ENTRUST
SECURING A WORLD IN MOTION

IoT, Authentication and Cloud Services Drive Staggering Increase in PKI adoption and in Certificate Volume, finds new research from Entrust

Annual PKI and IoT Trends Study finds unprecedented levels of PKI challenges, changes and uncertainty in 2020

MINNEAPOLIS – October 13, 2020 – Organizations are rapidly increasing the size, scope and scale of their data protection infrastructure, reflected in dramatic rises in adoption of public key infrastructure (PKI) across enterprises worldwide, according to new research from Entrust. PKI is at the core of nearly every IT infrastructure, enabling security for critical digital initiatives such as cloud, mobile device deployment, identities and the internet of things (IoT).

The annual 2020 Global PKI and IoT Trends Study, conducted by research firm the Ponemon Institute and sponsored by nCipher Security, an Entrust company, is based on feedback from more than 1,900 IT security professionals in 17 countries.

IoT, authentication and cloud are the top drivers in PKI adoption growth
As organizations become more dependent on digital information and face increasingly sophisticated cyberattacks, they rely on PKI to control access to data and ascertain the identities of people, systems and devices on a mass scale.

IoT is the fastest growing trend driving PKI application deployment, up 26 percent over the past five years to 47 percent in 2020, with cloud-based services the second highest driver cited by 44 percent of respondents.

PKI usage surging for cloud and authentication use cases
TLS/SSL certificates for public-facing websites and services are the most often cited use case for PKI credentials (84 percent of respondents). Public cloud-based applications saw the fastest year-over-year growth, cited by 82 percent, up 27 percent from 2019, followed by enterprise user authentication by 70 percent of respondents, an increase of 19 percent over 2019. All underscore the critical need of PKI in supporting core enterprise applications.

The average number of certificates an organization needs to manage grew 43 percent in the 2020 study over the previous year, from 39,197 to 56,192 certificates, highlighting a pivotal requirement for enterprise certificate management. The rise is likely driven by the industry transition to shorter certificate validity periods, and the sharp growth in cloud and enterprise user authentication use cases.

Challenges, change and uncertainty
The 2020 study found that IT security professionals are confronting new challenges to enabling applications to use PKI. More than half (52 percent) cited lack of visibility of an existing PKI's security capabilities as their top challenge, an increase of 16 percent over the 2019 study. This issue underscores the lack of cybersecurity expertise available within even the most well-resourced organizations, and the need for PKI specialists who can create custom enterprise roadmaps based on security and operational best practices. Respondents also cited inability to change legacy applications

and the inability of their existing PKIs to support new applications as critical challenges – both at 51 percent.

When it comes to deploying and managing a PKI, IT security professionals are most challenged by organizational issues such as no clear ownership, insufficient skills and insufficient resources. PKI deployment figures from the study clearly indicate a trend toward more diversified approaches, with as-a-service offerings even becoming more prevalent than on-premise offerings in some countries.

The two greatest areas of PKI change and uncertainty come from new applications such as IoT (52 percent of respondents) and external mandates and standards (49 percent). The regulatory environment is also increasingly driving deployment of applications that use PKI, cited by 24 percent of respondents.

Security practices have not kept pace with growth
In the next two years, a forecasted average of 41 percent of IoT devices will rely primarily on digital certificates for identification and authentication. Encryption for IoT devices, platforms and data repositories, while growing, is at just 33 percent – a potential exposure point for sensitive data. Respondents cited several threats to IoT security, including altering the function of IoT devices through malware or other attacks (68 percent) and remote control of a device by an unauthorized user (54 percent). However, respondents rated controls relevant to malware protection – like securely delivering patches and updates to IoT devices – last on a list of the five most important IoT security capabilities.

The US National Institute of Standards and Technology (NIST) recommends that cryptographic modules for certificate authorities (CAs), key recovery servers and OCSP responders should be validated to FIPS 140-2 level 3 or higher. Thirty-nine percent of respondents in this study use hardware security modules (HSMs) to secure their PKIs, most often to manage the private keys for their root, issuing, or policy CAs. Yet only 12 percent of respondents indicate the use of HSMs in their OSCP installations, demonstrating a significant gap between best practices and observed practices.

“PKI underpins the security of both the business and the consumer world, from digitally signing transactions and applications to prove the source as well as integrity, to supporting the authentication of smart phones, games consoles, citizen passports, mass transit ticketing and mobile banking, says Larry Ponemon, founder of the Ponemon Institute. “The 2020 Global PKI and IoT Trends Study shows a surge in the use of PKI credentials for cloud-based applications and enterprise user authentication, underscoring the criticality of PKI in supporting core enterprise applications.”

“We are seeing increasing reliance on PKI juxtaposed with struggles by internal teams to adapt it to new market needs -- driving changes to traditional PKI deployment models and methods,” says John Grimm, vice president strategy for digital solutions at Entrust. “In newer areas like IoT, enterprises are clearly failing to prioritize security mechanisms like firmware signing that would counter the most urgent threats, such as malware. And with the massive increase in certificates issued and acquired found in this year’s study, the importance of automated certificate management, a flexible PKI deployment approach, and strong best practice-based security including HSMs has never been greater.”

Download your copy of the new [2020 Global PKI and IoT Trends Study]

ENTRUST

SECURING A WORLD IN MOTION

2020 Global PKI and IoT Trends Study methodology

The 2020 Global PKI and IoT Trends Study captures the current state of PKI maturity, PKI challenges and the influence of the IoT on PKI trends. The report summarizes the fifth annual results of a survey completed by 1,934 IT security practitioners in the following 17 countries/regions: Australia, Brazil, France, Germany, Hong Kong, India, Japan, Mexico, Middle East (Saudi Arabia and the United Arab Emirates), Netherlands, Russian Federation, South Korea, Southeast Asia (Indonesia, Malaysia, Philippines, Thailand, and Vietnam), Sweden, Taiwan, United Kingdom, and the United States.

The 2020 study is the fifth annual report on global PKI and IoT trends, sponsored by nCipher Security, an Entrust company, and 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.

About Entrust

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. To learn more visit www.entrust.com.

###

For more information please contact:

Liz Harris liz.harris@ncipher.com +44 7973 903648
Ken Kadet ken.kadet@entrust.com +1 952-988-1154