ENTRUST
SECURING A WORLD IN MOTION

nCIPHER AN ENTRUST COMPANY

Ponemon INSTITUTE

2020 Global PKI and IoT Trends Study

Executive Summary

Ponemon Institute is pleased to present an executive summary of the findings of the *2020 Global PKI and IoT Trends Study*, sponsored by nCipher Security, an Entrust company.

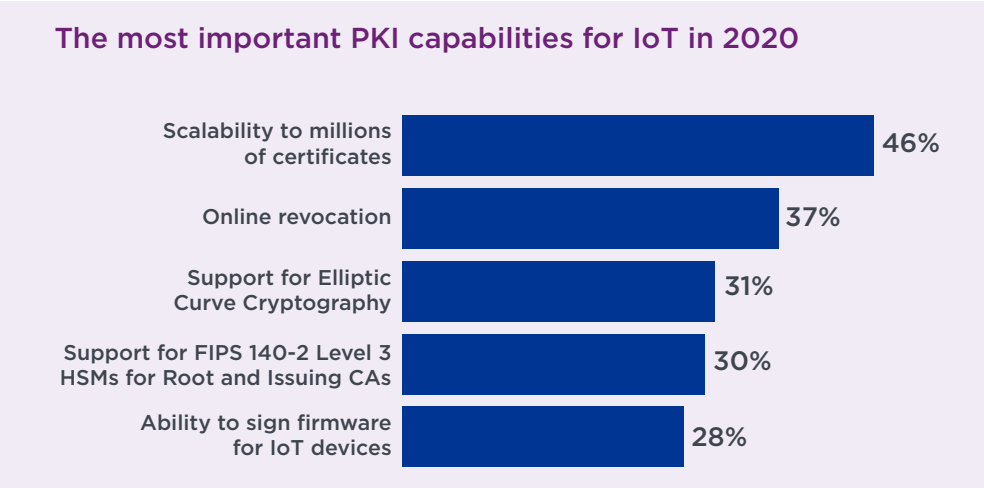
According to the findings, digital certificate use is growing rapidly for cloud applications and user authentication. Additionally, the rapid growth in the use of IoT devices[1] is having an impact on the use of PKI technologies and there is realization that PKI provides important core authentication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

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. Fifty-two 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.

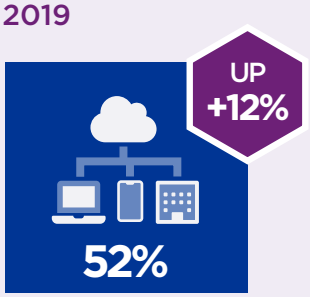


[1] IDC predicts by 2025 there will be 41.6 billion IoT devices connected to businesses and these "things" will generate 79.4 zettabytes of data.

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

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. This should define the challenges facing PKI vendors and administrators alike as they adapt the technology to these new realities.

Top area of change in PKI since 2019



New applications such as 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. Forty-five 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

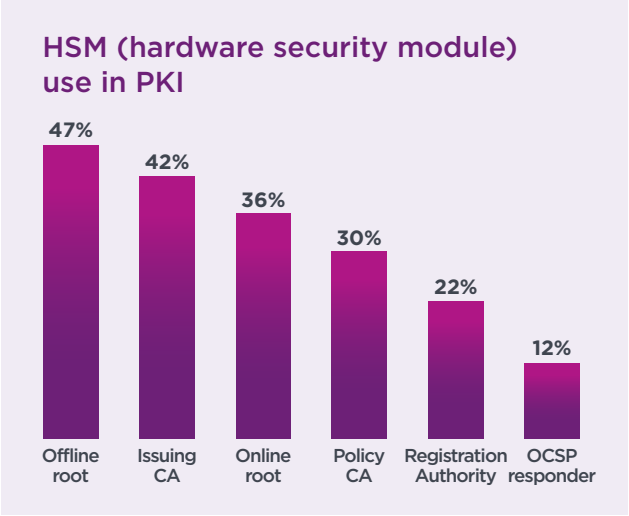
The certificate revocation technique most often deployed continues to be online certificate status protocol (OCSP), according to 53 percent of respondents (an increase from 46 percent of respondents since the 2015 study). The next most popular technique is the use of automated certificate revocation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

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. 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. 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.

> « Fifty-two 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. »

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.

