Ponemon INSTITUTE

NCIPHER
AN ENTRUST DATACARD COMPANY

2019 GLOBAL PKI AND IoT TRENDS STUDY

Executive Summary

Ponemon Institute is pleased to present an executive summary of the findings of the *2019 Global PKI and IoT Trends Study*, sponsored by nCipher Security, an Entrust Datacard company. According to the findings, 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.

This report summarizes the fifth annual results of a survey completed by 1,884 IT and IT security practitioners in the following 14 countries/regions: Australia, Brazil, France, Germany, Hong Kong and Taiwan, India, Japan, Mexico, the Middle East (Saudi Arabia and the United Arab Emirates), the Russian Federation, South Korea, Southeast Asia (Indonesia, Malaysia, Philippines, Thailand, and Vietnam), 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, 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 2019 involving 5,856 respondents in 14 countries/regions.[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.

The influence of the IoT

PKI changes due to external mandates continue to decline, but changes due to new applications continue to increase. Thirty-nine percent of respondents say the biggest change will be external mandates and standards (a significant decline from 56 percent of respondents in 2015) and 40 percent of respondents say new applications such as the Internet of Things will drive change (a significant increase from 14 percent of respondents in 2015). The influence of PKI technologies and enterprise applications also decreased significantly since 2015.

IoT is becoming a major driver for the use of PKI. There is growing recognition that PKI provides important core authentication technology for 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 to 41 percent in 2019. In contrast, cloud-based services as an influence in the deployment of applications that make use of PKI decreased from 64 percent of respondents in 2015 to 49 percent of respondents in this year's research. This should define the challenges facing PKI vendors and administrators alike as they adapt the technology to these new realities.

