ENTRUST

PKI capabilities become business possibilities.

Are you ready?

2021 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

Ponemon Institute is pleased to present the findings of the *2021 Global PKI and IoT Trends Study*, sponsored by Entrust.

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 the realization that PKI provides important core authentication technologies for the IoT.

The PKI research is part of a larger study published in April 2021 involving 6,610 respondents in 17 countries.[2] In this report, Ponemon Institute presents the findings based on a survey of 2,513 IT and IT security who are involved in their organizations' enterprise PKI in the following 17 countries and regions: Australia, Brazil, France, Germany, Hong Kong, Japan, Korea, Mexico, Middle East, the Netherlands, the Russian Federation, Southeast Asia, Spain, Sweden, Taiwan, the United Kingdom, and the United States.

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.

The pain of managing IoT keys

New applications such as IoT devices, continue to drive the most change and uncertainty. Forty-one percent of respondents say new applications such as the IoT will drive change. Although this is a significant decrease from 52 percent of respondents in 2020, it still marks the fourth consecutive year it's come in on top. The influence of changing PKI technologies and enterprise applications increased from 21 percent of respondents in 2020 to 27 percent of respondents in 2021. Internal security policies increased significantly from 12 percent of respondents in 2020 to 20 percent of respondents in 2021.

Plan for the unplanned

The top areas expected to experience the most change and uncertainty

The top area for the 4th straight year

New applications (e.g., Internet of Things)

41%

External mandates and standards (GDPR, CMMC, Fed IoT, etc.)

37%

[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: **2021 Global Encryption Trends & Key Management Study** (sponsored by Entrust), Ponemon Institute, April 2021.

Despite continuing to be the top area of change and uncertainty, IoT is identified as the major driver for the use of PKI for the second year in a row. There is growing recognition that PKI provides important core authentication technology in the IoT. Respondents who say IoT is the most important trend driving the deployment of applications using PKI has increased from 40 percent of respondents in 2017 to 47 percent in 2021. In contrast, cloud-based services decreased from 54 percent of respondents in 2017 to 44 percent of respondents in 2021. This should define the challenges facing PKI vendors and administrators alike as they adapt the technology to these new realities.

In the next two years, an average of 45 percent of IoT devices in use will rely primarily on digital certificates for identification and authentication. 42 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.

Trends in PKI Maturity

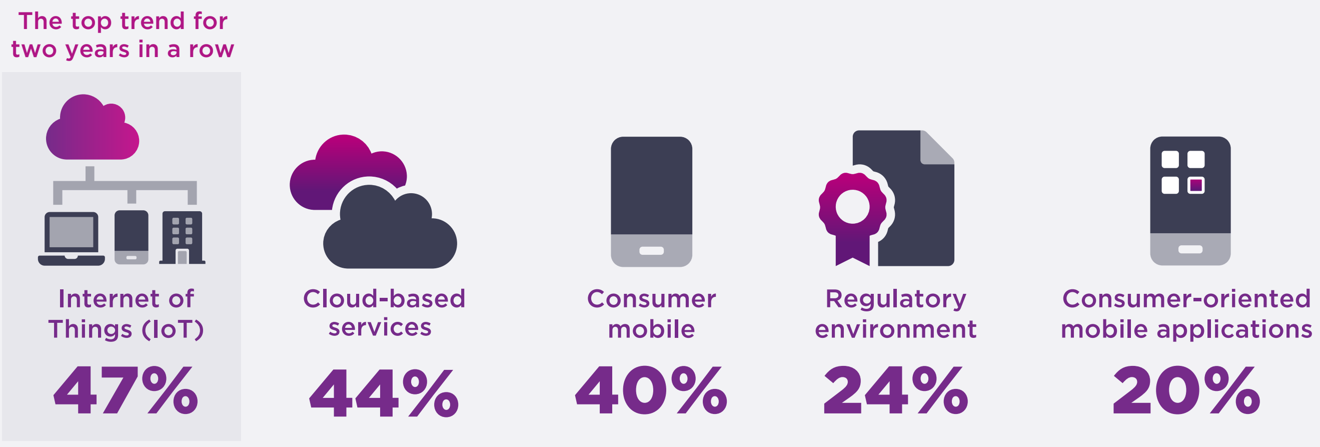
The certificate revocation technique most often deployed continues to be online certificate status protocol (OCSP), according to 57 percent of respondents. The next most popular technique is the use of automated certificate revocation list (CRL), according to 42 percent of respondents, a decrease from 47 percent of respondents in 2020.

Similar to the last couple of years, 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) continue to be most often used to manage the private keys for their root/policy/issuing CAs. Of the 40 percent of organizations in this study that use HSMs to secure PKI, they are used across the entire architecture of the PKI. Twenty-six percent of respondents say smart cards are used. Forty-one percent of respondents say they have PKI specialists on staff who are involved in their organizations' enterprise PKI.