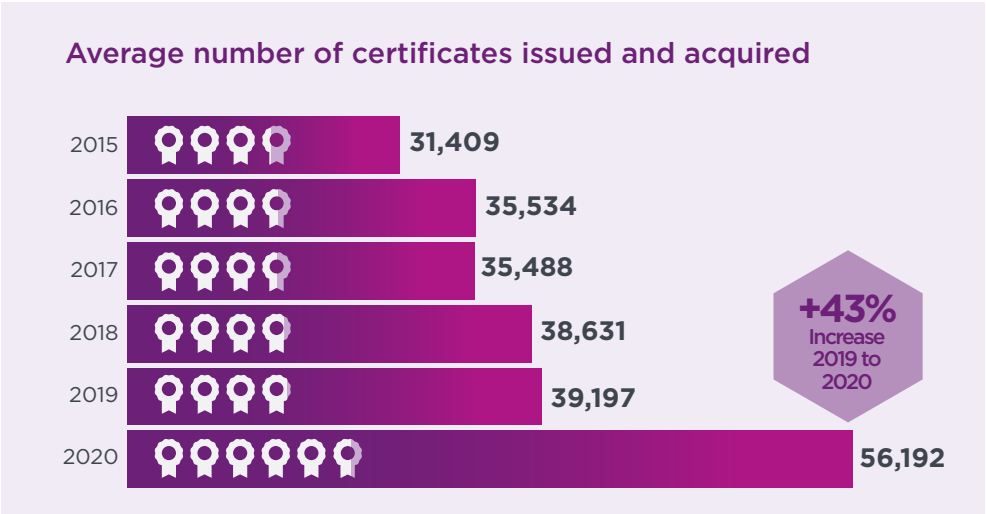


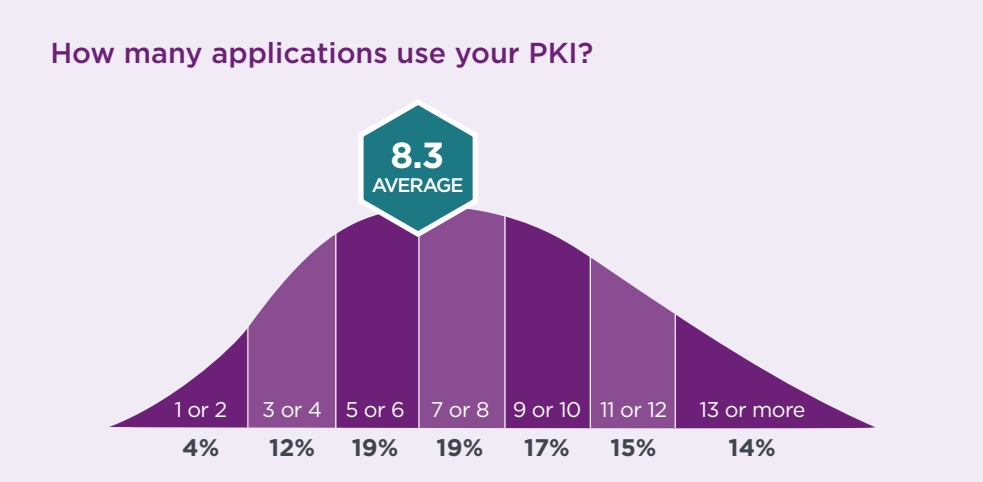
No clear ownership, insufficient resources and skills are the top three challenges to enabling applications to use PKI. The most significant challenges are based on organizational issues. These include no clear ownership (63 percent of respondents), insufficient skills (52 percent) and insufficient resources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

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.

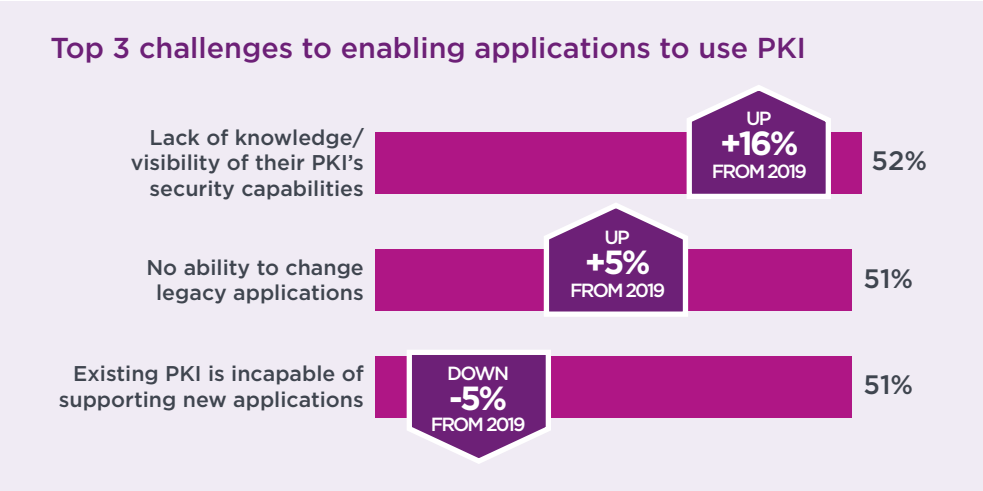
Trends in PKI challenges

Organizations with internal CAs use an average of 7.2 separate CAs, managing an average of 56,192 internal or externally acquired certificates. An average of 8.3 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.





