PKI Body of Knowledge: Development & Dissemination

Dr. Balaji Rajendran
Centre for Development of Advanced Computing
Bangalore

National Conference on Digital Signatures and PKI
Theme: PKI-enabled Digital Banking and Financial Services
Mumbai, 17th June 2016

Agenda

- Quick Facts about PKI
- PKI Body of Knowledge
- Call for Inputs

General Facts!

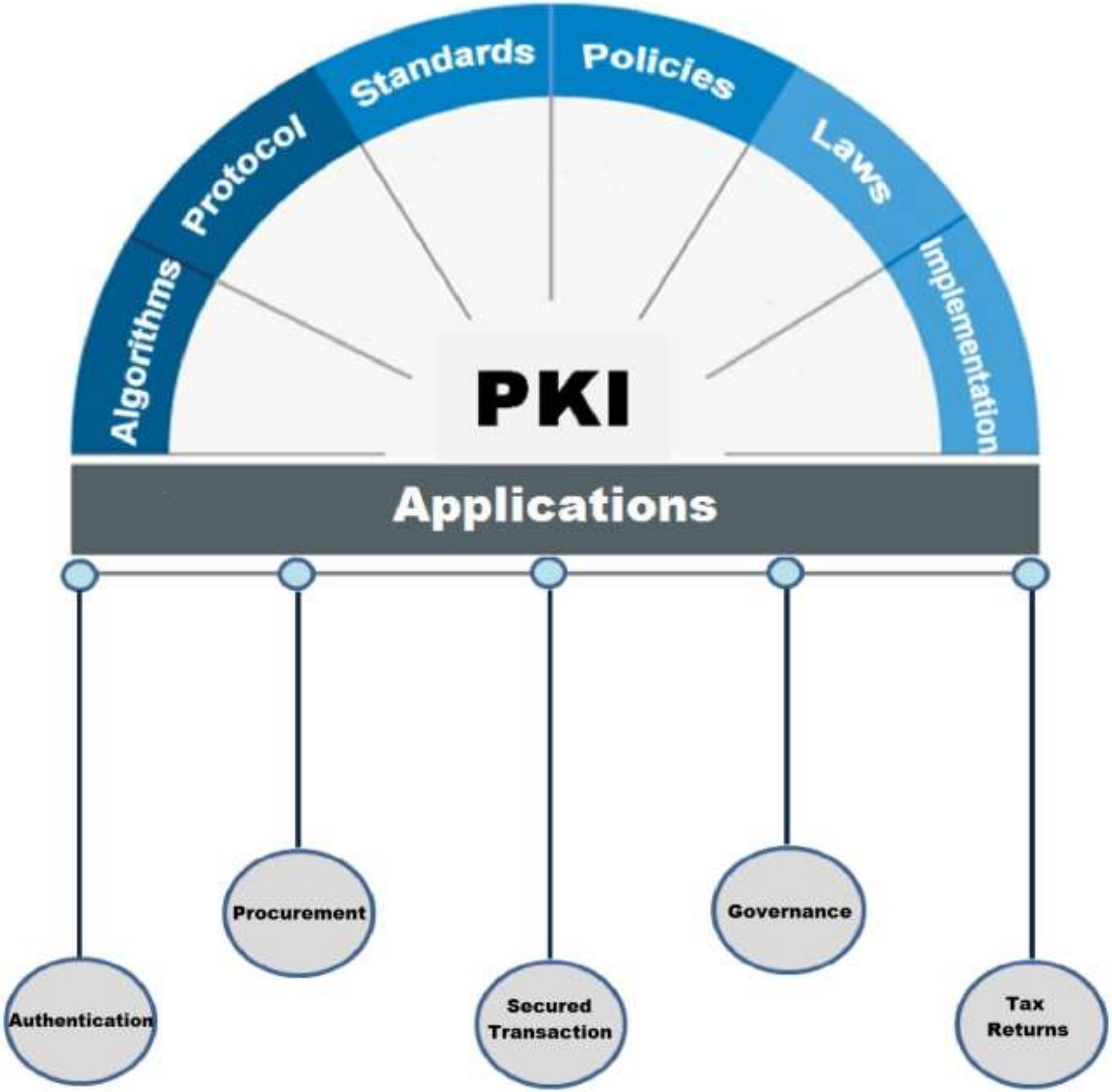
- Technology is best demonstrated by Applications
    - Herbert Kroemer, IEEE Fellow & Nobel Prize Winner
- PKI is a technological answer for ‘trust’ in electronic transactions
    - Came into existence around 1993;
    - Applications are ever increasing
        - As demand for ‘trust’ is increasing!

