Evolution of PKI Ecosystem

DR. BALAJI RAJENDRAN
PRINCIPAL TECHNICAL OFFICER
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
NO.68, ELECTRONICS CITY, BANGALORE

PKIA 2017 – INTERNATIONAL CONFERENCE ON PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS
15TH NOVEMBER 2017

Agenda

- Spectrum of Transparency
- Understanding Electronic Trust and its Elements
- Approaches to Electronic Trust
- Public Key Infrastructure
- PKI Ecosystem
- SWOT analysis of PKI Ecosystem
- Summary

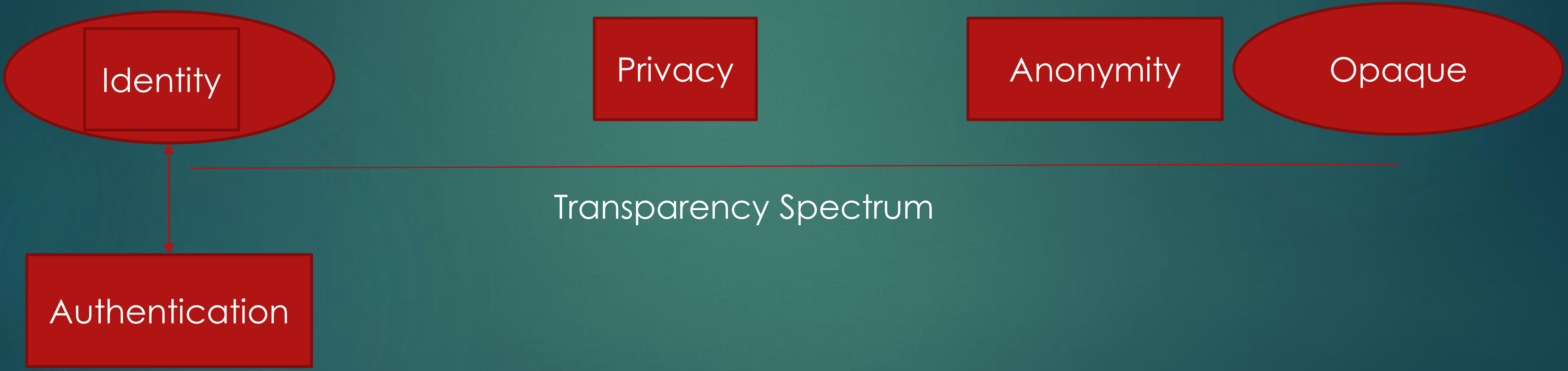
Spectrum of Transparency

Transparent

Opaque

Transparency Spectrum

Spectrum of Transparency



Electronic Transactions

- Transparency
  - Everyone knows who has done what
  - Identity is central to Transparency
- Opaque
  - No one knows who has done what
- Anonymity
  - Everyone knows something **particular** has been done, but none knows who has done that
- Privacy
  - No one knows what's happening, but everyone knows who are involved and know something is happening

