THALES

Ponemon INSTITUTE

2018 GLOBAL PKI TRENDS STUDY

Sponsored by Thales eSecurity

Independently conducted by Ponemon Institute LLC

SEPTEMBER 2018

EXECUTIVE SUMMARY

#2018GlobalPKI

Ponemon Institute is pleased to present the findings of the *2018 Global PKI Trends Study*, sponsored by Thales eSecurity. 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 fourth annual results of a survey completed by 1,688 IT and IT security practitioners in the following 12 countries: Australia, Brazil, France, Germany, India, Japan, Mexico, the Middle East, the Russian Federation, South Korea, the United Kingdom, and the United States.[2]

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 2018 involving 5,252 respondents in 12 countries.[3] 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 increasing influence of the IoT on PKI

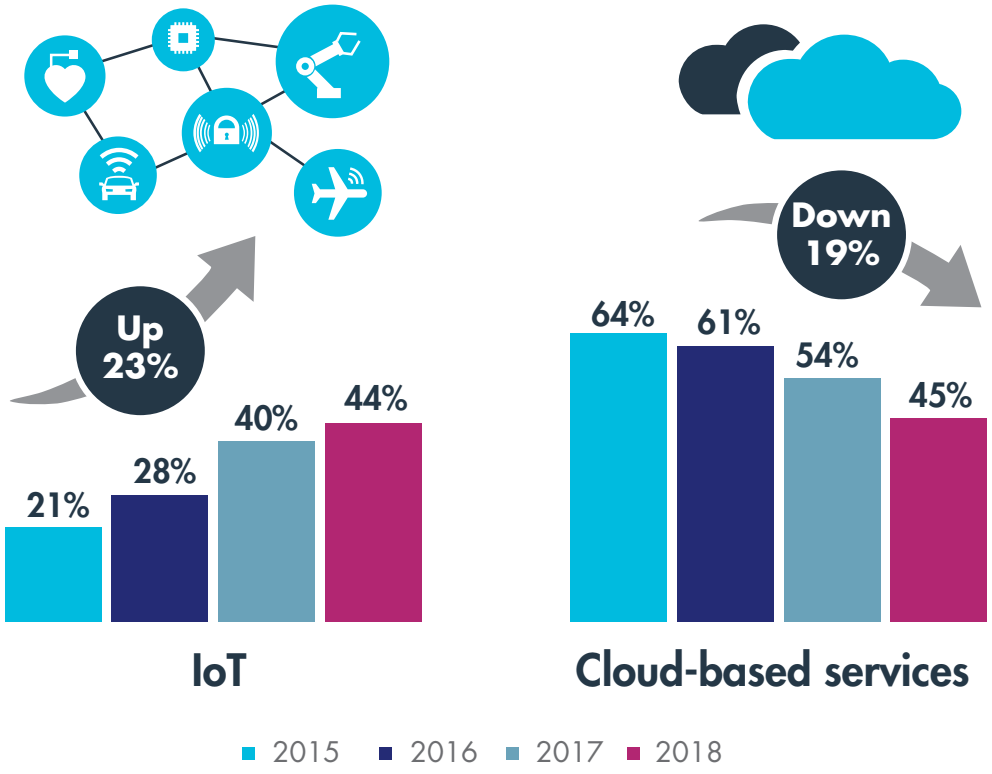
PKI changes due to external mandates continue to decline, but changes due to new applications like the IoT continue to increase. Forty-two percent of respondents say the biggest change will be external mandates and standards (a decline from 47 percent of respondents last year) and 42 percent of respondents say new applications such as the Internet of Things will drive change (an increase from 36 percent of last year's respondents). The influence of changing PKI technologies and enterprise applications also decreased significantly since 2015.

[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] The Middle East region includes the United Arab Emirates and Saudi Arabia.

[3] See: *2018 Global Encryption Trends Study* (sponsored by Thales eSecurity), Ponemon Institute, April 2018.

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 to 44 percent. In contrast, cloud-based services as an influence on deployment of applications that make use of PKI decreased from 54 percent of respondents in last year's study to 45 percent of respondents in this year's research. The needs of the IoT, cloud-based services, and consumer mobile are the most dominant influences that PKI vendors and administrators must contend with.



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-three 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.

