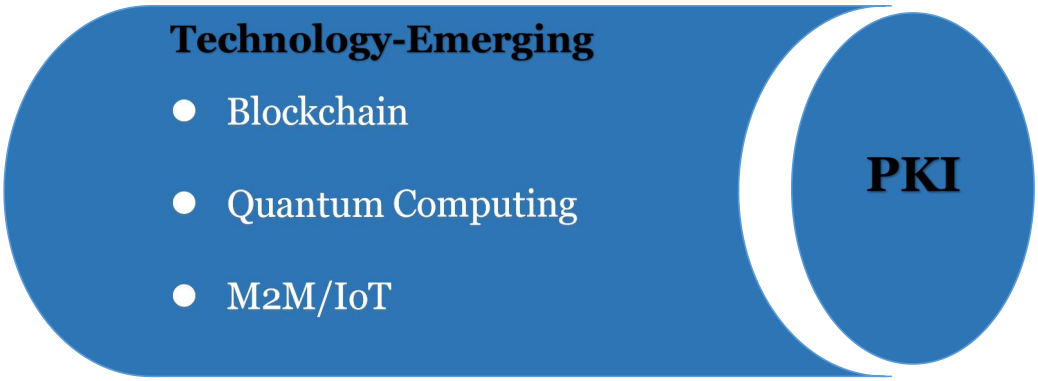
PKI BAROMETER 2019



PKI in Blockchain

Blockchain is a distributed database of transactions (ledger) that maintains a growing list of records (blocks). Each entry in the list is linked to a previous entry (blockchain). This results in a so-called hash-tree or hash-calendar. As a rule, the list is distributed and publicly visible, i.e. neither confidential nor centralized. But when it comes to PKI, the basic set up will stay the same. That is, a certificate authority (CA) will issue and manage the certificates needed for the trusted digital identities that are required to implement strong authentication, data encryption and digital signatures.

Anyone on a public Blockchain can read all of its contents. This feature eliminates the potential problems stemming from relying on a third party's actions. Everything that happens on a Blockchain is available to anyone using it. So if a CA inadvertently issues keys in someone else's name, that information is seen by everyone on the chain.

Information is time stamped, and a record is created each time an update occurs. Consequently, it is clear who did what when. Altering the source code becomes impossible. A hacker needs to change every entries in the Blockchain rather than just one record. Also, the metadata in its database is read only, which means that it is impossible to manipulate independently. The solution protects information in a secure distributed fashion and is more in tune with current needs than traditional PKI systems.

According to nexus-group study [1] *"instead of running a CA software on a computer, which requires backups, maintenance, etcetera, the CA will be run*

on a blockchain instead. When the single computer is replaced by a group of connected computers and when the code is accessible to anyone, PKI will be even more robust and trustworthy".

Building PKIs using blockchain removes the potential points-of-failure created by the use of CAs which, if subverted, can compromise entire certificate chains. Furthermore, blockchain-based PKI, as a public append-only log, provides the certificate transparency (CT) property implemented by Google to improve CA-based PKI security through public logging and monitoring of certificates.

PKI in Quantum Computing

Quantum computing is about processing information stored in individual atoms, electrons, ions and photons.Quantum computing uses quantum bits called Qubits which can exist in a super state with zeros and ones occurring together. This is a phenomenon called the superposition of states. In this state, a quantum computer can carry our parallel processing at a faster rate than our current processors.

According to report published on February 12, 2019;DigiCert, Inc., the world's leading provider of TLS/SSL, IoT and PKI solutions; Utimaco, one of the world's top three Hardware Security Module providers; and Microsoft Research, a leader in quantum-safe cryptography, announced *a successful test implementation of the "Picnic" algorithm, with digital certificates used to encrypt, authenticate and provide integrity for connected devices commonly referred to as the Internet of Things (IoT)*. This proof of concept provides a path toward a full solution, currently in development, that will protect IoT devices from future threats quantum computing could pose to today's widely used cryptographic algorithms.

Currently, most of the IoT devices use RSA and ECC to protect confidentiality, integrity and authenticity for device identities and communication. Experts from the security community from Microsoft Research, predict that large-scale quantum computers capable of breaking RSA and ECC public key

cryptography will exist within the next 10 to 15 years. Although this might seem like a long time away, many devices such as connected cars, smart homes, connected cities, connected medical devices and other critical infrastructures will either live longer than this or will take longer to update.