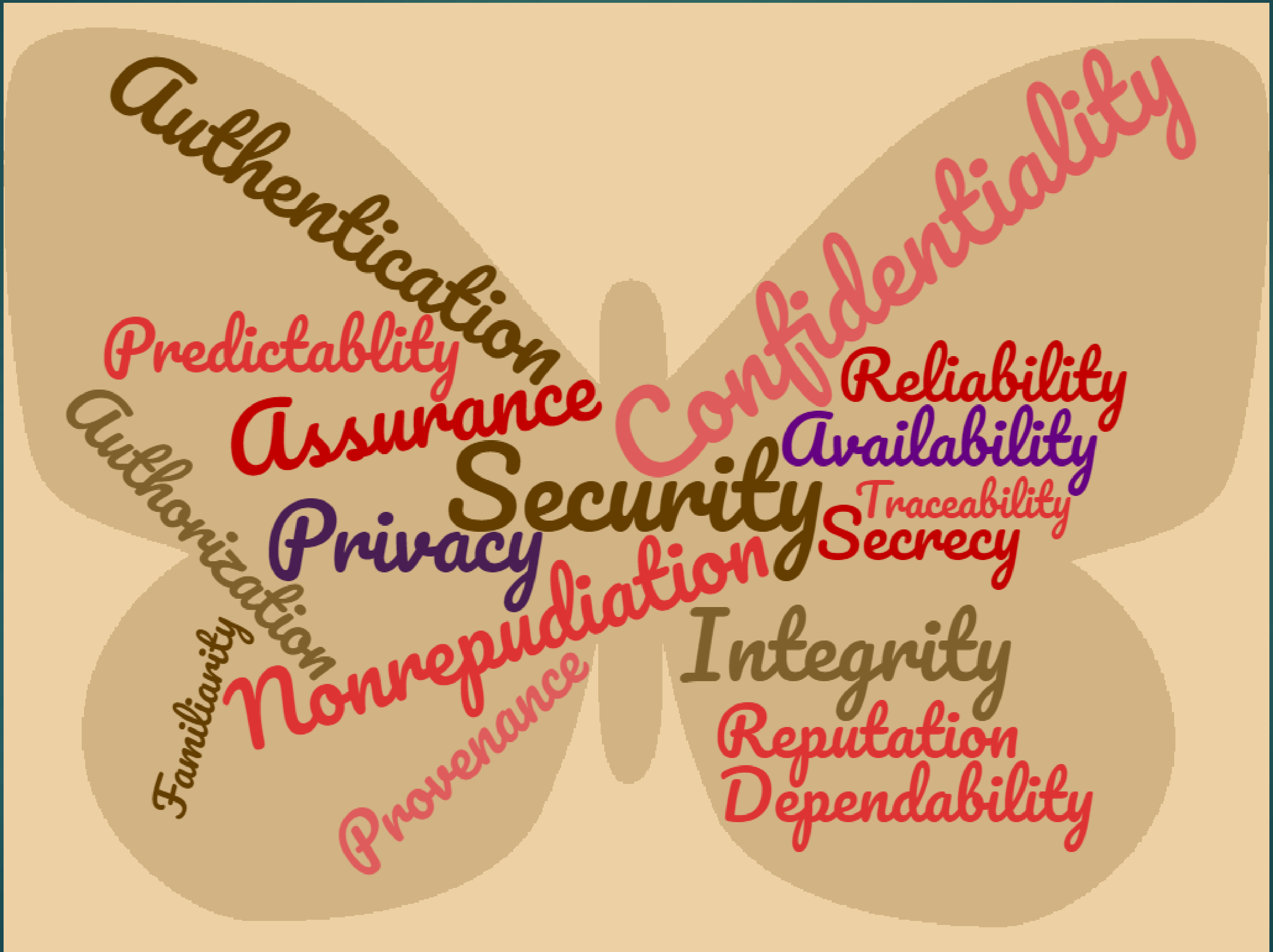
Legal World

- Confidentiality
  - Information shared by an entity in a transaction should not be disclosed without the consent
- Integrity
  - Accuracy of the information
- Non-Repudiation
  - Inability to repudiate (deny) an executed action

Non-Repudiation – A bit of Caution!

- Traditional Legal Definition for Repudiation:
  - The act can be a forgery;
  - The act is not a forgery, but was obtained via:
    - Unconscionable conduct
    - Stealing - Fraud
    - Undue influence