General Facts!

- Technology cannot exist in isolation
  - Requires an ecosystem to survive and nurture itself
    - Technology Developers and Application Builders
- PKI Technology
  - Being a technology for ‘trust’, it requires the support of legal system and proper regulatory mechanisms
  - India has been leading in the adoption, thanks to Indian IT Act 2000

CCA

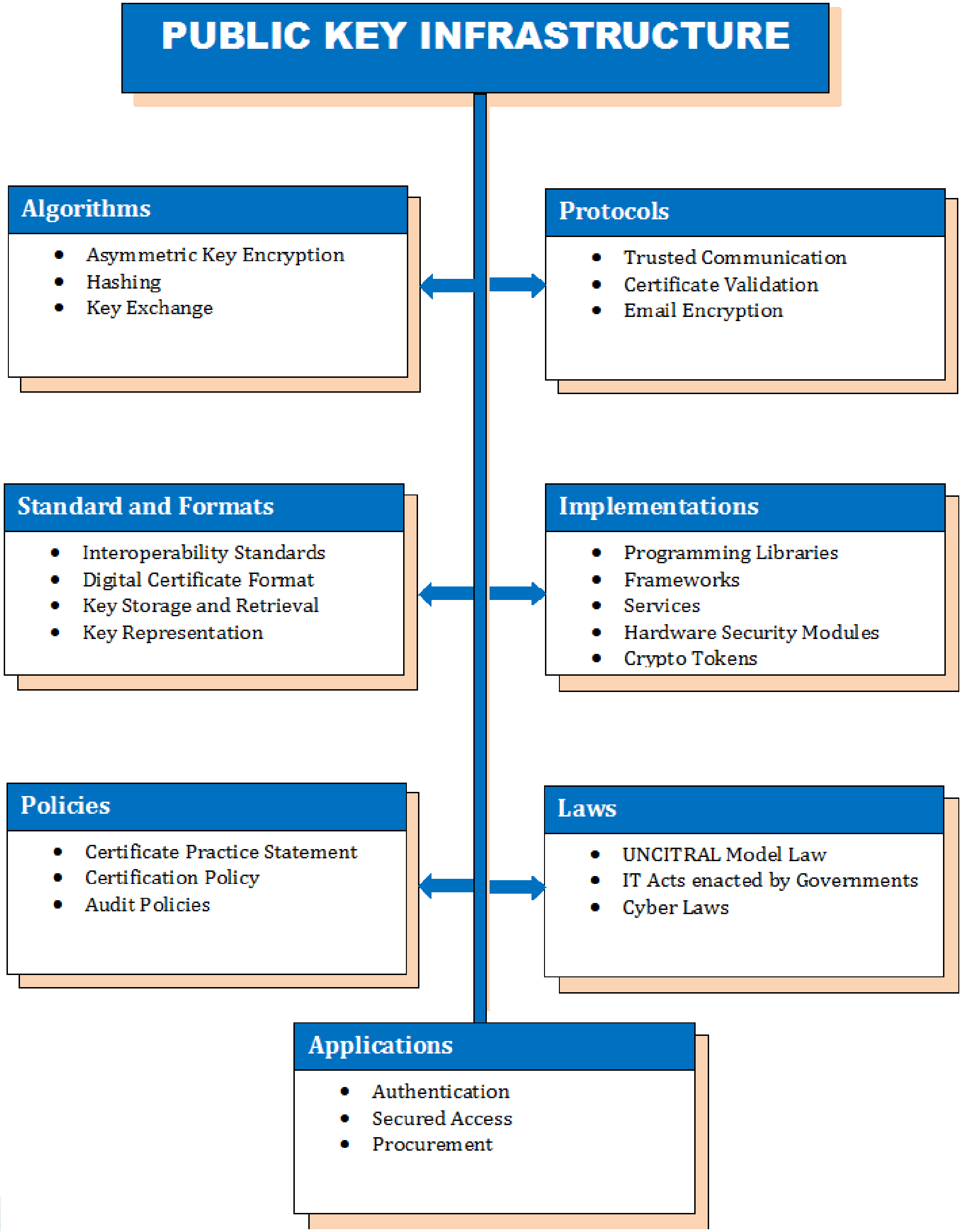
PKI Ecosystem



Framework of PKI BoK

- **Algorithms** drawn from Cryptography
- **Protocols** defining the rules of **implementations**
- **Standards** for interoperability
- **Policies** for Protection
- **Laws** enacted for Legal Sanctity and
- **Applications** for Perception & Utilization
- General Definition of PKI
  - PKI consists of hardware, software, policies and standards to manage the creation, administration, distribution and revocation of keys and digital certificates

PUBLIC KEY INFRASTRUCTURE



Algorithms

- Asymmetric Key Encryption
- Hashing
- Key Exchange

Protocols

- Trusted Communication
- Certificate Validation
- Email Encryption

Standard and Formats

- Interoperability Standards
- Digital Certificate Format
- Key Storage and Retrieval
- Key Representation

Implementations

- Programming Libraries
- Frameworks
- Services
- Hardware Security Modules
- Crypto Tokens