STRATEGIES FOR PROTECTING PKIS

- Replace PKI by a central key infrastructure that only works symmetrically
- Find a new, asymmetric algorithm that is quantum-proof.

Currently, there are so far four hopeful approaches:

- Hash-based cryptography
- Code-based cryptography
- Grid-based cryptography
- Cryptography based on multivariate polynomial equations
- One time Signature Algorithm

According to QSS Working Group [12] there are two significant risks in delaying a move to quantum-resistant cryptography. First, when considering information that needs to be kept confidential for many decades, there is the danger that an attacker could store off ciphertext and key establishment data that isn't protected with quantum resistant cryptography today and then break it with a quantum computer in the future. Information with a significant value well into the future should be protected against quantum computing attacks as soon as feasible. Second, there is a risk that digitally signed data may not be trustworthy in the future.If one is using a system that digitally signs data today with a non-quantum resistant digital signature, an attacker with a quantum computer in the future could change the signature or repudiate some of the information.The chain of trust would be broken,once quantum computers are able to break signatures.

QUANTUM SAFE DIGITAL SIGNATURE:

In classical public key method, the public key is created from a random, private sign key, using a one-way function. This is a function that is designed

in such a wat that computing the result is easy when the input is given , but computing the input given the result is very difficult.

A classic example is the multiplication of two very large primes: The multiplication is easy, but factoring the product without knowing the primes is normally considered infeasible.

$x \mapsto f(x)$ easy

$f(x) \mapsto x$ very difficult

Most of the requirements for a classical digital signature scheme also apply to the quantum digital signature scheme.Some propose quantum hard problems:

- Lattice based problems
- Symmetric key primitive(hash problems,block cipher)
- Multi-Variate polynomial problems
- Supersingular isogeny Deiffie-Hellman(SIDH)
- Code based problems

According to NIST PQC Standardization Process: The 17 Second-Round Candidate public-key encryption and key-establishment algorithms are:

- BIKE
- Round5
- NTRU Prime
- LED
- CRYSTALS-KYBER
- SIKE
- Acrypt
- NewHope
- HQC
- GeMSS
- Rainbow
- RQC
- NTS-KEM
- Classic McEliece
- FALCON
- SPHINCS+
- LUOV
- NTRU
- ROLLO
- SABER
- Picnic
- CRYSTALS-DILITHIUM
- Frodo
- Three Bears
- MQDSS
- KEM
- LAC
- qTESLA

Fig 1. NIST PQC Second Round Candidates

Picnic: A Family of Post-Quantum Secure Digital Signature Algorithms[14]

The Picnic family of digital signature algorithms is designed to provide security against attacks by quantum computers, in addition to attacks by classical computers. The building blocks are a zero-knowledge proof system (with post-quantum security), and symmetric key primitives like hash functions and block ciphers, with well-understood post-quantum security. Picnic does not require number-theoretic, or structured hardness assumptions.

- Picnic is new digital signature scheme based on symmetric-key algorithms
- Picnic is developed in collaboration with researchers and engineers from Aarhus University, AIT Austrian Institute of Technology GmbH, DFINITY, Graz University of Technology, Georgia Tech, Microsoft Research, Northwestern University, Princeton University, the Technical University of Denmark, and the University of Maryland.
- Submitted to NIST's project
- Currently Selected in 3rd Round of NIST 2020
- Built completely differently from hash-based signatures
- New design: a lot of room for optimizations
- 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.

According to NIST Second PQC Standardization Conference August 2019 Report[15] Compared to Round 1 changes in the PICNIC now the algorithm offers additional flexibility shorter signature are now an option with Picnic2.

QUANTUM SAFE DIGITAL SIGNATURE:

Those digital signature which are strong enough to resist the quantum attack are called as quantum safe digital signature.However it's not a easy way to make any digital signature quantum proof ,there is complex underlying math required in designing.

Just like classical digital signatures, quantum digital signatures make use of asymmetric keys. Thus, a person who wants to sign a message creates one or more pairs of sign and corresponding public keys.

In general we can divide quantum digital signature schemes into two groups:

- A scheme that creates a public quantum-bit key out of a private classical bit string.
- A scheme that creates a public quantum-bit key out of a private quantum bit string.

ISARA[19] is a security solutions company specializing in quantum-safe cryptography.The ISARA Catalyst Agile Digital Certificate Technology is a technique for creating an enhanced X.509 digital certificate that simultaneously contains two sets of cryptographic subject public keys and issuer signatures while maintaining full backward compatibility with current X.509 formats. It's integrated by developers who create and manage identity and access management systems serving enterprise and government.