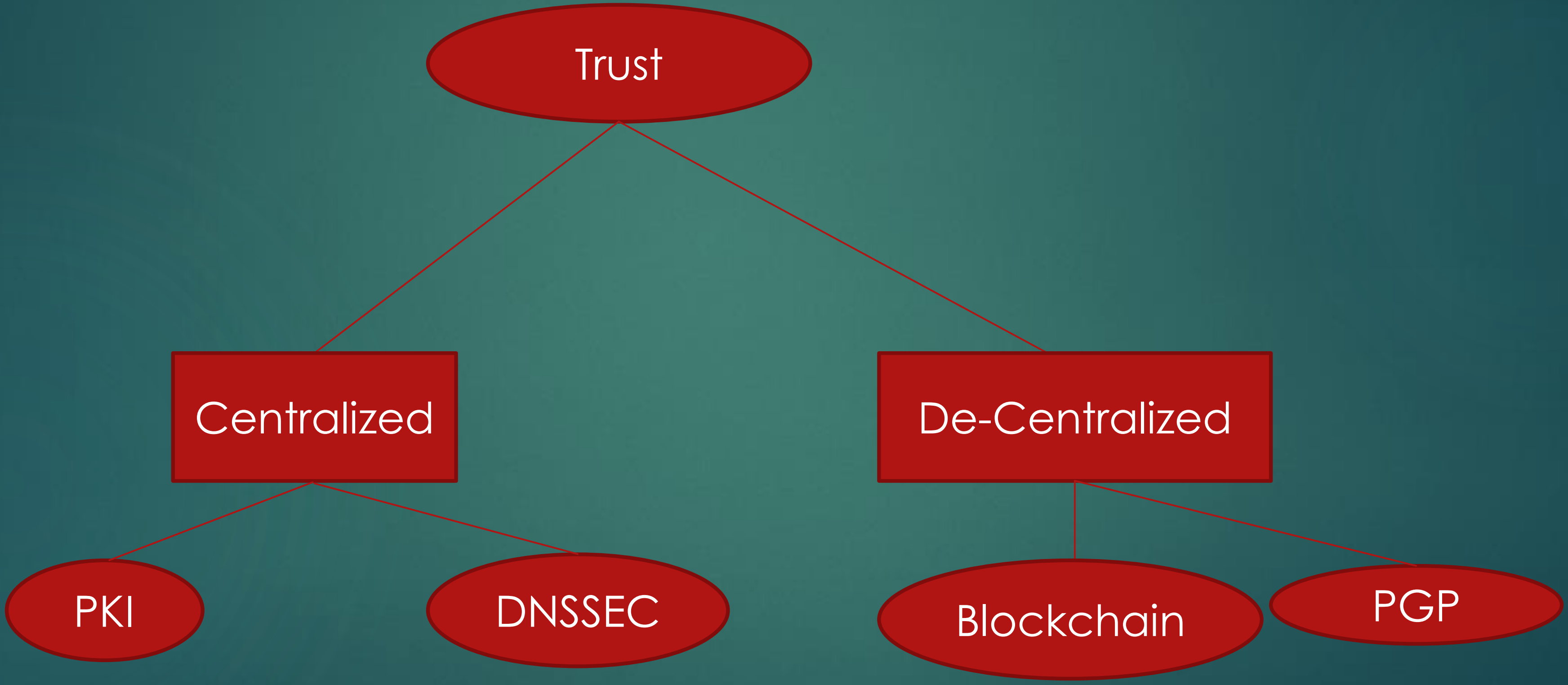
Defining Trust



Essential Factors of Trust

- **Privacy (Confidentiality):** Ensuring that **only authorized** persons read the Data/Message/Document
- **Authenticity:** Ensuring that Data/Message/Document originated from the **claimed** signer / sender
- **Integrity** : Ensuring that Data/Message/Document are **unaltered** by any unauthorized person
- **Non-Repudiation:** Ensuring that one **cannot deny** their signature or origination of a message

Approaches to Electronic Trust



Certifying Authority (CA)

- Certifying authority is an entity which issues Digital Signature Certificate **(DSC)**
- It is a **trusted third party**
- CA’s are the important components of Public Key Infrastructure (PKI)

Responsibilities of CA

- Verify the credentials of the person requesting for the certificate (RA’s responsibility)
- Issue certificates
- Revoke certificate
- Generate and upload CRL

