Asia Pacific Countries | Globalization of Trust Services

23 May 2019

Keio University, Tokyo, Japan

Vijay Kumar
SVP & CTO, eMudhra | www.emudhra.com
Chair (TSWG), Asia PKI Consortium | www.asiapki.org

Introduction

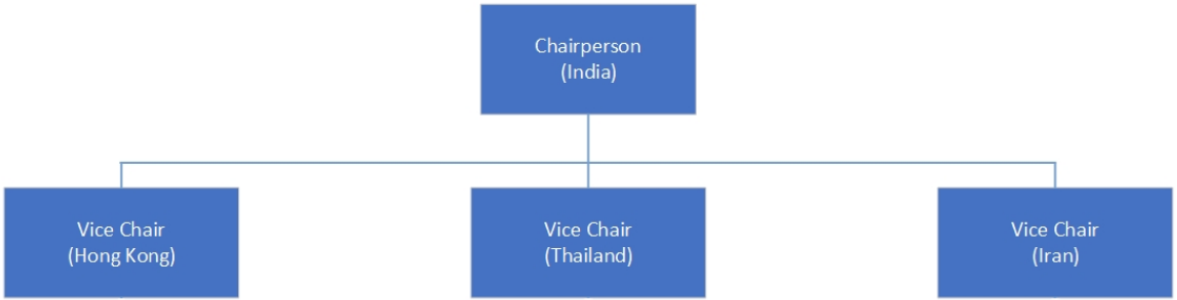
Contents

About Asia PKI Consortium

The Consortium

Established in June 2001

Trust Services across Asian Countries



Major Objectives

- Adoption
- Awareness
- Interoperability
- Mutual Recognition

About Asia PKI Consortium

Members and Meetings

1. **Members:**
    1. Members from over 10 Asian Countries
    2. Additional 10 countries under progress towards membership.
2. **Types of Members**
    1. Principal Members (One per country / economy)
    2. Enterprise Members
    3. NPO members
    4. Individual members
3. **Member meetings:**
    1. One General Assembly meeting
    2. One Steering Committee meeting
    3. One Special Steering Committee meeting