Evolving for the connected world

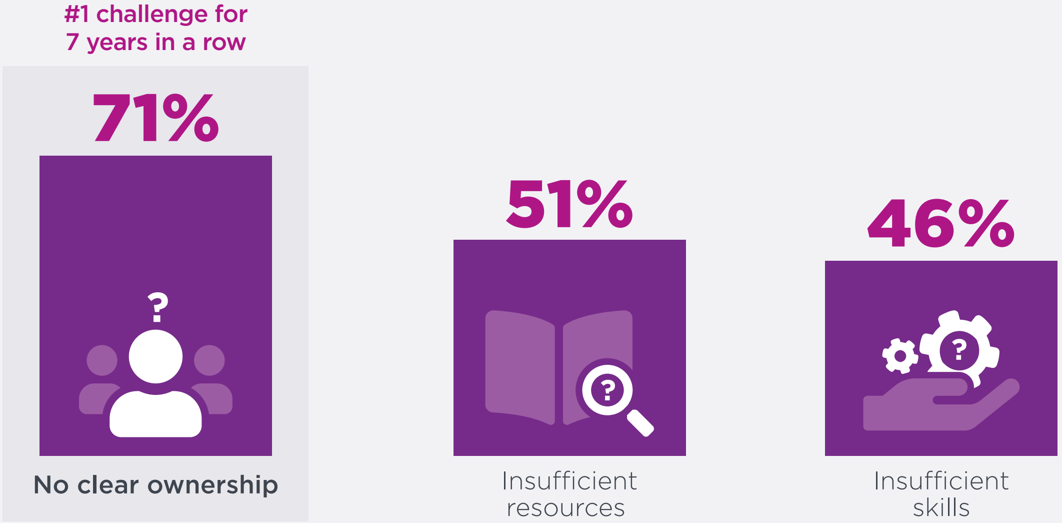
The most important trends driving the deployment of applications using PKI



As an example of best practices, 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.

No clear ownership and insufficient resources and skills are the top three challenges to enabling applications to use PKI. The challenge of not having clear ownership was the top challenge for the 5th year in a row and increased significantly from 63 percent of respondents in 2020 to 71 of respondents in 2021. Other challenges are insufficient resources (51 percent) and insufficient skills (46 percent of respondents).

Help needed!
Top PKI deployment and management challenges



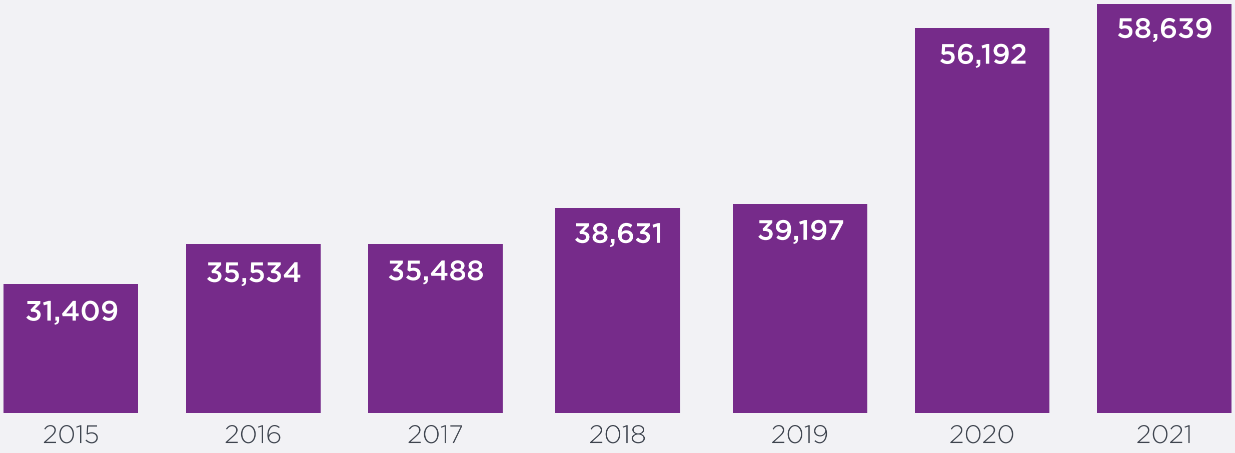
Too much change or uncertainty has decreased from 45 percent of respondents in last year's research to 34 percent of respondents in 2021. However, lack of visibility of the applications that will depend upon PKI increased from 28 percent of respondents in 2020 to 34 percent of respondents in this year's research.

