The PKI Imperative: Securing and Connecting Asia's Digital Future

Latest Trends, Interoperability, and the Economic Dividend

Hong Kong | 6th November, 2025

Biju Varghese, Vice Chairman,
Asia PKI Consortium
Meeting: GA & SC

Welcome to all Asia PKI Consortium Members and Invited Guests To the General Assembly and Steering Committee Meeting

Agenda : Charting PKI's Strategic Role

1. The New PKI Landscape: Key Market Trends and Disruptions
2. PKI Beyond SSL: Modern Business Applications and Use Cases
3. Interoperability - The Economic Enabler: Why Cross-Border Trust is Critical
4. Strategic Recommendations

Asia as the Global PKI Growth Engine

- **Market Context:**
  The global PKI market is projecting massive growth (CAGR over 20%); Asia is driving the highest growth rate globally, fuelled by rapid digitalization.

- **Key Drivers:**
  Escalating digital transactions, widespread e-commerce adoption, and increasing cybersecurity awareness across both large enterprises and SMEs.

- **The Scale Challenge:**
  We are moving from securing hundreds of web servers to securing billions of mobile devices, IoT sensors, and cloud workloads. PKI must ***scale rapidly and efficiently*** to meet this demand.

- **PKI's New Role:**
  PKI is no longer just for website security; it is the fundamental engine of ***digital trust*** for the entire connected ecosystem.

Key Technological Shifts Disrupting PKI

- **Cloud PKI Adoption:**
  Organizations increasingly demand cloud-based PKI for its scalability, agility, and reduced infrastructure complexity. This shift simplifies certificate lifecycle management for distributed and remote work environments.

- **Post-Quantum Cryptography (PQC):**
  This is the single most urgent threat. Quantum computing will render our current asymmetric cryptography obsolete.
  - APKIC's Role: We must prioritize the development and adoption of the PQC Maturity Model and push for hybrid certification authorities to ensure a smooth, secure migration path before a quantum threat materializes.

- **Zero Trust Architecture (ZTA):**
  PKI is foundational to ZTA. It enables robust, certificate-based authentication for every user, device, and application attempting to access network resources, enforcing the principle: ***"never trust, always verify"***

Next Gen PKI Applications beyond Basic Encryption

- **Passwordless Authentication:**
  PKI enables certificate-based authentication for VPNs, Wi-Fi, and enterprise access, eliminating the weakest link in security—the password.

- **Digital Wallets & Client Authentication:**
  PKI is central to verifiable digital identity wallets, allowing citizens and businesses to prove their identity and access services securely (e.g., e-Government portals, financial onboarding).

- **IoT Device Trust:**
  In Industrial IoT (IIoT) and Smart Cities, PKI uniquely provides a tamper-proof digital identity for every device, ensuring only authenticated devices communicate and receive legitimate over-the-air updates.

Next Gen PKI Applications beyond Basic Encryption

- **Passwordless Authentication:**
  PKI enables certificate-based authentication for VPNs, Wi-Fi, and enterprise access, eliminating the weakest link in security—the password.

- **Digital Wallets & Client Authentication:**
  PKI is central to verifiable digital identity wallets, allowing citizens and businesses to prove their identity and access services securely (e.g., e-Government portals, financial onboarding).

- **IoT Device Trust:**
  In Industrial IoT (IIoT) and Smart Cities, PKI uniquely provides a tamper-proof digital identity for every device, ensuring only authenticated devices communicate and receive legitimate over-the-air updates.

The Ever-Evolving PKI Landscape

- **Increased Focus on Identity and Access Management (IAM):** PKI is playing a more central role in comprehensive IAM strategies. **Digital certificates provide strong authentication for users, devices, and applications**, enhancing security beyond traditional password-based systems.

- **The Rise of Machine Identity Management:** With the proliferation of IoT devices, microservices, and other non-human entities, managing their digital identities is crucial. **PKI provides a scalable and secure way to authenticate and authorize these machines**, ensuring the integrity of their communications and operations. Consider a network of industrial sensors, each with a unique digital certificate, securely transmitting data without human intervention.

PKI in Business : Building Digital Trust

For businesses across Asia, PKI is no longer just a security measure; it's a key enabler of digital transformation and trust:

- **Secure E-commerce and Online Transactions:** SSL/TLS certificates, a cornerstone of PKI, are essential for securing online transactions, protecting sensitive customer data, and building trust in e-commerce platforms.
- **Secure Communication and Collaboration:** PKI enables secure email communication through S/MIME certificates, ensuring confidentiality and integrity. **Digital signatures provide non-repudiation for important documents and agreements exchanged electronically, fostering trust in online collaborations.**

PKI in Business : Building Digital Trust

- **Protecting Intellectual Property and Sensitive Data:** Digital Rights Management (DRM) systems leveraging PKI can control access to and usage of **valuable digital assets, preventing unauthorized copying and distribution**.
- **Enhancing Supply Chain Security:** PKI can be used to authenticate participants and ensure the integrity of data exchanged throughout the supply chain, **reducing the risk of counterfeiting and tampering**. Imagine tracking a high-value shipment where each scan and update is digitally signed, providing an immutable audit trail.