Digital Signatures

- Establishes
  - **Identity and Authenticity** of the Signer
  - **Integrity** of the document
  - **Non-Repudiation** (through Certificates issued by CA)
- Rules
  - **Signing – Private Key of the Signer**
  - **Verification – Public Key of the Signer**

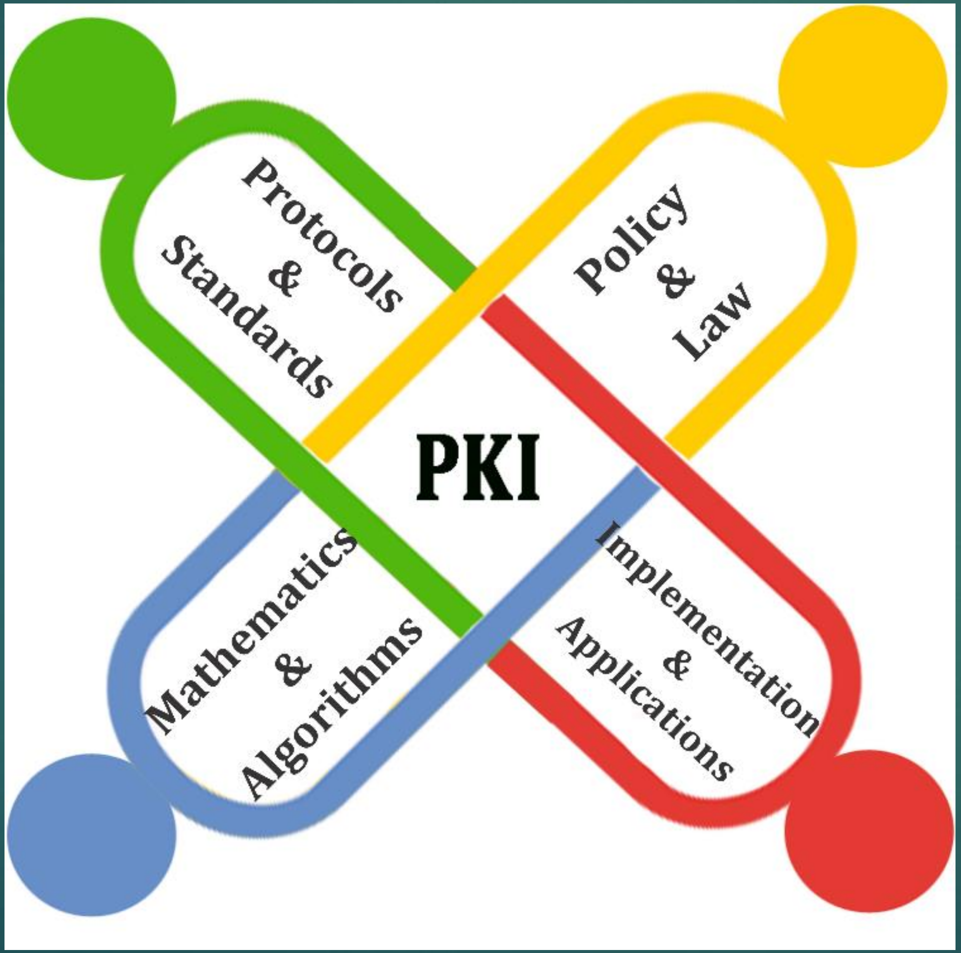
Asymmetric Encryption

- Provides **Privacy** / **Confidentiality**
- Rules
  - Encryption – Public Key of the Receiver
  - Decryption – Private Key of the Receiver
- Essential Trust Factors
  - Digital Signature + Asymmetric Encryption

What is PKI (Quo Vadis PKI)