PKI ENABLES ORGANIZATIONS TO EMBRACE MARKET TRENDS

49%
CLOUD-BASED SERVICES

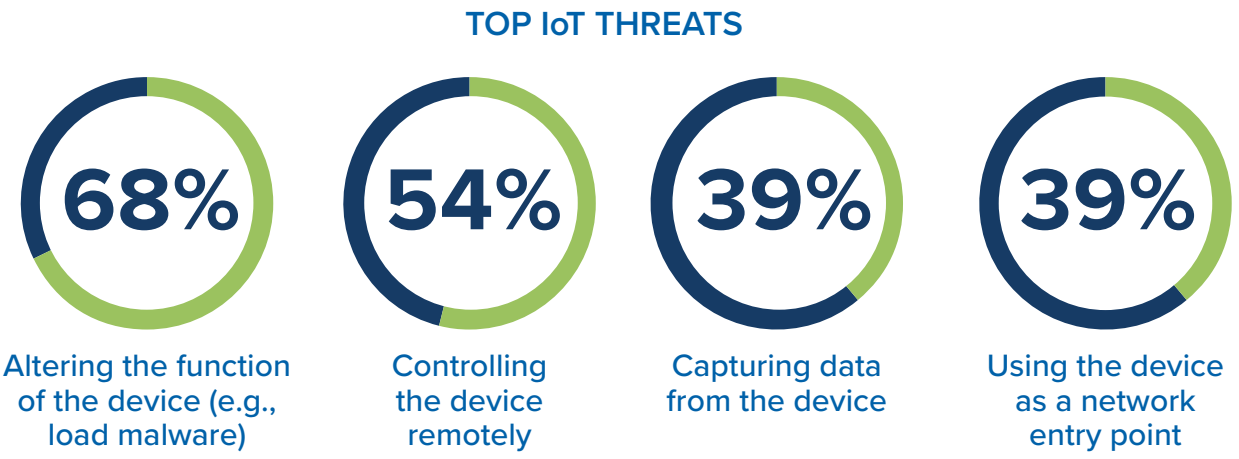
44%
CONSUMER MOBILE

41%
INTERNET OF THINGS *(fastest growth)*

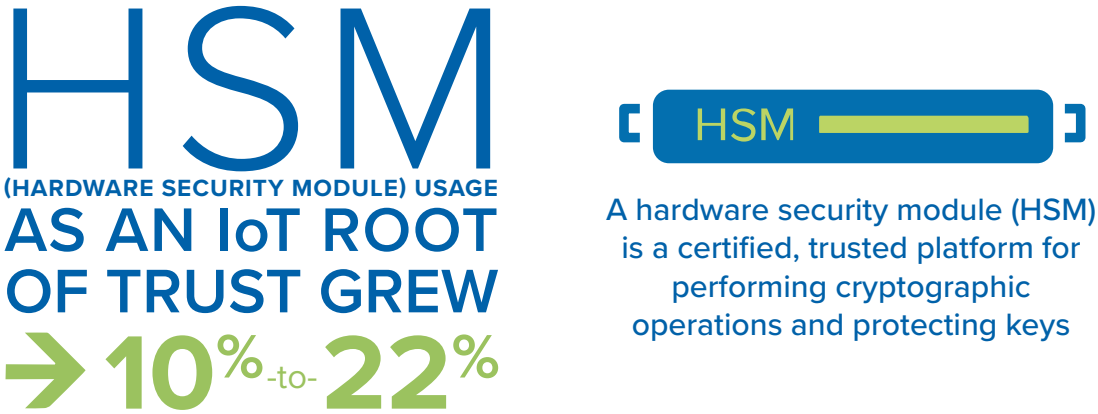
[1] Gartner predicts by 2020 there will be 20.4 billion IoT devices, of which 7.5 billion will be for business purposes and 12.8 will be for consumers.
[2] See: *2019 Global Encryption Trends Study* (sponsored by nCipher), Ponemon Institute, April 2019.

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

Altering the function of an IoT device is the most significant threat to IoT deployments. When rating the top IoT threats, 68 percent of respondents chose altering the function of a device (e.g., by loading malware), followed by controlling the device remotely (54 percent). The threat of use of an IoT device as a network entry point, as well as capturing data from an IoT device, each were rated as top threats by 39 percent of respondents.



Protecting confidentiality and integrity of device data is the most important IoT security capability today. Out of five IoT security capabilities, respondents rated protection of the confidentiality and integrity of device data as the most important, followed by device authentication, monitoring device behavior, device discovery, and delivery of patches and updates to devices.



Trends in PKI maturity

The certificate revocation technique most often deployed continues to be online certificate status protocol (OCSP), according to 58 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) (44 percent of respondents).

Similar to last year, 30 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 the most common method used to manage the private keys for root/policy/issuing CAs. Twenty-six percent of respondents say smart cards are used. A related question revealed that almost half of respondents (45 percent) say they have PKI specialists on staff.

