Cyber Security & Public Key Infrastructure

Opening Presentation

Mumbai, India| 05-Dec-2019

V Srinivasan, Chairperson, Asia PKI Consortium

Welcome

Asia PKI Members
International Speakers
CCA Office Members
India PKI Forum Members
& Esteemed Delegates

Contents

Contents

1. Public Key Infrastructure – Origin & Evolution
2. Adoption of PKI
3. PKI usage in various countries
4. Importance of PKI
5. Acceleration by Industry bodies
6. The future

PKI: Origin & Evolution

Public key to secure communications

1. Publication of two major works in 1976-77 became a starting point.
    1. RSA Asymmetric Key Algorithm by Ron Rivest, Adi Shamir, and Leonard Adleman
    2. Diffie–Hellman key exchange by Whitfield Diffie and Martin Hellman
2. Rapidly, these works became de-facto technology for strong secure communication channel.

Public Key Infrastructure (PKI)

1. Around 1995 - 1998, evolution of internet and world wide web, created a large adoption for Netscape's protocol called "SSL" (by Taher Elgamal)
2. This uses public keys published on centralized infrastructures, along with providing information and status of those keys/certificates.
3. A PKI structure was thus created for Web users/ Websites wishing for the secure communications.

PKI: Origin & Evolution

Towards a trusted ecosystem

1. The advantage of PKI system was later adopted in several use cases, like Encrypted emails, Electronic Signatures, e-Authentication and many more.
2. With more organizations taking part, the need for standardization emerged.
3. Several countries have enacted laws and regulations to operate PKI, thus giving legal recognition as well as assuring trust to the users and applications adopting it.
4. The operating procedures are more standardized over the past decade, making it as a globally interoperable trust layer for digital transactions.

Legal backing to PKI based Security

1. UNCITRAL Model Law on e-commerce (1996) and electronic signatures (2001) gave a big boost for using PKI in electronic transactions
2. These 2 laws gave the ‘guide to enactment’ by the countries worldwide.
3. During 1998 to 2005, majority of nations passed the law for enactment of secure electronic transactions.
4. With a local law in force in each country, several government & public applications took benefit of PKI and adopted it as part of the digitization process.

Adoption of PKI

1. Over last 25 years, PKI has seen a large adoption.
2. Adoption by World Wide Web gave a huge popularity to the security quotient that PKI was adding to the electronic systems

Slow beginning

1. The first decade of PKI adoption was very slow and limited to largely websites (SSL)
2. Even though law was passed, several countries did not have strong use case, or necessary participation from industry, to adopt PKI in large scale.
3. North American enterprises as well as US Federal government implemented private PKI systems. These were relatively smaller ecosystems, and lacked interoperability.
4. But, PKI had not solved some of the problems they were expected to, and several major vendors in PKI business had gone out of business or been acquired by others.
5. Technically, using PKI was a big challenge. Users had to install specific tools and software, have Java plug-in, etc, and required non-standardized hardware.
6. The setup of infrastructure was also complicated with lack of CA hardware & software providers.

Adoption of PKI

Gaining momentum

1. Post 2006-07, PKI started gaining momentum as it slowly emerged as de-facto standard for identity backed digital mechanisms.
2. National Root CA became operational in several Asian countries, who became part of cross-border trade & shipment platform which relied on PKI backed signature.
3. Countries like India, Malaysia, China, etc rolled out PKI in Banking, Tax Filing, Company Law returns, Court Filings, etc
4. Public CAs found a business opportunity, and became successful in enabling the trusted ecosystem.

Recent drivers

1. European eIDAS implementation gave a huge leap for Identity Backed signatures. This coming as a standard from ETSI is expected to Globalize the Trust Services / PKI with simplified interoperability.
2. Mobile PKI is taking importance with Android / iPhone supporting hardware backed signatures.
3. Internet of things (IoT) requires secure communication between mutually trusted devices. PKI plays a key role in trusted devices, as well as encrypted communications.

PKI use cases in India

1. While the usage of PKI in India started with Import/Export (DGFT), over time it has extended to corporate law administration, Income Tax and GST, Tenders, Travel, Defense and several mission mode projects of Central & State governments like e-Office, e-District, Police, Smart City, etc
2. Until 2015, in India, only Digital Signatures in Crypto Tokens were used.
3. In 2015, eSign (one time use - short term certificates) were introduced into the Information Technology Act. This gave a big boost for various government and private sector use cases.
4. In the last few months, government has introduced improved versions of e-signatures, which enables public to easily sign any documents.
   - Public can easily enroll to eSign using any of their government issued IDs or even Organization IDs, and get a long term eSign account, which can be used for repeated signatures. Thanks to CCA for implementation of this.
5. With this, several use cases across various industries such as, BFSI, Health care, Education, Manufacturing, IT/ITES, Legal, etc for complete digital transformation are emerging.