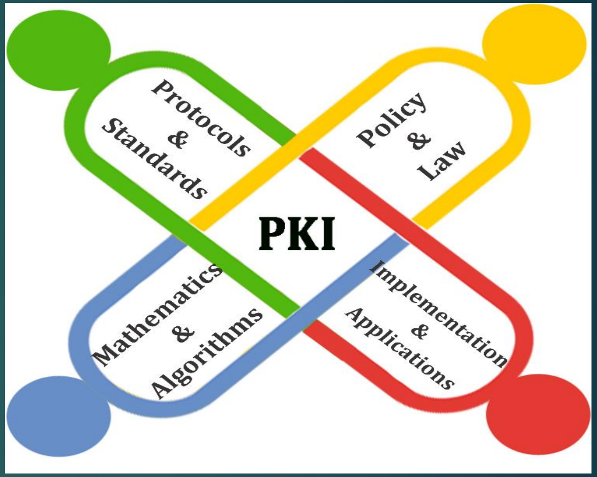
- Layman’s Definition
  - PKI = PKC + CA + PKCS + Legislations + Applications
- PKI had evolved into a complete **ecosystem** for facilitating trust in electronic transactions

PKI Ecosystem



PKI Ecosystem & Stakeholders

- PKI is an ecosystem comprising of:
  - Math & Algorithms
    - Key Stakeholder: Cryptographers, Researchers
  - Standards & Protocols
    - Key Stakeholder: Application Developers, Standard developers
  - Policy & Law
    - Key Stakeholder: Regulatory bodies, Law Protection Agencies
  - Implementations & Applications
    - Key Stakeholder: End-Users & Systems