Key advantages are:

- Gradual migration
- Eliminate duplication and management of multiple public key infrastructure (PKI)
- Protect using the cryptographic algorithms you need to use, faster
- Transparency to end-users

PKI in Internet of Things (IoT) / Machine to Machine (M2M) Interaction

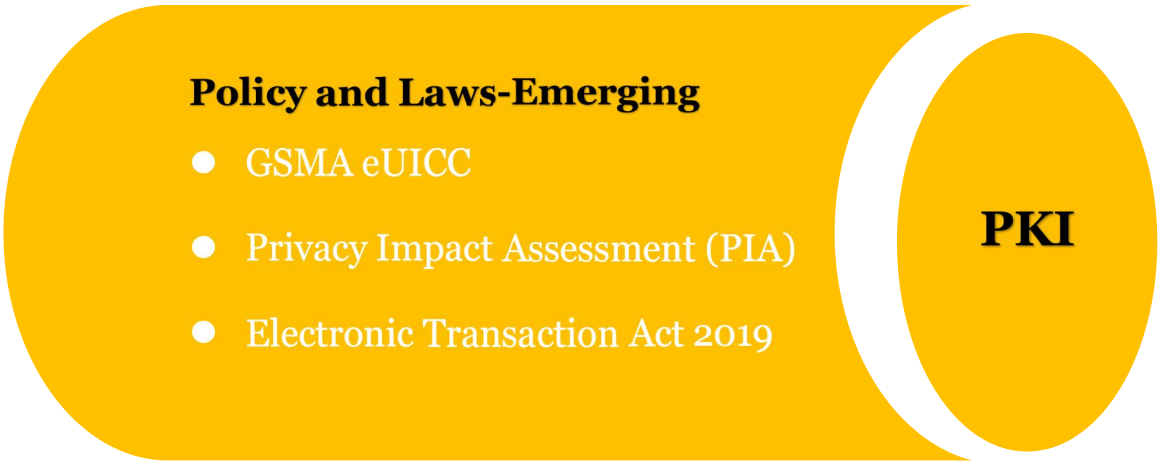
PKI can build and support security and trust in IoT ecosystems. PKI's role in IoT provides strong identity authentication and creates the foundation of trust that systems, devices, applications, and users need to safely interact and exchange sensitive data.

According to report from nCipher[10], an average of 42 percent of IoT devices in use will primarily rely on digital certificates for identification and authentication, in the next two years.

Most important pki capabilities for IoT

- Scalability to millions of managed certificates
- Online revocation
- Support for Elliptic Curve Cryptography (ECC)
- FIPS 140-2 Level 3 HSMs (Hardware Security Modules) for Root and Issuing CAs
- Cloud deployment model
- Ability to sign firmware for IoT devices

For active technology trend in PKI you can refer to our previous year barometer i.e PKI Barometer 2018



GSMA eUICC Version 2.0 18 Septemeber 2019

According toGSMA eUICC PKI Certificate Policy[13] The ability to provision operator subscription data securely "over the air" to change from one operator to another requires secure connections, as well as data confidentiality and integrity, and system

availability. Paramount to the achievement of these objectives is the establishment and maintenance of an efficient and effective end-to-end trust infrastructure within the ecosystem. For the eUICC and Servers defined by GSMA for remote provisioning an eUICC Public Key Infrastructure (PKI) to support the use of Certificate for authentication has been defined.

Mobile Network Operators relying on the eUICC PKI need to be able to determine the degree of trust which can be placed in the authenticity and integrity of the Certificates issued by a Certificate Authority(CA).

UICC (Universal Integrated Circuit Card) is the hardware used in mobile devices that contains SIM and/or USIM applications enabling access to GSM, UMTS/3G and LTE networks. **Embedded UICC** (also known as eSIM) is a UICC that supports "over the air" provisioning of an initial operator subscription and the subsequent change of subscription from one operator to another in accordance with GSMA specifications.

