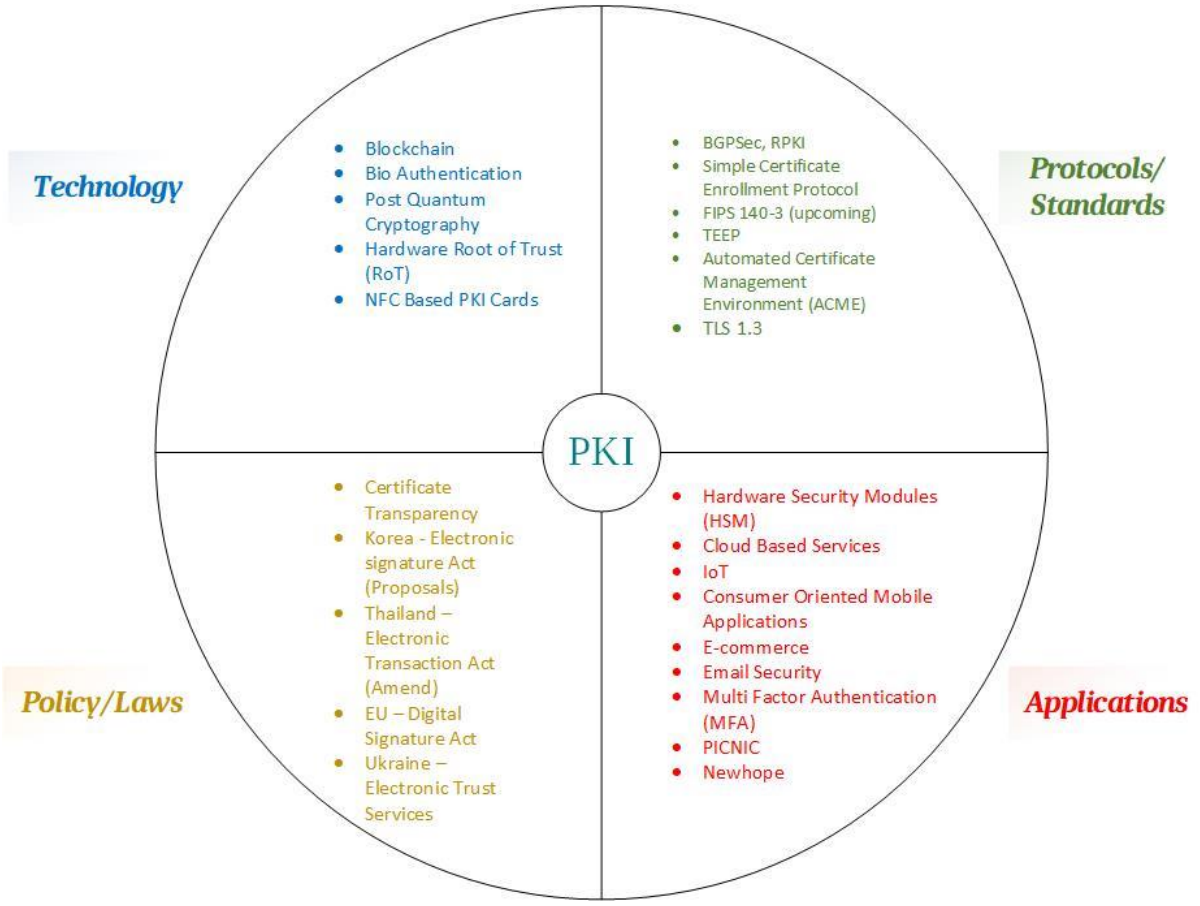
PKI Barometer 2018



This year's PKI Barometer 2018, captures the developments happening in the PKI's 4 core segments namely: Technology, Protocols & Standards, Applications and Policy & Laws.

PKI is gaining new grounds in IoT and Cloud Computing. This is evident in the market studies, wherein the Global Public Key Infrastructure (PKI) market was valued at USD 689.1 million in 2017 and is now estimated to reach **USD 1.98 billion by 2023** with an annual compounded growth rate of 21.12%.

Source: https://www.marketresearchfuture.com/reports/public-key-infrastructure-market-3627

Technology

Blockchain

PKI is the undisputed technology for trust. The emergence of Blockchain as a distributed trust model, and as a technology for providing strong integrity (immutability) and resilience (distributed nodes) is ushering in a revolution in various domains. PKI can leverage Blockchain in its various workflows to strengthen the immutability – including certificate issuance and their recordings in Certificate Transparency Logs.