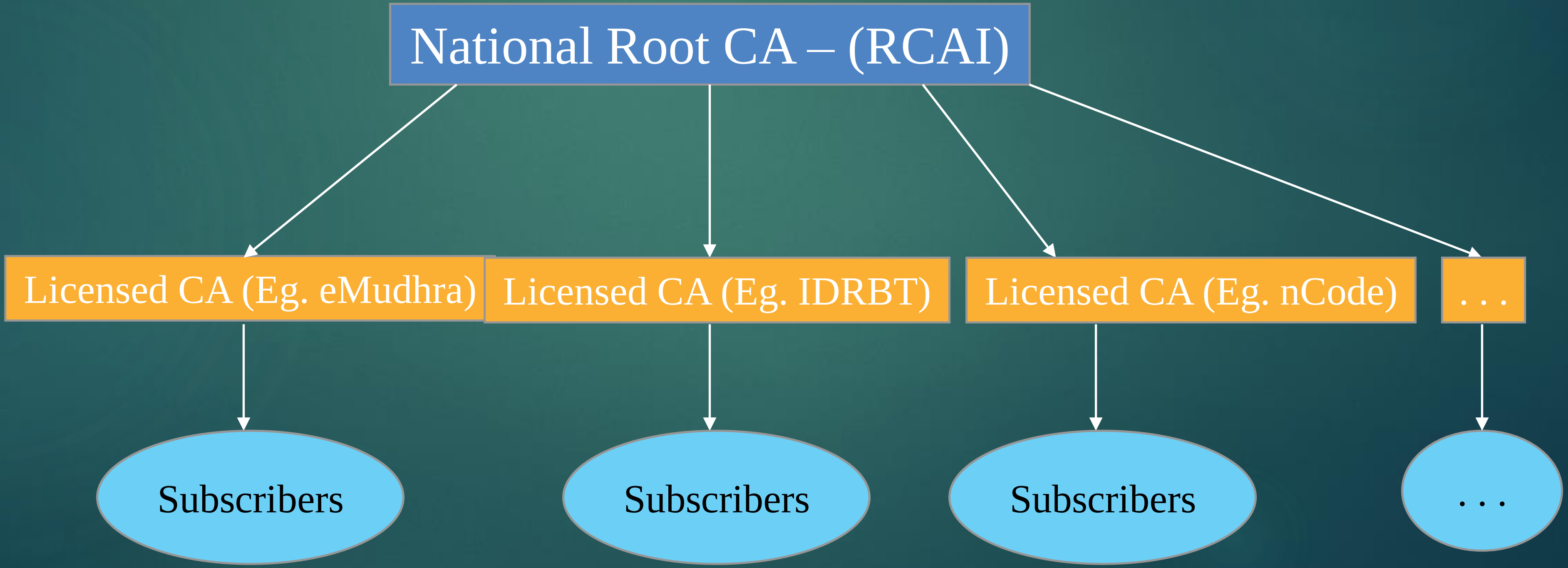
SWOT Analysis of PKI Ecosystem

- Strengths
  - Reliable and Trust-worthy System
    - Have stood the test of time! (25+ years)
  - Ability to adapt, and standardize
    - Changing technology landscapes (Hashing algo, crypto algos)
    - Standards (PKCS, IETF, IEEE etc..)
- Opportunities
  - Ability to diversify and penetrate!
    - Cloud, IoT, Energy sectors …
- Threat
  - Usability
- Weakness
  - Absence of Globally anchored trust models (Cross Certification)
  - Attacks on Weakest links in Ecosystem – CA Infrastructure

Indian PKI Ecosystem

Trust Model in India

- Hierarchical model is followed
- For a Digital Certificate to be trusted, it must derive its trust from CCA – the apex regulatory & licensing body in India – established through Indian IT Act 2000



Licensed CA’s in India

- National Root CA (RCAI) – operated by **CCA**
  - Only issues CA certificates for licensed CAs
- CAs licensed under the National Root CA
  - eMudhra (www.e-mudhra.com)
  - nCode Solutions CA(www.ncodesolutions.com)
  - SafeScrypt (www.safescrypt.com)
  - IDRBT CA (www.idbrtca.org.in)
  - Capricorn (www.certificate.digital)
  - NSDL (www.egov-nsdl.co.in)
  - C-DAC (http://esign.cdac.in)

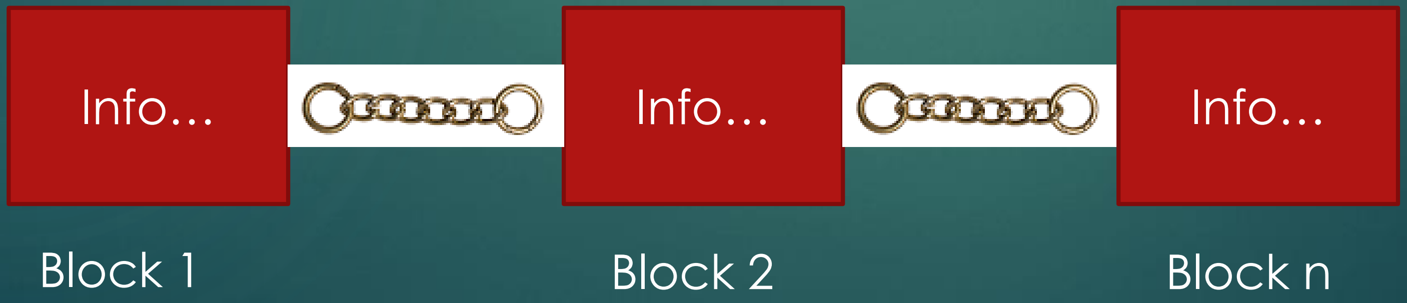
PKI: India’s answer

- Threat
  - Usability
  - Indian answer: Digital Signatures leveraging Aadhaar – e-Sign
- Weakness
  - Attacks on Weakest links in Ecosystem – CA Infrastructure
  - Indian answer: Central Regulatory Authority – CCA

Looking Through the Future

Layman’s view of Blockchain

- Block-Chain
  - Block: A logical container of information
    - Information is verified before it is added to the block
      - By a group of **competing** people/entities
    - Information within a Block is arranged in a tree-based structure that’s easy to discover a piece of info and errors
  - Chain: Logically and Cryptographically linked structure