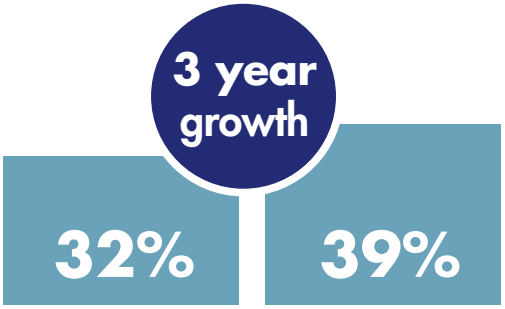
42%

of IoT devices in use will use **digital certificates** for identification/authentication in the next **two years**.

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 (an increase from 54 percent of respondents in last year's study). The next most popular technique is the use of automated certificate revocation list (CRL) (47 percent of respondents). Interestingly, and somewhat surprisingly, 30 percent of respondents say they do not deploy a certificate revocation technique.

Hardware security modules (HSMs) are the dominant means used to manage private keys for root/policy/issuing CAs. Twenty-eight percent of respondents say smart cards are used, and another 23 percent use removable media.



HSMs

Increasing use of HSMs to protect root/policy/issuing CAs

Of the 39 percent of organizations in this study that use HSMs to secure PKI, they are used across the 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 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.

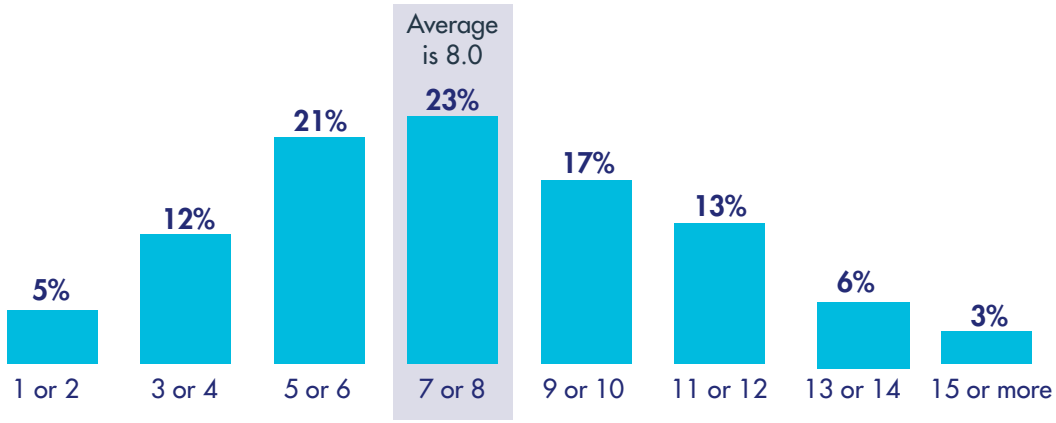
It is often difficult for applications to use PKI. The most significant challenge organizations will continue to face, with respect to enabling applications to use PKI, is the inability of an existing PKI to support new applications, according to 57 percent of respondents. However, this has declined from 63 percent of respondents in 2015. This finding could be based on respondents' concerns about a dearth of resources and expertise.

"30 PERCENT OF RESPONDENTS SAY THEY DO NOT DEPLOY A CERTIFICATE REVOCATION TECHNIQUE."

Trends in PKI challenges

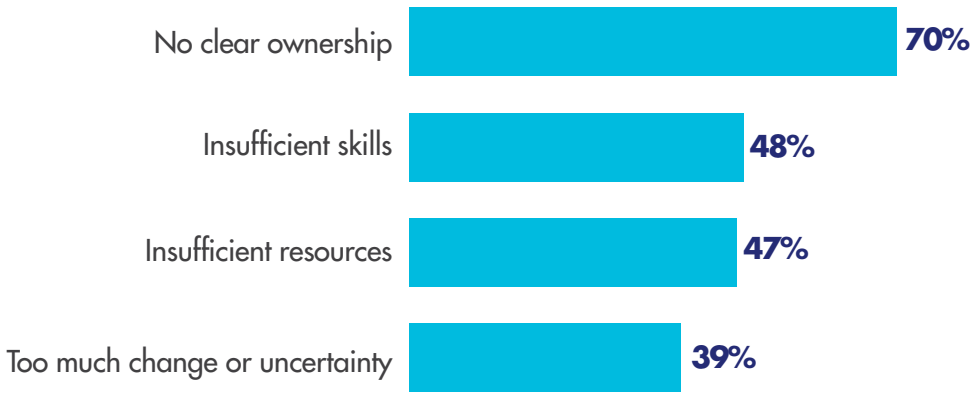
Organizations with internal CAs use an average of eight separate issuing CAs, managing an average of 38,631 internal or externally acquired certificates. An average of eight distinct applications, such as email and network authentication, are supported by an organization's PKI. This indicates that the PKI is at the core of the enterprise IT backbone.