Bangladesh

China

Hong Kong

India

Iran

Japan

Korea

Macau

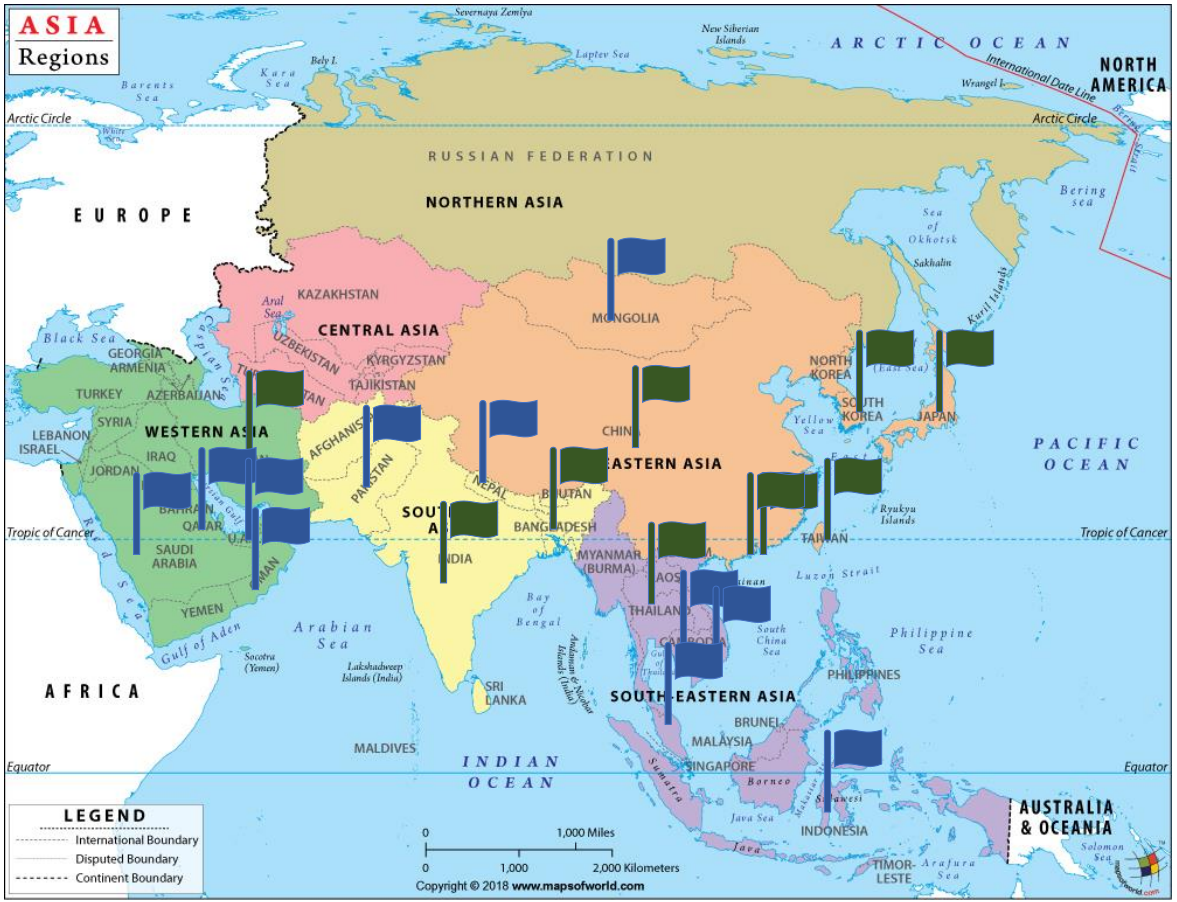
Taiwan

Thailand

Geographical Coverage

Members

In Progress



About Asia PKI Consortium

Working Groups

1. **Business Application Working Group**

   Chair: Ms. Karen Cheng, Taiwan & Co-Chair: Mr. Vijay Kumar, India

   1. To resolve cross-domain & cross-region issues
   2. To promote the exchange and collaboration between members
   3. To explore and enrich the information applications & IT-enabled services

2. **Legal & Policy Working Group**

   Chair: Mr. Gordon Szetu, Hong Kong

   1. To influence interoperability initiatives
   2. To collaborate with government and related industries
   3. To produce policy papers and regulative awareness among the members.

3. **Technology & Standards Working Group**

   Chair: Mr. Vijay Kumar, India

   1. To standardize and make technological advancements.
   2. To work on Public Key Cryptography, and the emerging technologies.
   3. To help bring technological platforms together for the members.
   4. To produce whitepapers and case studies

Trust Services in Asian Countries

Trust Services in Asian Countries

Overview

1. Trust Services in Asian Countries are mostly **regulation driven**.
2. Based on **THE UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES** (2001)
   - United Nations Commission on International Trade Law
3. Most of the countries have enacted **Electronic Transactions Law** under various names.
4. Introduces **Trust Service Providers / Certification Authorities** for electronic signatures.
5. Most of the countries appoint National Regulator to
   1. Operate Root CA, and appoint Issuing CAs under the Root. OR,
   2. Accredit / Empanel Issuing Cas
6. Adopt Web trust principles for Assessment, or have their own customized assessment criteria.

Country Wise

Trust Services in Asian Countries

India 

1. National Root Certificate by Government of India (Controller of Certifying Authorities).
2. Information Technology Act, 2000 provides legal validity.
3. Userbase: 50 million+
   - 45 million+ online electronic signature users
   - 5 million+ smart card (USB Crypto Token) based electronic signature users
4. Mandatory for several classes of Tax filing, Company law filings, e-Procurement / tendering systems, etc.
5. Trust Service Providers:
   - 5 Trust Service Providers for public
   - Couple of them for Military, Government, etc.
6. Custom Audit Criteria for TSPs with government auditor empanelment and training program.

Trust Services in Asian Countries

China

1. “Electronic Signature Law of the People's Republic of China” in 2004
2. Trust Service Provider is called as “**Electronic Verification Service Provider**”.
3. Regional Trust Services are established based on this law. Banks and several organizations run their own PKI system.
4. Implementations: eID project (Optional), E-Governance applications, E-Commerce applications
5. In Banking, it is mandatory to use PKI based electronic authentication / signature for transactions above certain limit. But there is no interoperability and customer should use bank specific key.