Trends in PKI challenges

Organizations with internal CAs use an average of 7.2 separate CAs, managing an average of 58,639 internal or externally acquired certificates. An average of 9.12 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.

More certificates, more problems

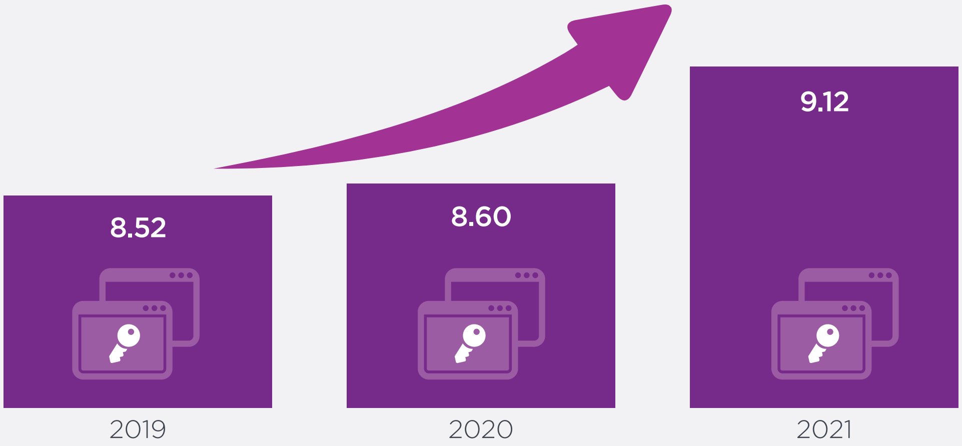
The average number of certificates is up 50% since 2019, yet with a PKI skills shortage, is there a management issue?



*Average number of certificates issued by organization

PKI is the pulse of enterprise IT

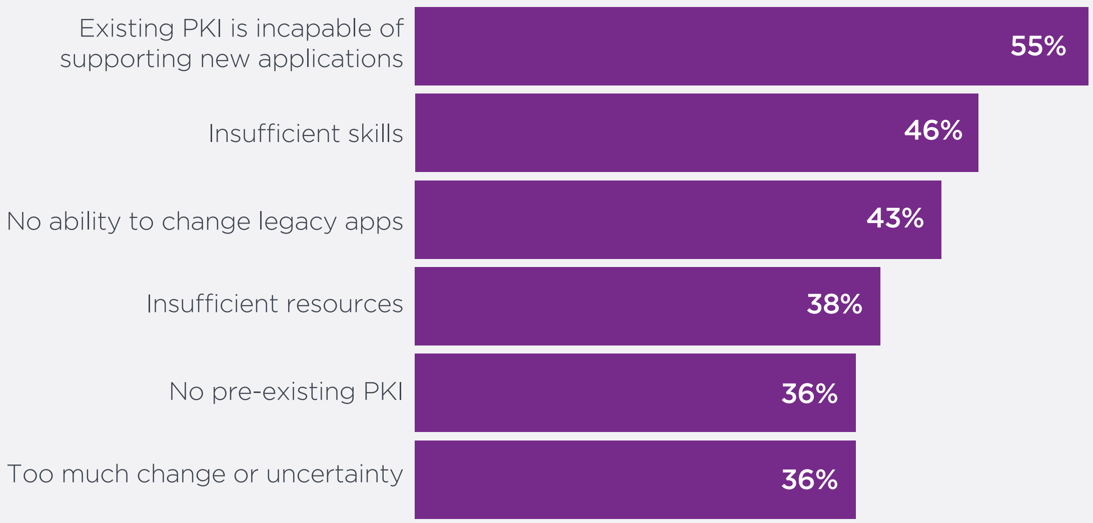
Average number of distinct applications using PKI continue to rise for organizations with internal CAs



In many cases, existing PKI is incapable of supporting new applications. The number one challenge is that 55 percent of respondents say existing PKI is incapable of supporting new applications. The challenge of insufficient skills increased significantly from 34 percent of respondents to 46 percent of respondents. The lack of visibility of the security capabilities of existing PKI has decreased significantly from 52 percent of respondents in 2020 to 33 percent of respondents in 2021.

Common Criteria EAL Level 4+ is the most important security certification when deploying PKI infrastructure and PKI-based applications. Sixty-three percent say common criteria followed by 62 percent who say FIPS 140 is the most important when deploying PKI. Twenty-five percent of respondents say regional standards such as digital signature laws are important. 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.