Introducing eUICC PKI gives advantages to mobile operators such as,

- No need to spend money and time conducting individual audits
- Audits are conducted by highly-qualified individuals at no cost to the operator
- The scheme sets a rigorous security standard requiring a high-level of supplier commitment
- Offers peace of mind that suppliers have implemented appropriate security measures

Privacy Impact Assessments (PIAs)

Privacy Impact Assessments (PIAs) providse a method of identifying privacy risks so that these can be highlighted and addressed when PKI systems or PKI-supported business applications are being designed, implemented, revised or extended. A PIA may be part of a larger risk assessment and management procedure.Properly done, this assessment will include an

understanding of which parties will bear what risks. Agencies that are Gatekeeper accredited may have substantially met this requirement by conducting a risk assessment process regarding privacy as part of the Gatekeeper accreditation process.A PIA may also play an important role in the formulation of the Agency's security awareness campaign, as it can identify issues that can directly affect clients and highlight areas of particular privacy sensitivity.Certain countries has implemented the PIA in their PKI ecoystem.

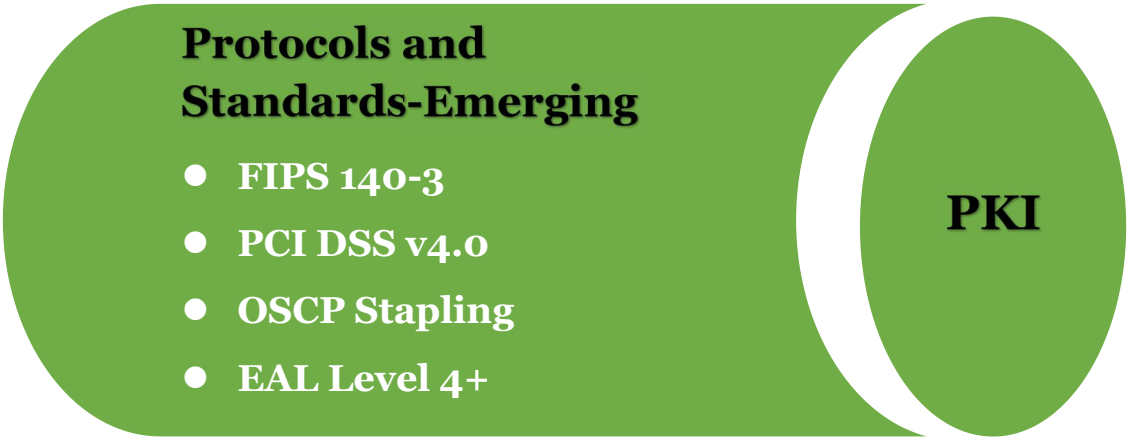
Electronic Transaction Act(ETA)

In Thailand Electronic Transaction Act[17],was promulgated into law in 2019 with the aim of mitigating hindrances to the country's ability to facilitate electronic transactions and aligning Thailand's digital regulations with the United Nations Convention on the Use of Electronic Communications in International Contracts. The Amendments brings about greater flexibility for conducting electronic transactions as the Act.

Electronic Transactions Act (3rd and 4th amendments) B.E.2562 (2019)

Aiming to be the business hub of Southeast Asia, Thailand has been trying to cope with the world of technologies for decades. In 2001 (B.E. 2544), the Electronic Transactions Act (ETA) was introduced but despite the flexibility of the provisions therein, actual usage and adaptation of electronic transactions by the public sector has been scarce until recent years[18].

For active trend in policy and laws in PKI you can refer to our previous year barometer i.e PKI Barometer 2018



FIPS 140-3 Security Standard

According to NIST Update [4] following are the important updates regarding FIPS140-3.

- FIPS 140-3 becomes effective on September 22, 2019.
- FIPS 140-3 testing, through the Cryptographic Module Validation Program (CMVP), will begin September 22, 2020; and
- FIPS 140-2 testing will continue for at least a year after FIPS 140-3 testing begins.

FIPS 140-3 introduces a fifth interface, called the control output interface. A control output interface is used for the output of commands. Signals and control data are used to control or indicate the state of operation. This control output may be information that is sent to another cryptographic module. The power interface is also an interface required on all but the software modules.

Security Level 4 provides the highest level of security. At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate deletion of all plaintext CSPs.

FIPS 140-3 includes references to two existing international standards :

- International Organization for Standardization/International Electro technical Commission (ISO/IEC) 19790:2012(E) Information technology — Security techniques — Security requirements for cryptographic modules; and
- ISO/IEC 24759:2017(E) Information technology — Security techniques — Test requirements for cryptographic modules.

Payment Card Industry (PCI) Data Security Standards (DSS):

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard to prevent credit card scams and numerous additional security threats & vulnerabilities.