Hong Kong

1. “Electronic Transaction Ordinance” in 2000
2. Root Certificate Operated by **Hong Kong Post**.
3. Implementations: eID project, E-Governance applications, E-Commerce applications
4. Optional usage in Banking.
5. No third party trust provider. Hong Kong Post e-Cert services is operated by “Certizen” (private sector).
6. Separate Issuing CAs for Banking, Individuals, Corporates, etc

Trust Services in Asian Countries

Korea

1. "Electronic Signature Act" in 1999
2. Two Certification Authorities Schemes
   - National PKI operated by Korea Internet Security Agency (KISA) catering to general public
   - Government PKI operated by Government Certification Management Authority (GCMA) catering to government officers
3. KISA issued certificates are used in Internet banking, Online stock trading, online shopping and e-government (G2C) services

Taiwan

1. "Electronic Signature Act" in 2001
2. Two Certification Authorities Schemes
   - Taiwan Certification Authority (TWCA) setup by financial bodies catering to public using financial services
   - Government PKI operated by Taiwan Government for G2C use cases
3. TWCA is also assessed under Webtrust principles for CA.
4. TWCA has issued nearly 5 million certificates till 2018.

Trust Services in Asian Countries

Thailand 

1. “Electronic Transactions Act” in 2001
2. National Root setup by Electronic Transactions Development Agency (ETDA)
3. Two issuing CAs setup under the national root:
    1. Thai Digital ID: established in 2014
    2. INET: established in 2019
4. Thai Digital ID has setup services for e-Tax Invoice and e-Insurance Policy
5. Export-Import (Customs) has been one of the main use case of Digital Signature adoption.

Macao 

1. “Electronic Documents and Signatures Law” in 2005
2. Macao Post and Telecommunications Bureau is the regulator
3. One Trust Service Provider operated by the regulator called eSignTrust
4. Provides legal definitions for Advanced and Qualified Digital Signatures.
5. eSignCloud services enable cloud based signatures similar to remote signing.

Trust Services in Asian Countries

Malaysia 

1. “Electronic Commerce Act” in 2000 (Earlier Digital Signature Act, 1997)
2. Malaysian Communications And Multimedia Commission (MCMC) is the national regulator.
3. Trust Service Providers are accredited based on their Webtrust seal
4. Four TSPs: Pos Digicert, MSC Trustgate, Telekom Applied Business and Raffcomm Technologies
5. Tax Filing is the biggest use case. Other use cases include marriage certificates, educational certificates, and PKI is also used in document movement across government.

Saudi Arabia 

1. “Electronic Transactions Law” in 2007
2. National Center for Digital Certification (NCDC) is the regulator
3. One Trust Service Provider operated by the regulator for Government PKI usage
4. New Trust Service Provider being setup in private sector for usage by general public.
5. Trust Service Providers are accredited based on their Webtrust seal, in addition to Saudi National PKI Policy adherence.

Trust Services in Asian Countries

Asian Trends

- PKI is in **continuous demand**.
  - The need for PKI has seen a consistent growth, and has been part of new emerging applications.
- **e-Authentication & Signing** has been a larger use case.
  - Digital Signing Certificates using Public PKI has grown many folds due to regulatory mandates & paperless initiatives coming from several countries / regions.
- New Trends:
  - PKI Technology has matured with **adoption of newer algorithms** (like ECC) and technological use cases (like Blockchain, IoT).
  - There is a move towards **cloud & mobile PKI**, which is set to improve the way users use PKI.
  - **Short Term Certificates** are seen as better alternates in cloud PKI, instead of Long Term Certificates, as key-protection / sole-control is a challenge.
  - IoT is emerging as a new application use case for PKI. However, regulations are at nascent stage and use of Public PKI is slowly emerging. Else, it is being done using Private PKI.

Trust Services in Asian Countries

Summary

1. Every country has enacted Electronic Transaction Law in some form or the other.
2. Implementation Status:
   - Some of the countries have well established PKI ecosystem like India, Malaysia, Taiwan, Korea, etc
   - Some of the countries have passed the law but yet to implement for large public use cases.
3. Policy Requirements of every country vary a bit, but largely based on RFC 3647. Physical controls, environmental controls, key controls, etc are mostly identical.
4. Assessment schemes vary from country to country, as there is no common standard adopted in the region.
5. Interoperability and Mutual recognition is still in nascent stage between the countries.
6. Asia PKI Consortium continues to work towards filling these gaps.


Asia PKI Consortium


emudhra
Trust Delivered


India PKI Forum

THANK YOU