PKI capabilities become business possibilities. Are you ready?
The top challenges to enable applications to utilize PKI

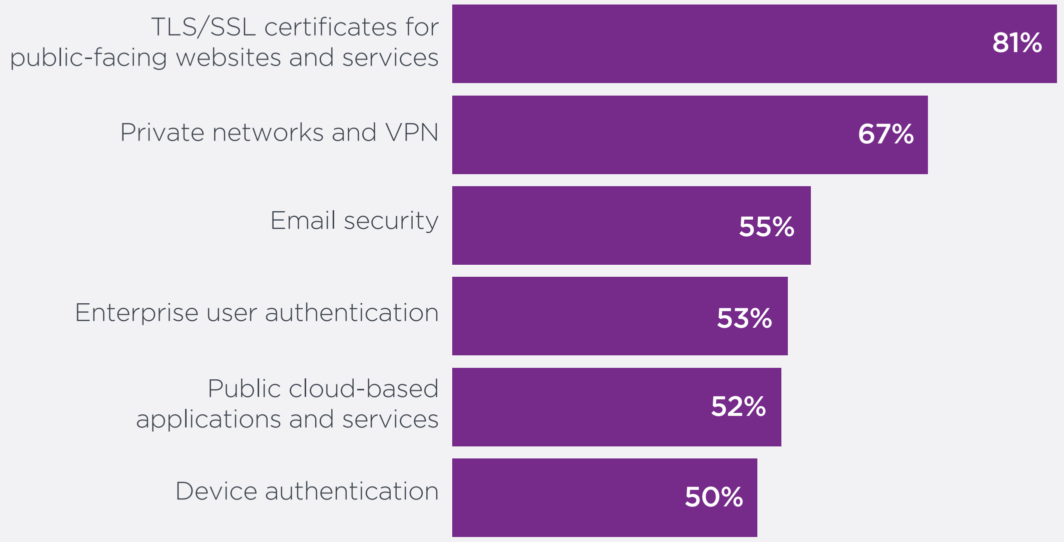


TLS/SSL certificates for public-facing websites and services are most often using PKI credentials. Eighty-one percent of respondents say the application most often using PKI credentials is TLS/SSL certificates for public-facing websites and services. However, enterprise user authentication has decreased significantly from 70 percent of respondents in 2020 to 53 percent of respondents in 2021, and the use of public cloud-based applications and services has decreased significantly from 82 percent in 2020 to 52 percent of respondents in 2021. Private networks and VPN have increased from 60 percent to 67 percent of respondents in 2021.

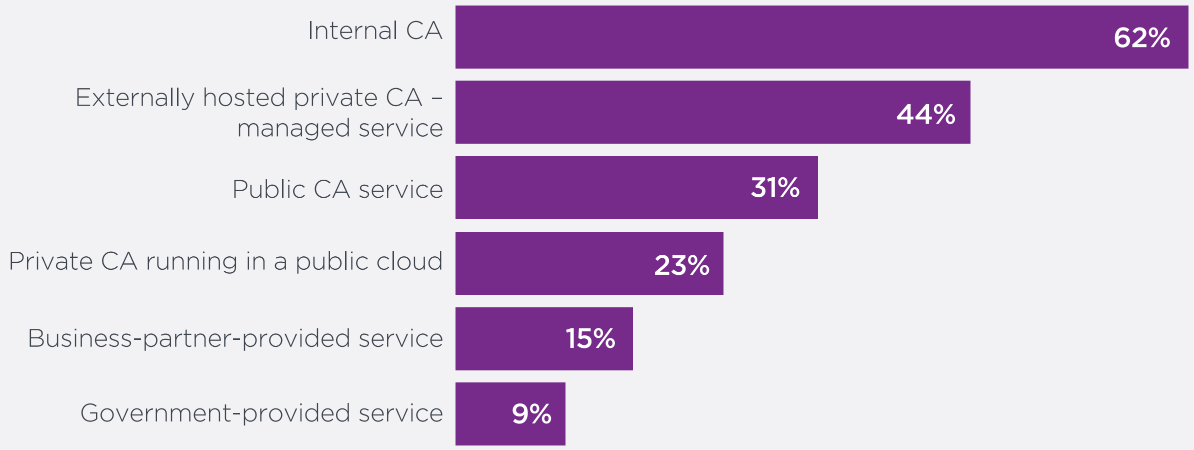
What are the most popular methods for deploying enterprise PKI? The most cited methods for deploying enterprise PKI are through an internal corporate certificate authority (CA) or an externally hosted private CA – managed service, according to 62 percent and 44 percent of respondents, respectively.

Externally hosted private CAs have increased in usage since 2017 from 38 percent of respondents to 44 percent of respondents in 2021.

How PKI is driving the connected world
Top applications for PKI credentials



Diversified PKI deployment
The most popular methods for deploying PKI



Ponemon INSTITUTE

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.

ENTRUST

SECURING A WORLD IN MOTION

About Entrust Corporation

Entrust keeps the world moving safely 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. For more information, visit **entrust.com.**