Bio authentication

Bio authentication, or biometric authentication, is a method of authentication (proving you are who you say you are) based on something biological to the human being. Biometric authentication is another form of multi-factor authentication (providing several separate pieces of evidence proving who you are), and can be used in conjunction with another form of authentication, such as a password.

Post Quantum Cryptography

Post-quantum cryptography (sometimes referred to as quantum-proof, quantum-safe or quantum-resistant) refers to cryptographic algorithms (usually public-key algorithms) that are thought to be secure against an attack by a quantum computer. As of 2018, this is not true for the most popular public-key algorithms, which can be efficiently broken by a sufficiently strong ***hypothetical*** quantum computer. The problem with currently popular algorithms is that their security relies on one of three hard mathematical problems: the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem. All of these problems can be easily solved on a

sufficiently powerful quantum computer running **Shor's algorithm**. Even though current, publicly known, experimental quantum computers lack processing power to break any real cryptographic algorithm, many cryptographers are designing new algorithms to prepare for a time when quantum computing becomes a threat.

In contrast to the threat quantum computing poses to current public-key algorithms, most current symmetric cryptographic algorithms and hash functions are considered relatively secure against attacks by quantum computers. While the quantum Grover's algorithm does speed up attacks against symmetric ciphers, doubling the key size can effectively block these attacks. Thus, post-quantum symmetric cryptography does not need to differ significantly from current symmetric cryptography.

Reference: https://en.wikipedia.org/wiki/Post-quantum_cryptography

Hardware Root of Trust (RoT)

A hardware Root of Trust can be defined by the four basic building blocks:

• The protective hardware provides a trusted execution environment (TEE) for the privilege software to run.

• At a minimum, it must perform one or more proven cryptographic functions like AES based.

• A form of tamper protection must be present and available for the entire runtime.

• A flexible, yet simple user interface that the host can interact with, through either the host CPU and/or a host controller

Reference: https://www.synopsys.com/designware-ip/technical-bulletin/understanding-hardware-roots-of-trust-2017q4.html

NFC based PKI Cards

Estonia, known for using PKI based ID cards for its citizens had updated its cards for use in the contactless NFC environments.

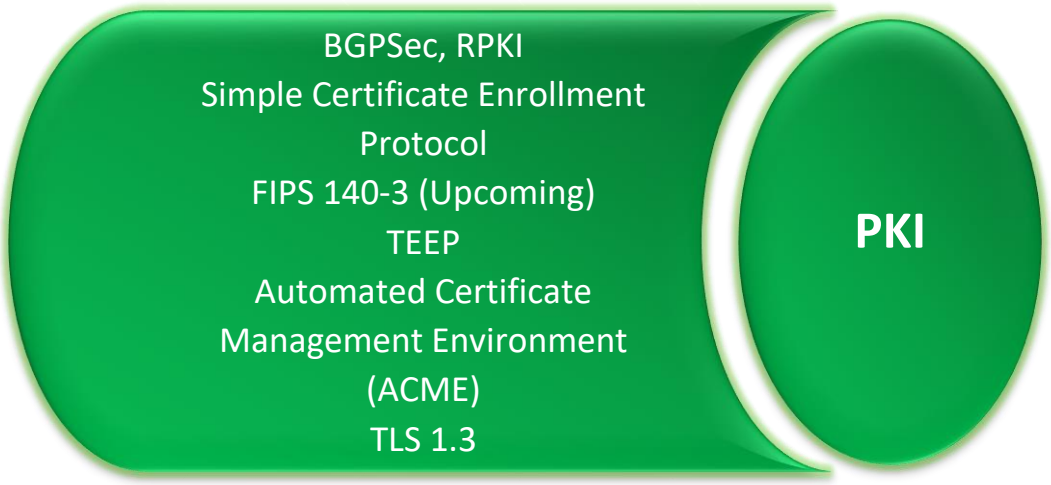
Reference: https://www.securerf.com/securerf-announces-lime-tag-nx01/

Lightweight Public Key Infrastructure (LPKI)

Lightweight Public Key Infrastructure (LPKI) is introduced that is so suitable for the resource-constrained platforms, and for applications such as mobile commerce. It is based on the elliptic curve cryptography, deploys sign cryption, assigns only one pair of private-public keys to each subscriber, delegates all the validations to a TTP called Validation Authority (VA). It has a compact compatibility with the well tried PKIX infrastructure since its certificates have the same format of the popular X.509v3 certificates. However, this does not cause any problem since all the validations are delegated to the VA.