PKI can address some requirements of PCI DSS and can also provide design/security recommendations with regards to the workflows and processes of key management.

Goals for PCI DSS v4.0

The PCI DSS v4.0 draft provided for RFC in 2019 included proposed new requirements and changes to existing requirements. The intent of these updates was to address evolving risks and threats to payment data, improve flexibility for stakeholders, and to reinforce security as a continuous process.

According to the study [5], the 12 core PCI DSS requirements are not expected to fundamentally change with PCI DSS v4.0, as these are still the critical foundation for securing payment card data. However, based on feedback received, PCI SSC is evaluating how to evolve the standard to accommodate changes in technology, risk mitigation techniques, and the threat landscape. PCI SSC is also looking at ways to introduce greater flexibility to support organizations using a broad range of controls and methods to meet security objectives.

Key high-level goals for PCI DSS v4.0 are:

- Ensure the standard continues to meet the security needs of the payments industry
- Add flexibility and support of additional methodologies to achieve security
- Promote security as a continuous process
- Enhance validation methods and procedures.

Compliance levels

All companies who are subject to PCI DSS standards must be PCI compliant. There are four levels of PCI Compliance and these are based on how much you process per year, as well as other details about the level of risk assessed by payment brands.

At a high level, the levels are following:

- Level 1 – Over 6 million transactions annually
- Level 2 – Between 1 and 6 million transactions annually
- Level 3 – Between 20,000 and 1 million transactions annually
- Level 4 – Less than 20,000 transactions annually

The recent Version of PCI DSS is 3.2.1 which was released in May 2018 [5].

PKI for EMV cards compliant to PCI DSS

PCI DSS describes the requirements about cryptographic mechanisms as "Strong Cryptography" for all the key and certificate management. With respect to PKI, the recommendation for the use of PKI can be enlisted as:

- **The standard for Digital Certificates:** PKI setup must issue the digital certificates according to the RFC 5280. The standard currently in use by all well-known corporations for digital certificates is X.509 Version 3.
- **The standard for CRL:** PKI setup must issue the CRL according to the RFC 5280. The standard currently in use by all well-known corporations for CRL is X.509 Version 2. Revocations in case of EMV cards are very

important because millions of EMV cards are being used at national/international level by state departments, corporate organizations, and banks. Hence the revocation rate is very high.

- **Generation & Size of Public/Private Keys:** The RSA/ECC public and private keys should be generated securely and should be equal to or higher than 2048/224-bits respectively.KI for EMV cards compliant to PCI DSS.

Online Certification Revocation Protocol (OCSP) and OCSP Must-Stapling

One of the most important aspects in the design of a public key infrastructure (PKI) is certificate revocation or, more specifically, automated revocation checking. Certificate revocation ensures that the PKI system adds a certificate's serial number to a blacklist, called the certificate revocation list (CRL), when a PKI user's private key is compromised. Certificate revocation also guarantees that the PKI system efficiently distributes the revocation information to all PKI clients and PKI-enabled applications.

Not all PKI-enabled applications automatically perform revocation checking. Also, revocation checking is sometimes dependent on an application-specific configuration setting

An alternative to using CRLs is the certificate validation protocol known as Online Certificate Status Protocol (OCSP). OCSP has the primary benefit of requiring less network bandwidth, enabling real-time and near real-time status checks for high volume or high-value operations.

According to 2019 Global PKI and IoT Trends Study, by nCipher[10] OCSP continues to be the way for checking the status of the certificates followed by the CRL (Certificate Revocation List). However according to nCipher there is reduction in Automated CRL from 2018 to 2019 by 3%, while OCSP increased to 1% in the same duration.

OCSP Stapling

OCSP, however, has multiple issues; first, because clients depend on the OCSP response, the OCSP responders need to provide responses with low latency and high availability; second, the CAs can observe users' browsing behaviour by monitoring incoming OCSP requests from the clients.

OCSP Stapling was introduced to address these two problems. The web server obtains an OCSP response ahead of time from the CA and then it provides the certificate, along with this stapled OCSP response, to the client during the TLS handshake. As a result, the client receives both the certificate with its OCSP response at the same time without any additional requests to the CA.

The main disadvantages of OCSP Stapling are:

- Only supported in TLS 1.2

  TLS 1.3 removes obsolete and vulnerable features from TLS 1.2, including SHA-1, RC4, DES, 3DES, AES-CBC, MD5, and more

- Not supported by many browsers. This results in either the OCSP validity method not being used or standard OCSP being used instead.