Policies

- Certificate Practice Statement
- Certification Policy
- Audit Policies

Laws

- UNCITRAL Model Law
- IT Acts enacted by Governments
- Cyber Laws

Applications

- Authentication
- Secured Access
- Procurement

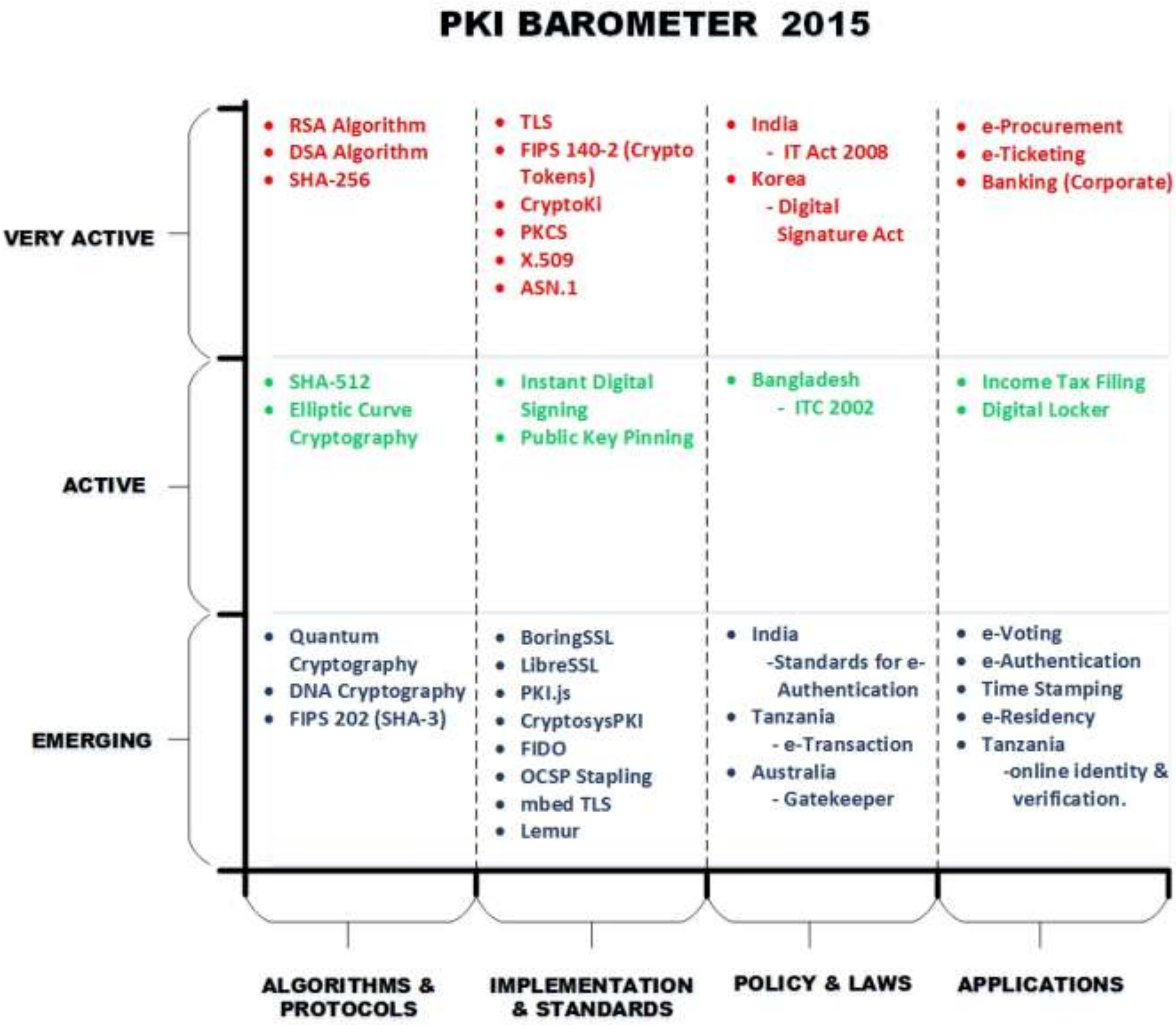
Framework of PKI BoK

- Knowledge Areas & Relevant Stakeholders
  - Algorithms –Cryptographers, Researchers
  - Protocols – Internet Protocol Development Community
  - Standards – Industry Consortiums and Government Standards
  - Implementations – System Software Developers, H/W Manufacturers
  - Policy– CA, Organizational Policy, Information Security Analysts
  - Law – Legal Fraternity focusing on Cyber Space
  - Applications –PKI-enabled Application Developers

What we need from you?

- Why You?
  - BFSI across the world over has been the early adopter of Technology
- Your Stories & Experience
  - Paint points faced by you
    - Eg: Implementation issues
  - Transaction Experience
    - Speed & Ease of Use
    - Transparency & Accountability

PKI Barometer



PKI BAROMETER 2015

	ALGORITHMS & PROTOCOLS	IMPLEMENTATION & STANDARDS	POLICY & LAWS	APPLICATIONS
VERY ACTIVE	• RSA Algorithm • DSA Algorithm • SHA-256	• TLS • FIPS 140-2 (Crypto Tokens) • CryptoKi • PKCS • X.509 • ASN.1	• India - IT Act 2008 • Korea - Digital Signature Act	• e-Procurement • e-Ticketing • Banking (Corporate)
ACTIVE	• SHA-512 • Elliptic Curve Cryptography	• Instant Digital Signing • Public Key Pinning	• Bangladesh - ITC 2002	• Income Tax Filing • Digital Locker