Reference: http://aircconline.com/ijcnc/V10N2/10218cnc07.pdf

Protocols & Standards



BGPSec

BGPsec, an extension to the Border Gateway Protocol (BGP) that provides security for the path of Autonomous Systems (ASes) through which a BGP UPDATE message passes. BGPsec is implemented via an optional non-transitive BGP path attribute that carries digital signatures produced by each AS that propagates the UPDATE message. The digital signatures provide confidence that every AS on the path of ASes listed in the UPDATE message has explicitly authorized the advertisement of the route.

Reference: https://tools.ietf.org/html/rfc8205

RPKI

Resource Public Key Infrastructure (RPKI) is a public key infrastructure framework designed to secure the Internet's routing infrastructure, specifically the Border Gateway Protocol. RPKI provides a way to connect Internet number resource information (such as IP Addresses) to a trust anchor. Using RPKI, legitimate holders of number resources are able to control the operation of Internet routing protocols to prevent route hijacking and other attacks.

Reference: https://www.apnic.net/get-ip/faqs/rpki/

FIPS 140-3

On March 22, 2019, the Secretary of Commerce approved Federal Information Processing Standards Publication (FIPS) 140-3, Security Requirements for Cryptographic Modules, which supersedes FIPS 140-2. This was announced in the Federal Register on May 1, 2019.

FIPS 140-3 aligns with ISO/IEC 19790:2012(E) and includes modifications of the Annexes that are allowed to the Cryptographic Module Validation Program (CMVP), as a validation authority. The testing for these requirements will be in accordance with ISO/IEC 24759:2017(E), with the modifications, additions or deletions of vendor evidence and testing allowed as a validation authority under paragraph 5.2. Major changes in FIPS 140-3 are limited to the introduction of non-invasive physical requirements.

Reference: https://csrc.nist.gov/Projects/FIPS-140-3-Development

Automated Certificate Management Environment

The Automatic Certificate Management Environment (ACME) protocol is a communications protocol for automating interactions between certificate authorities and their users' web servers, allowing the automated deployment of public key infrastructure

at very low cost. It was designed by the Internet Security Research Group (ISRG) for their Let's Encrypt service.

Public Key Infrastructure using X.509 (PKIX) certificates are used for a number of purposes, the most significant of which is the authentication of domain names. Thus, certification authorities (CAs) in the Web PKI are trusted to verify that an applicant for a certificate legitimately represents the domain name(s) in the certificate. The proposed ACME Internet draft describes a protocol that a CA and an applicant can use to automate the process of verification and certificate issuance. The protocol also provides facilities for other certificate management functions, such as certificate revocation.

Reference: https://ietf-wg-acme.github.io/acme/draft-ietf-acme-acme.html

TLS 1.3

Transport Layer Security (TLS) 1.3 protocol provides unparalleled privacy and performance compared to previous versions of TLS and non-secure HTTP. Working with the IETF, Cloudflare engineers have been active contributors to the development of the latest TLS protocol.

A core tenet of TLS 1.3 is simplicity. In the new version, all key exchange algorithms, except the Diffie-Hellman (DH) key exchange, were removed. TLS 1.3 has also defined a set of tried and tested DH parameters, eliminating the need to negotiate parameters with the server.

What's more, TLS 1.3 no longer supports unnecessary or vulnerable ciphers, such as CBC-mode and the RC4 cipher. These ciphers are known to be susceptible to attacks, but were still supported in most TLS implementations for legacy compatibility. Fortunately, the recent rush of downgrade attacks affecting early TLS versions motivated IETF to entirely remove such ciphers from TLS 1.3.

In addition, TLS 1.3 requires servers to cryptographically sign the entire handshake, including the cipher negotiation, which prevents attackers from modifying any handshake parameters. This means that TLS 1.3 is architecturally impervious to the downgrade attacks that affected earlier TLS versions.

Finally, the signatures themselves were also improved by implementing a new standard, called RSA-PSS. RSA-PSS signatures are immune to cryptographic attacks affecting the signature schemes employed in earlier TLS versions.

Reference: https://kinsta.com/blog/tls-1-3/

Reference: https://www.cloudflare.com/learning-resources/tls-1-3/

Policy & Laws

Certificate Transparency

Initially started as an experimental Internet Security Standard, invented by Ben Laurie and Adam Langley at Google, the system has become a de-facto standard for publishing the digital certificates issued to domains (websites) in the Certificate Transparency lists (CTL). These lists have become the trust-lists for the popular browsers including Mozilla's Firefox and Google's Chrome browsers, to name a few. More and more CA's are adopting them as the CA/B forum pushing for its adaptation.

EU Electronic Transaction Act

EU has made amendments to the Electronic Identification and Trust Services (eIDAS) for Electronic Transaction Act, wherein they have merged the technical regulatory authority and the information system authority as a single competent authority.