HOW MANY APPLICATIONS USE YOUR PKI?

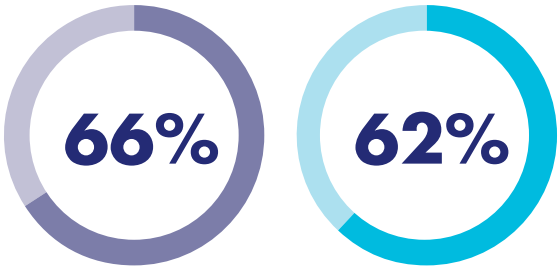


The main PKI deployment challenge is the lack of clear ownership of the PKI function. Seventy percent of respondents believe there is no one function responsible for managing PKI, a slight increase from 2015 and by far the top challenge year after year. This lack of clear ownership is not in line with 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.

TOP CHALLENGES IN DEPLOYING/MANAGING PKI



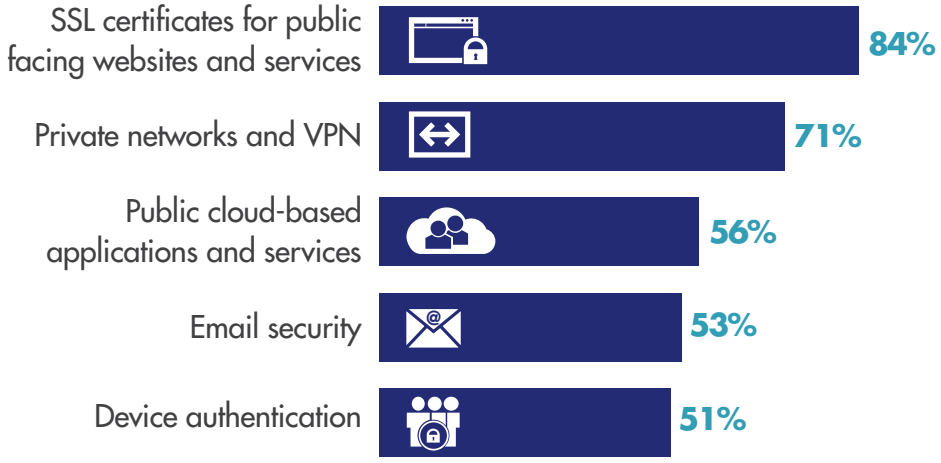
Common Criteria EAL Level 4+ is the most important security certification when deploying PKI infrastructure and PKI-based applications. According to Figure 11, 66 percent say Common Criteria followed by 62 percent say FIPS 140 is the most important when deploying PKI. Twenty-six percent say it is regional 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.



IMPORTANCE OF COMMON CRITERIA AND FIPS CERTIFICATION FOR PKI

Private networks and VPN and cloud-based applications 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), private networks and VPN (71 percent of respondents), public cloud-based applications and services (56 percent of respondents), email security (53 percent of respondents), and device authentication (51 percent of respondents).

APPLICATIONS THAT MOST COMMONLY USE DIGITAL CERTIFICATES



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 56 percent and 40 percent of respondents, respectively.

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 a 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

The people we all rely on to make the world go round – they rely on Thales. Our customers come to us with big ambitions: to make life better, to keep us safer. Combining a unique diversity of expertise, talents and cultures, our architects design and deliver extraordinary high technology solutions. Solutions that make tomorrow possible, today. From the bottom of the oceans to the depth of space and cyberspace, we help our customers think smarter and act faster – mastering ever greater complexity and every decisive moment along the way. With 65,000 employees in 56 countries, Thales reported sales of €15.8 billion in 2017.

CLICK HERE TO READ THE FULL REPORT

OUR SPONSORS

VENAFI

GEOBRIDGE

CSA cloud security alliance

GuidePoint SECURITY

CRITICALSTART

OASIS

SAMSUNG

THALES

www.thalesesecurity.com

#2018GlobalPKI