EMERGING	• Quantum Cryptography • DNA Cryptography • FIPS 202 (SHA-3)	• BoringSSL • LibreSSL • PKI.js • CryptosysPKI • FIDO • OCSP Stapling • mbed TLS • Lemur	• India -Standards for e-Authentication • Tanzania - e-Transaction • Australia - Gatekeeper	• e-Voting • e-Authentication • Time Stamping • e-Residency • Tanzania -online identity & verification.

Contents Developed

- Code Snippets
  - Digital Signing and Asymmetric Encryption using Blank Crypto Token
  - Use of C# Bouncy Castle API
  - iOS based App for Digital Signing
  - Android based App for Digital Signing and Encryption
- Kit comprising of
  - Bookmarks
    - Signing and Verification
    - Encryption and Decryption
  - Crossword Puzzle
  - Graphical Illustrations targeted towards novice audience
  - Glossary
  - FAQ
  - Movies
- Evaluations
- Resource Sharing
  - Online Sharing of resources used in each program
  - Use of Social Media

Knowledge Dissemination Program (KDP) – Activities

PKI Knowledge Dissemination Program (KDP)

- KDPs are of following types:
  - Awareness Program
    - Initiates the users into the world of Digital Signatures & PKI
      - Half-day and 1-day programs are offered; No. of Participants: 25-200;
      - Targeted Audience: Officials of State & Central Govt., Banking & Finance; General Public
  - Training Program
    - Intensive programs delivering hands-on experience
      - 1-Day & 2-Day courses are offered; No. of Participants: 15-60;
      - Typically tailored to meet the needs of an organization
      - Targeted Audience: PKI Application Developers, PKI Administrators
  - Conference
    - Theme-based – Applicable to particular Sector
    - General – Covering the entire spectrum of PKI

International Conference

- www.pkiindia.in/ic.jsp

Thank You