 60 percent and 42 percent of respondents, respectively.

Figure 11. **How is PKI deployed?** (Consolidated view — more than one response permitted)



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.

SECURING A WORLD IN MOTION

About Entrust Corporation

Entrust keeps the world moving safely by enabling trusted experiences for identities, payments, and digital infrastructure. We offer an unmatched breadth of solutions that are critical to enabling trust for multi-cloud deployments, mobile identities, hybrid work, machine identity, electronic signatures, encryption, and more. With more than 2,800 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us. For more information, visit **entrust.com.**

Entrust, nShield, and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners.

© 2022 Entrust Corporation. All rights reserved.