OCSP Must-Staple

OCSP Must-Staple aims to solve the problem of soft-failure: it is an X.509 certificate extension, which tells a client to expect an OCSP response to be provided (stapled) by the web server whenever it sees the extension in the certificate. If the extension is included in the certificate, it acts as an explicit signal to the client that it must hard-fail if the server does not provide a fresh, valid OCSP response in the TLS handshake.

According to APNIC Report 2019 [3] It is observed that:

- 36.8% of OCSP responders experienced at least one outage, which typically lasted a few hours.
- All major browsers other than Firefox do not bother to ensure that stapled OCSP responses are actually included (stapled).
- Neither the Apache nor Nginx web servers prefetch an OCSP response.

Therefore OCSP Must-Staple responses, can operate optimally, only if each of the above issues are addressed.

Common Criteria Evaluation Assurance Levels (EAL) Level 4+

nCipher[10] says in its report *"Common Criteria EAL Level 4+ is the most important security certification when deploying PKI infrastructure and PKI-based applications."*

The functional and assurance security requirements are the basis for the Common Criteria. There are seven Evaluation Assurance Levels (EALs). The higher the level, the more confidence you can have that the security functional requirements have been met. The Evaluation Assurance Level (EAL1 through EAL7) of an IT product or system is a numerical grade assigned following the completion of a Common Criteria security evaluation, an international standard in effect since 1999.

The levels are as follows:

- **EAL1: Functionally Tested**.
- **EAL2: Structurally Tested.**
- **EAL3: Methodically Tested and Checked.**
- **EAL4: Methodically Designed, Tested, and Reviewed**. Applies when developers or users require moderate to high independently assured security in conventional commodity products and are prepared to incur additional security-specific engineering costs.

For active protocols and standards in PKI you can refer to our previous year barometer i.e PKI Barometer 2018

Bring Your Own Devices (BYOD) or Mobile Device Management (MDM)

Personal devices containing corporate credentials and data require strict security management to ensure trusted access. Typically, this is done with the combination of a Mobile Device Management (MDM) solution, and the strong security credentials (i.e., digital certificates) of PKI. Without digital certificates, the communications to authenticate a user and validate a device wouldn't be secure and would pose a great risk.

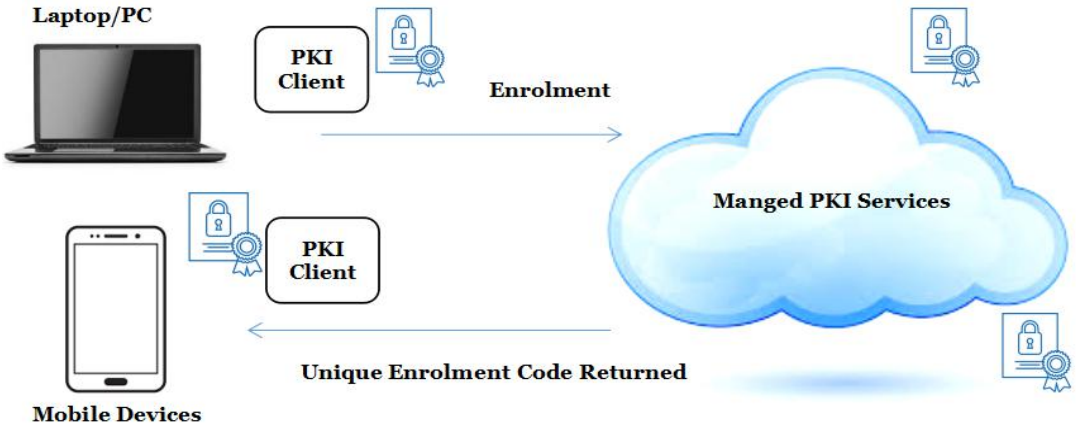


Figure 2 : BYOD PKI Services

Both consumer mobile applications as well as enterprise mobility (e.g. BYOD or Bring Your Own Device) scenarios are driving PKI usage. The challenges of mobile device management, especially from an authentication and data security perspective are often underestimated. Enterprises need a reliable

method to verify the mobile user's identity, validate the device itself, and secure the information through encryption. This is where digital certificates and PKI play a big role.

According to Study from nCipher [10], BYOD increased from 8% to 9% from 2018 to 2019.