ENTERPRISES ARE MISSING THE MARK ON BEST PRACTICES

30%

not using ANY **certificate revocation technique**

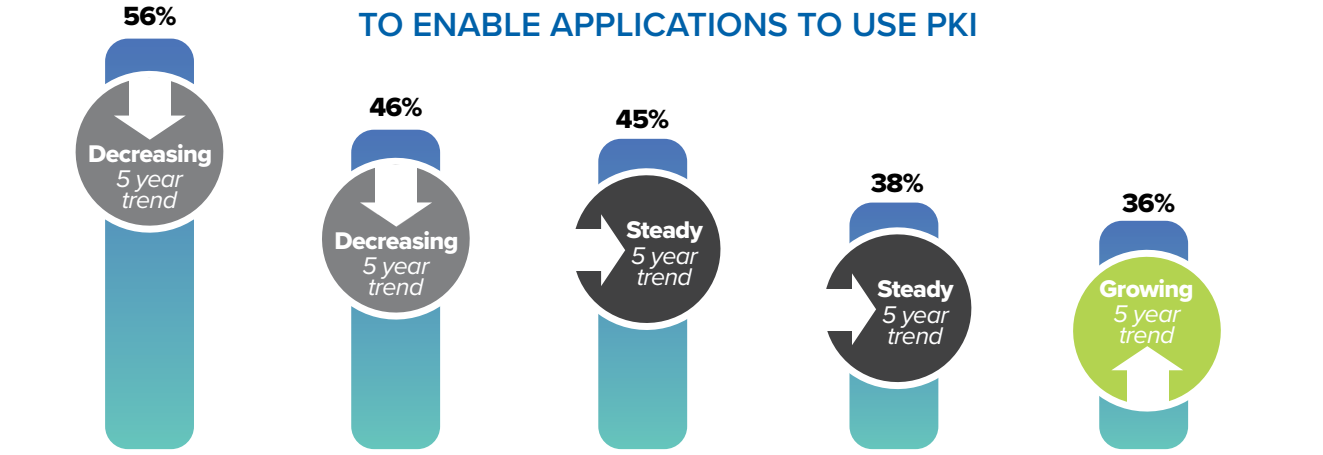
BUT THEY ARE ALSO INCREMENTALLY IMPROVING SECURITY IN SOME AREAS

Use of ***HSMs to manage private keys*** is up *3% from 2018 to 42% (top method)*

Of the 42 percent of organizations in this study that use HSMs to secure PKI, they are used across the entire architecture of the PKI. 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.

It is often difficult for applications to use PKI. The most significant challenge organizations will continue to face, with respect to enabling applications to use PKI, is the inability of an existing PKI to support new applications, according to 56 percent of respondents. However, this has declined from 63 percent of respondents in 2015. This finding could be based on respondents' concerns about a dearth of resources and expertise.

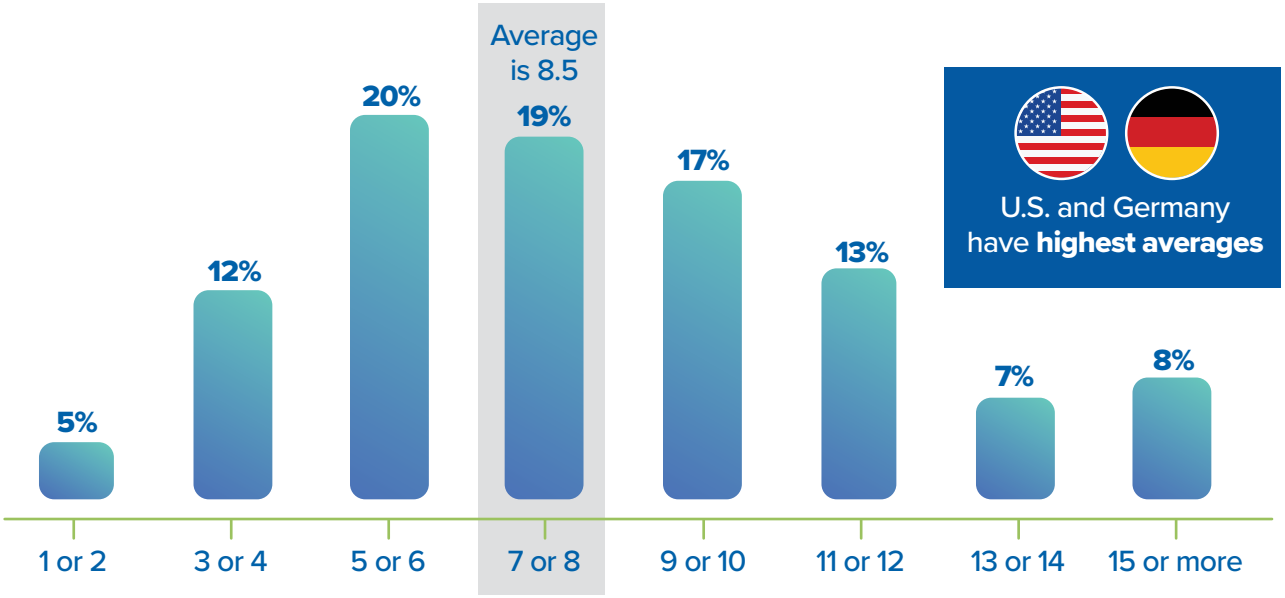
BUSINESSES FACE MANY CHALLENGES TO ENABLE APPLICATIONS TO USE PKI



Trends in PKI challenges

Organizations with internal CAs use an average of eight separate issuing CAs, managing an average of 38,631 internal or externally acquired certificates. An average of eight distinct applications, such as email and network authentication, are supported 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.