PKI: Use cases in a few Countries

Malaysia:
CAs are empanelled by government based on Webtrust accreditation.
Tax Filing is the biggest use case, but now they are progressed to use for marriage certificates, educational certificates, and PKI is used in document movement across government.

Thailand:
Government (ETDA) operates the root CA.
Currently with 3 issuing CAs, and used in Customs department.
Other use cases are in early stages which revolves around Banking security, Insurance documents issuance.

Colombia:
Empanelled by Government (ONAC), based on Webtrust accreditation.
Use cases, Education Diplomas, etc

USA:
Federal PKI is operated by US Government. It empanels private CAs based on custom criteria set. But, FPKI is for government officers usage only.
US eSign Act allows other trusted CAs.
Use cases are in Real Estate documentation, Healthcare (Patient onboarding), Universities (transcript signing), contract signing, and more.

We have speakers from several countries in today's Symposium who will cover the PKI proliferation in their region.

PKI as a layered innovation

- In initial days, Business applications faced challenges in implementing PKI as it required the main system to be modified, and make hardware integration like smart cards, Crypto Tokens, etc. This not only complicated the application workflow, but also lacked user experience.
- With the advent of technologies, last few years has seen major uptake in PKI.
  - PKI has become a layer to easily fit in any existing business application.
  - The Digital Certificate function is modular and can be integrated easily in applications like ERP and CRM systems (SAP / Oracle / Salesforce / etc).
  - These are now simple APIs, standardized to be consumed with least change in user experience.

PKI as a layered innovation

- Cloud & Mobile PKI:
  - In recent days, Cloud PKI has been in demand and countries like India, Macao, etc has enabled large scale cloud signature, which enables user to sign without smart card / USB token.
  - European eIDAS regulation has also come with detailed security approaches for remote signing.
  - Additionally, Cloud Signature Consortium has published standards for such cloud signatures.
  - Mobile platform providers like Android and iOS have also brought in security in their hardware by supporting PKI based digital certificate function.

Thus, Cloud & Mobile PKI has become a reality.

Emerging Use cases

With PKI as a layer of innovation, there are multiple use cases across various industries.

- **Government**: Most of the Government to Citizen services have found successful use cases with Digital Certificates
  - Tax Filing Systems, Export / Import Systems, E-Procurement Systems, Company Law return Filing, Social Welfare Systems among various others.
- **Banking**: Several banks have introduced complete digital banking, which is enabled with PKI towards secure banking.
  - Customer On-boarding, Digital lending, Remittance, Info Updates & many more.
- **Organizational use cases**: Any organization including Private / Government have started adopting Digital Certificate based transaction:
  - Human Resources (Employment forms, agreements, etc), Finance (Purchase Order, Invoices, etc), Administration (Vendor On-boarding, Quotations, Approvals, etc), Legal department and so on.

PKI: Importance in Cyber Security

1. Public Key Infrastructure is playing a crucial role in cyber security
2. It is a de-facto standard to secure the documents with non-repudiation and authenticity
3. Securing your documents with PKI backed electronic signatures is taking the main stage across the world.
4. Data protection between trusted parties is achieved using secure encryption methodologies backed by PKI.
5. Such secure encryption techniques are widely accepted as a standard for encryption of data in transit, rest and in-use.
6. PKI is providing a trusted identity, making it easier for independent parties to perform electronic transactions that are easily trusted.
7. It has made cross border transaction, may it be in banking or trade, to go fully secure and electronic.
8. In the new age of Internet of Things (IoT), PKI has played a vital role in device identity, data encryption and integrity of the communication.

PKI: Acceleration by Industry Bodies

Several Industry Bodies are driving PKI based security practices across the Globe.

Asia PKI Consortium

PKI Adoption, Awareness, Interoperability & Mutual Recognition

CAB CA/BROWSER FORUM

Baseline requirements to operate PKI & driving the adoption of standard practices

CLOUD SIGNATURE CONSORTIUM

Remote Signing Standards enabling Cloud PKI

ETSI

Audit Criteria, Standards and Globalization of Trust Services

Webtrust

PKI Practices, Audit Criteria & Display of Trust Seals

W3C®

Standards & specifications for securing internet through world wide web

Above logos are the properties of respective owners. The usage here is for information purposes only.
Use of them does not imply any affiliation with or endorsement by them.

PKI: The Future

With the advent of PKI usage in

- Electronic signatures
- Adoption of newer algorithms like ECC
- Usage in Blockchain & IoT
- Cloud & Mobile PKI
- Short Term Certificates
- Adoption by multiple industries across the world

these are exciting times for the PKI & increased Cyber Security through PKI.

Let us listen to CCA & experts from various countries…

THANK YOU