PKI in Vehicular Communication (V2X)

Vehicle-to-Everything' also known as V2X, refers to the passing of information from a vehicle to any entity that may affect the vehicle, and vice versa. The principle of V2X communication security is based on signed messages using Public Key Certificates.

In Europe and the US, ETSI ITS and IEEE have both respectively defined PKI architectures to secure all V2V and V2I communications. For privacy protection purposes certificates have a reasonably limited validity period and need to be changed regularly.

Microsec [8] V2X PKI is a security framework for providing the safety of vehicle-to-everything communication. In such environments, public key infrastructures are used to secure the environment by verifying the participants' permissions with the usage of certificates. V2X PKI does this so with the most up-to-date cryptographic solutions, including Elliptic Curve Cryptography (ECC) which is a more secure encryption method than the widely used RSA algorithm.

V2X covers:

V2I or 'Vehicle-to-Infrastructure' which is the exchange of data between a car and equipment installed alongside roads and that is generally called a 'roadside unit' (RSU). V2I can be typically used to broadcast traffic conditions and emergency information to drivers.

V2V or 'Vehicle-to-Vehicle' relates to the transfer of data between vehicles. Compared to what sensors can provide to the vehicle, information transmitted

via V2V technology can come from cars a few hundred meters ahead or even hidden cars from behind trucks or buildings

According to a March 2019 research from market intelligence firm SNS Telecom & IT[8] *"Despite the ongoing 802.11p/DSRC versus C-V2X debate, regulatory uncertainty and other challenges, global spending on V2X communications technology is expected to grow at a CAGR of more than 170% between 2019 and 2022.*

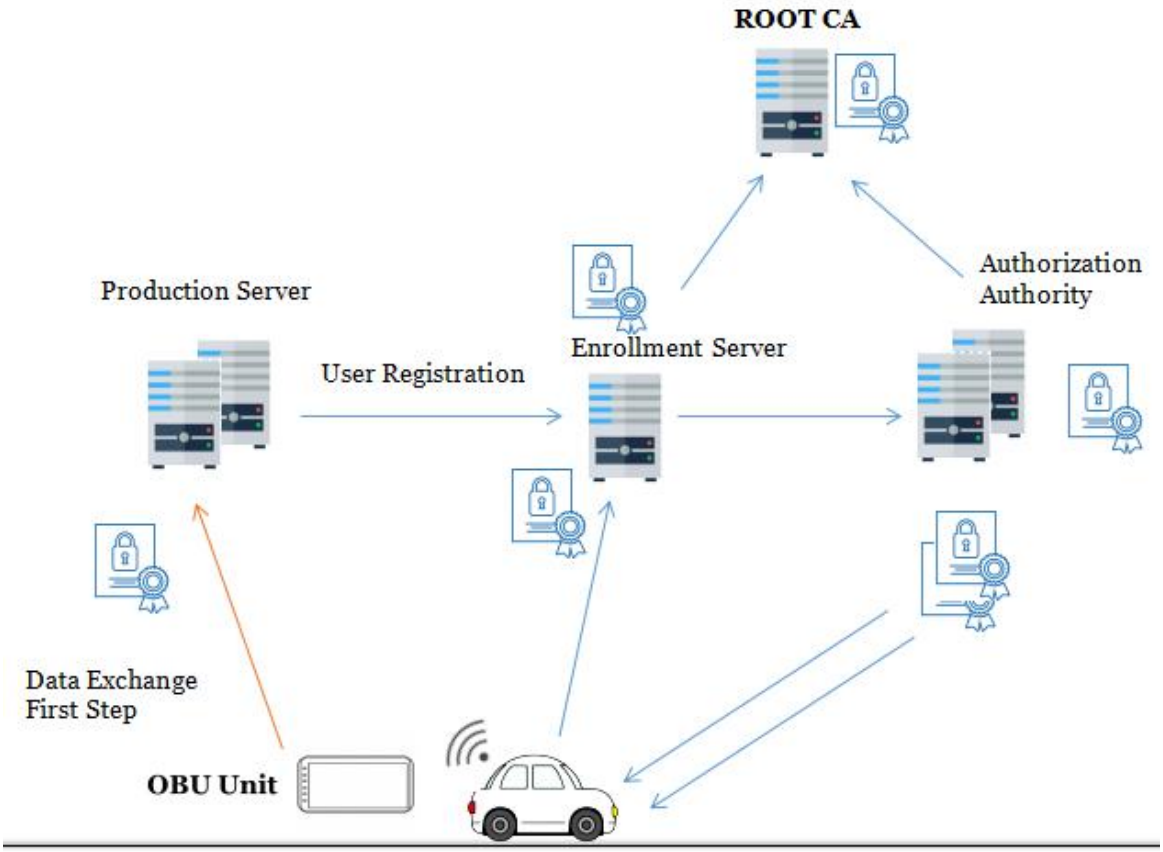


Figure 3 : Public Key Infrastructure for V2X

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.