Reference: https://www.riigiteataja.ee/en/eli/530102013080/consolide

Korea - Electronic Signature Act

Seoul, seems to be mulling over the scrapping of the Certifying Authority (CA) and instead adopt Blockchain and Biometric authentication. CA's were under the regulatory control of NPKI (National PKI) and aims to give up the same.

Reference: https://www.itu.int/en/ITU-T/Workshops-and Seminars/bsg/201712/Documents/3.Jonghyun-Baek.pdf

Thailand – Electronic Transaction Act (Amend)

Thailand is likely to amend their Electronic Transaction Act, and Digital ID in 2019.

Reference: http://www.indiapki.org/presentation/PKI%20Development%20in%20Thailand%20-%20by%20Dr_Chaichana.pdf

Ukraine – Electronic Trust Services

Ukraine brought out the law on Electronic Trust Services this year (November 2018) for electronic identification and electronic fiduciary services. It brings out a mutual recognition of Ukrainian and foreign certificates of public keys and electronic signatures. Their electronic identification would be in accordance with European requirements and Standards.

One of the interesting methods of electronic identity and verification methods include MobileID, wherein identification certificates would be embedded in the SIM cards.

Reference: http://zakon.rada.gov.ua/laws/show/2155-19

Applications

Hardware Security Modules (HSM)

HSMs offer a certified and tamper-resistant environment for the cryptographic aspects of business processes like encryption and digital signing. The use cases of HSMs have been increasing and getting diversified. It has been noted that HSMs are increasingly being used for database encryption (36%), PKI (29%), and now newly joined by public cloud encryption (32%) and payment credential provisioning (30%). HSMs use reached an all-time high this year, with specific use cases of application level encryption (48%) and TLS/SSL (45%) topping the charts. The use of HSM's for code signing, big data encryption and IoT (Internet of Things) root of trust all jumped with double-digit growth.

Reference:https://www.ncipher.com/blog/global-encryption-trends-study-2019-biggest-year-yet

Cloud Based Services

PKI is increasingly being offered as a SaaS (Software as a Service) service to the enterprises, commonly referred as Managed PKI. These services are offered to enterprises either to have their private PKI or a dedicated CA managing their trust and identity services in their cloud.

Internet of Things (IoT)

The need for trust and security in IoT environment is well evident and PKI remains as the only reliable solution. From the stages of production to deployment, there is a possibility of compromise of the device at every stage. (for example the device could be embedded with a rogue software, are during operations could be controlled by a malicious bot or hacker).

The dangers of a compromised single IoT device can even bring down a huge network, owing to the cascading effects. Therefore it is necessary and essential to protect all IoT devices. The practical challenge of using PKI to safeguard IoT devices, is that there are many machines in industry that were never designed to be networked. However the good news is that the end IoT devices are getting smarter with the new-age processors and PKI could soon find its way to them.

Multi Factor Authentication (MFA)

Multifactor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

Multifactor authentication combines two or more independent credentials: what the user knows (password), what the user has (security token) and what the user is (biometric verification). The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

Reference: https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA

PICNIC

"Picnic" is the code name for a post-quantum digital signature algorithm. Picnic is developed in collaboration with researchers and engineers from Aarhus University, AIT Austrian Institute of Technology GmbH, Graz University of Technology, Microsoft Research, Princeton University, and the Technical University of Denmark.

Unlike most other public-key cryptography, Picnic isn't based on hard problems from number theory. Instead, it uses what is called a zero-knowledge proof – where Alice can convince Bob that she knows a secret, without disclosing the secret itself. Picnic uses this concept together with symmetric cryptography, hash functions, and block ciphers, to create a unique signature scheme. The hard problems Picnic relies on for security relate only to hash functions and block ciphers, that are thought to be secure against quantum attacks.

Reference: https://www.microsoft.com/en-us/research/project/picnic/

NewHope

NewHope is a key-exchange protocol based on the Ring-Learning-with-Errors (Ring-LWE) problem, which was submitted to the NIST post-quantum crypto project. The submission proposes four different instantiations:

NewHope512-CPA-KEM and NewHope1024-CPA-KEM, which are IND-CPA-secure key encapsulation mechanisms which target level 1 and level 5, respectively, in the NIST call for proposals (matching or exceeding the brute-force security of AES-128 and AES-256, respectively)

NewHope512-CCA-KEM and NewHope1024-CCA-KEM, which are IND-CCA-secure key encapsulation mechanisms which target level 1 and level 5, respectively, in the NIST call for proposals (matching or exceeding the brute-force security of AES-128 and AES-256, respectively)

Reference: https://newhopecrypto.org/