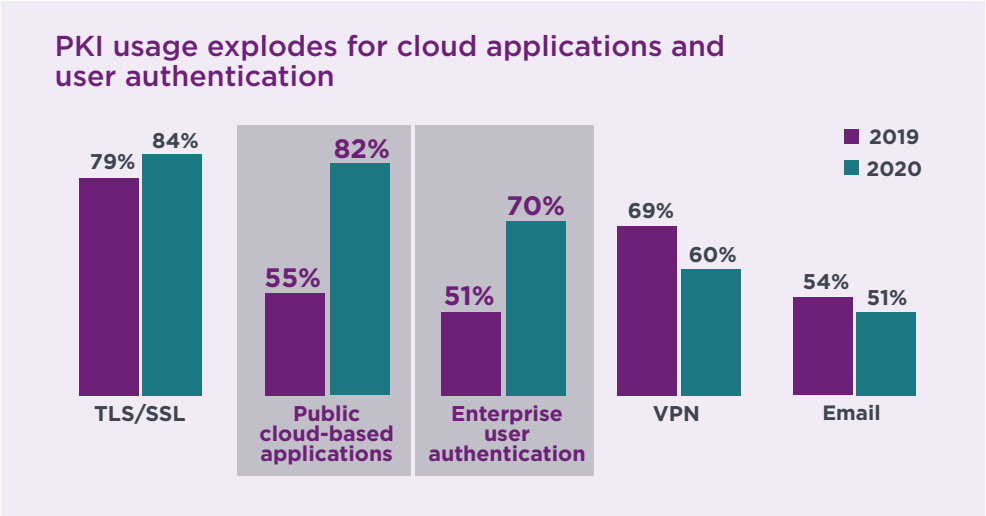
The primary challenges to enabling applications to utilize PKI are the lack of visibility of the security capabilities of existing PKI, the inability of existing PKI to support new applications and the inability to change legacy apps. Since 2019 the lack of visibility of the security capabilities of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



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).

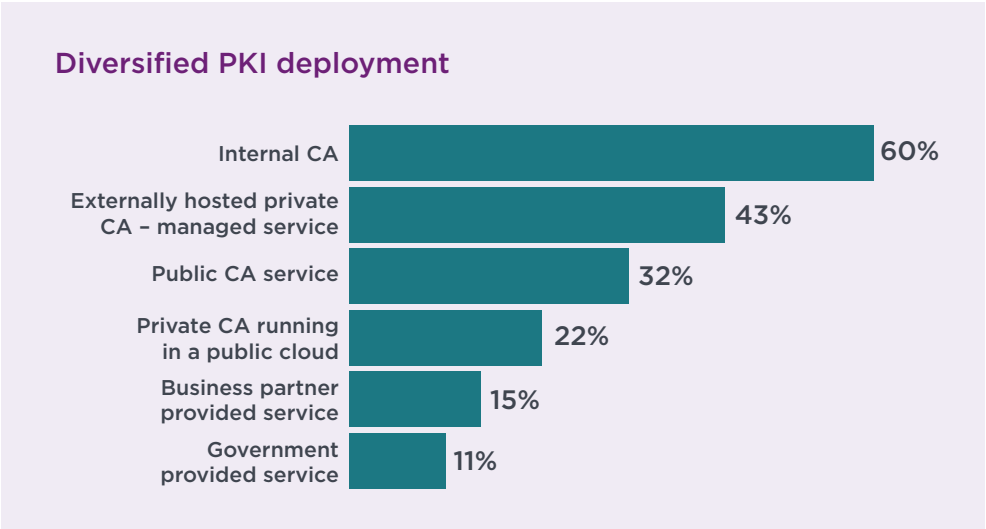
Common Criteria EAL Level 4+ is the most important security certification when deploying PKI infrastructure and PKI-based applications. Sixty-seven percent say Common Criteria followed by 60 percent who say FIPS 140 is the most important when deploying PKI. Twenty-six percent of respondents say regional 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.

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



What are the most popular methods for deploying enterprise PKI? The most cited method for deploying enterprise PKI 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.



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

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**

CLICK TO DOWNLOAD THE FULL REPORT

entrust.com

ncipher.com