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.

Organisations implementing on premise PKI must consider many issues, including the infrastructure, policy, implementation, routine audits etc... For instance replacing an expiring certificate with fresh one need to be done well in advance, which warrants continuous attention and separate teams to manage them.

Cloud based PKI Services are hosted externally for supplying the capabilities on demand.Therefore there is less burden on individual organisations - financial ,resources and time wise - by eliminating the need to set up any infrastructure in-house.

Only the service provider is responsible for handling the ongoing maintenance of PKI thus ensuring scalability, hassle free and efficient service.The service provider also handles all the additional requirements - installing software,hardware ,backup,disaster recovery and other infrastructure.

nCipher Study[10] shows that there is increase in deployment in PKI Services to cloud from 45% to 49% during period 2018 to 2019.

According to Study form nCipher[10] cloud based PKI services increased from 45% to 49% from 2018 to 2019. Deploying the PKI to cloud provides a rapid deployment and ease of scale are two of the advantages. There is no upfront investment in hardware, servers and software which minimizes risk and makes it is easy to get started. A cloud deployment thus enables to start small and grow with the use case.

For active applications in PKI you can refer to our previous year barometer i.e PKI Barometer 2018

Glossary

BYOD	Bring Your Own Device
CA	Certification Authority
CCA	Cross-Certification Arrangement
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
EAL	Evaluation Assurance Levels
ECC	Elliptic Curve Cryptography
FIPS	Federal Information Processing Standard Publication
GSMA	Global System for Mobile Communications
HSM	Hardware Security Module
ISO	International Standards Organisation
ITSEC	Information Technology Security Evaluation Criteria
IoT	Internet of Things
LOA	Level of Assurance
M2M	Machine to Machine
OCSP	Online Certificate Revocation Protocol
PKI	Public Key Infrastructure
PIA	Privacy Impact Assessment
RCA	Root Certificate Authority
UICC	Universal Intergrated Circuit Card

References:

1. https://www.nexusgroup.com/public-key-infrastructure-pki-blockchain-technology/
2. https://www.venafi.com/blog/blockchain-form-distributed-pki
3. https://blog.apnic.net/2019/01/15/is-the-web-ready-for-ocsp-must-staple/
4. https://csrc.nist.gov/publications/detail/fips/140/3/final
5. https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard
6. https://blog.apnic.net/2019/01/15/is-the-web-ready-for-ocsp-must-staple/
7. https://docs.broadcom.com/doc/mobile-byod-security-challenges-en
8. https://www.microsec.hu/en/v2x-pki
9. https://www.ssl247.com/kb/mpki/cloudvslocal
10. https://go.ncipher.com/rs/104-QOX-775/images/2019-Ponemon-Global-PKI-and-IoT-Trends-Study-ar.pdf
11. https://apexassembly.com/wp-content/uploads/2020/04/eBook_-_5_Reasons_to_Move_Your_PKI_to_the_Cloud.pdf
12. https://downloads.cloudsecurityalliance.org/assets/research/quantum-safe-security/State_of_PQC_web.pdf
13. https://www.gsma.com/esim/wp-content/uploads/2019/12/SGP.14-v2.0.pdf
14. https://www.cs.technion.ac.il/~biham/Workshops/Cryptoday/2018/Slides/cryptoday-2018-itai-dinur-picnic.pdf
15. https://csrc.nist.gov/CSRC/media/Presentations/picnic-round-2-presentation/images-media/picnic-zaverucha.pdf
16. https://www.digicert.com/news/pr/securing-the-future-of-iot-with-digicert-utimaco-microsoft-research/
17. https://www.bakermckenzie.com/en/insight/publications/2019/04/amendment-to-thai-electronic-transaction-act
18. https://www.southasia-law.com/news/newsdetail?news_id=27
19. https://www.isara.com/downloads/datasheets/ISARA_RadiateQSToolkit_Datasheet.pdf