HOW MANY DISTINCT APPLICATIONS DOES YOUR PKI MANAGE CERTIFICATES ON BEHALF OF?



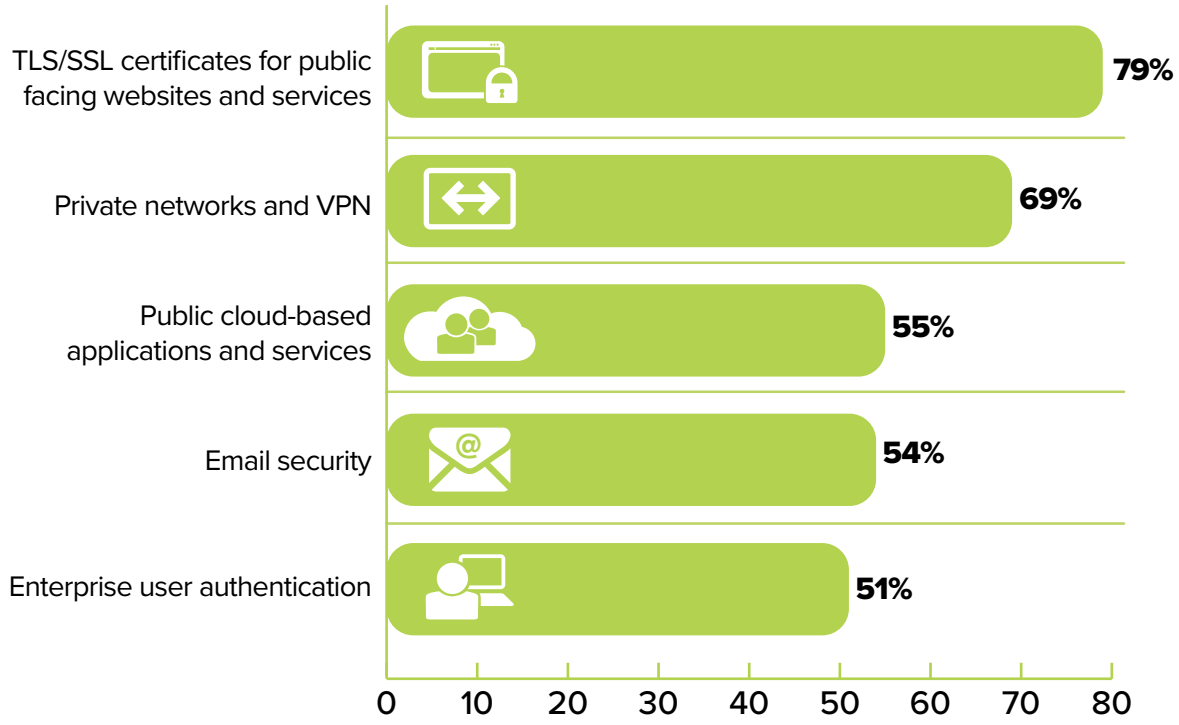
The main PKI deployment challenge continues to be the lack of clear ownership of the PKI function. Sixty-eight percent of respondents believe there is no one function responsible for managing PKI. This is not in line with best practices, which assume as a baseline a sufficient degree of staffing and competency to define and maintain the process and procedures of which a modern PKI depends.

No clear ownership continues to be the **top PKI challenge**

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

Private networks and VPN and cloud-based applications and services increase the use of PKI credentials significantly. Seventy-nine percent of respondents say the application most often using PKI credentials is SSL certificates for public facing websites and services. However, this finding decreased from 84 percent of respondents in last year's research. Other applications and services primarily used are private networks and VPN (69 percent of respondents), public cloud-based applications and services (55 percent of respondents), email security (54 percent of respondents) and enterprise user authentication (51 percent of respondents). 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.

TOP APPLICATIONS USING PKI



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 63 percent and 43 percent of respondents, respectively.

> PKI is at the core of the enterprise IT backbone.

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 Datacard 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**

CLICK TO DOWNLOAD THE FULL REPORT

Search: nCipherSecurity

www.ncipher.com

nCIPHER
AN ENTRUST DATACARD COMPANY