PKI in Business : Building Digital Trust

- **Protecting Intellectual Property and Sensitive Data: Digital Rights Management (DRM) systems** leveraging PKI can control access to and usage of valuable digital assets, preventing unauthorized copying and distribution.
- **Enhancing Supply Chain Security:** PKI can be used to authenticate participants and ensure the integrity of data exchanged throughout the supply chain, **reducing the risk of counterfeiting and tampering**. Imagine tracking a high-value shipment where each scan and update is digitally signed, providing an immutable audit trail.

Case Study : Digital Transformation in IT/ITES Company

Requirements:

- The company decided to adopt eSignatures as an organization wide initiative to go paperless across several departments. This has helped in significant cost reduction, operational efficiency and increased TAT.

Solution:

Enterprise wide eSignature Workflow solution enabled with:

- Integration with ERP system (SAP S4/HANA) for digital signing of purchase orders and invoices.
- Integration with HRMS system for Employee onboarding and release of offer letters
- Integration with Contract management system for NDA's and Vendor, Partner agreements

Customer Data

- Largest Indian multinational IT company with more than 500,000 employees
- Procurement process became 75% faster
- Able to easily handle 2000+ vendor contracts every year
- Seamlessly sign 40,000+ POs every year

PKI in Banking : Ensuring Financial Security and Compliance

The banking sector, with its high-value transactions and stringent regulatory requirements, has long been a significant adopter of PKI:

- **Secure Online Banking and Payment Systems:** PKI underpins secure online banking portals and payment gateways, protecting customer credentials and financial data from cyber threats. **Multi-factor authentication** often leverages digital certificates for enhanced security.
- **Secure Interbank Communication and Transactions:** PKI ensures the secure exchange of financial information between banks, maintaining the integrity and confidentiality of critical data.
- **Digital Signatures for Financial Documents:** Digital signatures provide legal validity and non-repudiation for electronic financial documents, streamlining processes and reducing the risk of fraud. Consider **loan agreements or account opening forms signed digitally, eliminating the need for physical paperwork** and ensuring authenticity.
- **Compliance with Regulatory Standards:** Many financial regulations across Asia mandate the use of strong authentication and data protection mechanisms, making PKI a crucial tool for compliance.

Case Study : Secure Access to Financial Data and Services

Requirements:

- Centralized identity and access management
- Secure and seamless user authentication across multiple channels
- Adaptive authentication based on risk profiles

Solution:

Customer Identity and Authentication Solution powered with PKI implemented with microservices architecture to handle increased load, serving as a unified platform for all access management requirements of the bank.

Customer Data

- Largest bank in India
- **500+ Million Users**
- 15+ Banking Channels include Retail Int Banking, Merchant Int Web, Mobile Banking
- Used for Authentication, Onboarding, user state mgmt, Pwd Mgmt and Enquires
- 35000+ TPS

PKI in Defense : Safeguarding National Security

In the realm of defence, the need for secure and reliable communication and data protection is paramount. PKI plays a critical role in:

- **Secure Military Communications:** PKI enables encrypted communication channels for **voice, data, and video transmissions**, ensuring confidentiality and preventing eavesdropping.
- **Authentication of Personnel and Devices:** Digital certificates can be used to **strongly authenticate military personnel accessing sensitive systems** and to verify the identity of devices operating on secure networks.
- **Protection of Classified Information:** PKI-based encryption protects classified **data at rest and in transit**, preventing unauthorized access and ensuring national security.
- **Secure Drone and Autonomous Systems Operation:** As defence forces increasingly adopt autonomous systems, PKI provides a mechanism for **secure command and control**, ensuring the integrity and authenticity of commands sent to these systems.

Case Study : Secure Access to Sensitive Applications

Requirements:

- Customizable IAM solution
- Single Sign On
- Strict Role based access control
- Implementation in air gap environments

Solution:

Identity and access management solution powered with PKI implemented with **cryptographic tokens issued to all defence personal** to address the above requirements.

Customer Data

- Fourth largest global military power with over **1.45M** active troops
- Managing user access, authentication with PKI, and authorization
- 400+ Apps
- Defence-specific workflow customisations

The Way Forward : Collaboration and Innovation

To ensure its continued effectiveness and widespread adoption across Asia, we, as the Asia PKI Consortium, must focus on:

- **Fostering Collaboration:** Encouraging greater collaboration between industry stakeholders, governments, and research institutions to drive innovation and address common challenges.
- **Promoting Education and Awareness:** Raising awareness about the importance of PKI and best practices for its implementation across different sectors.
- **Developing Interoperable Standards:** Working towards the development of interoperable PKI standards to facilitate seamless communication and data exchange across different systems and jurisdictions.
- **Supporting Research and Development:** Investing in research to explore new applications of PKI and to prepare for future cryptographic challenges, such as the advent of quantum computing..

Conclusion

PKI remains a cornerstone of digital trust in an increasingly interconnected world.

- As we've seen, PKI is a dynamic field constantly innovating to safeguard digital interactions.
- Its evolving landscape, driven by cloud technologies, automation, and the need for robust identity management, presents both opportunities and challenges..
- The ecosystem players including the Regulators, Certification Authorities / Trust Service Providers, Solution & Service Providers, Auditors and Consultants play a crucial role in strengthening the PKI adoption across the regions and use cases.

By embracing these trends and fostering collaboration, **the Asia PKI Consortium can play a vital role** in ensuring that businesses, banks, and defence organizations across the region can leverage the power of PKI to build a **secure and trusted digital future**.

THANK YOU

vicechair2@asiapki.org

+91 99005 03217