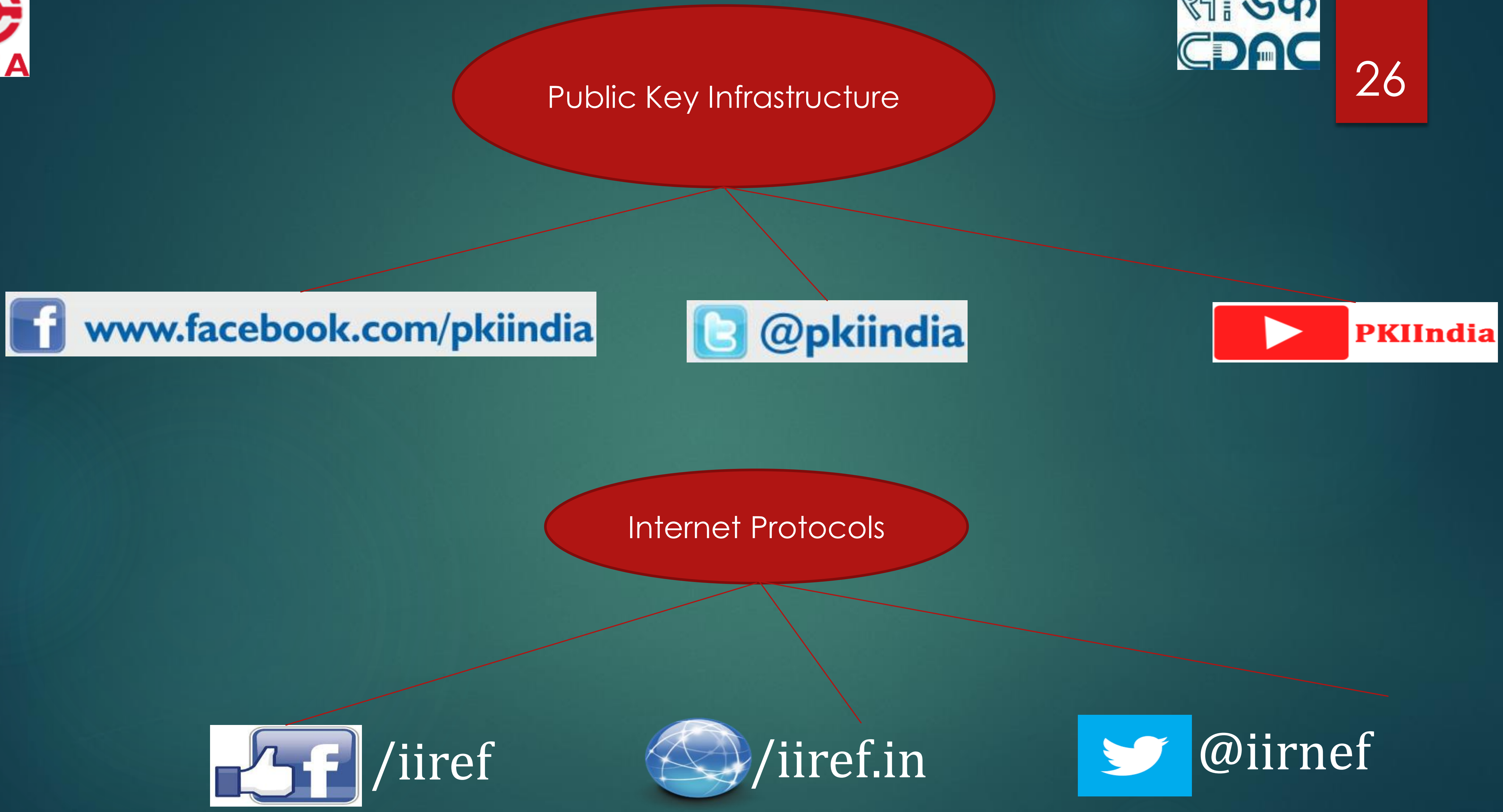


Elements of Trust Vs Technologies

	Integrity	Confidentiality	Authentication	Non-Repudiation
Hashing	✓	✗	✗	✗
Encryption	✗	✓	✗	✗
Signature	✓	✗	✓	✓
Certificate	✗	✗	✓	
Signcryption	✓	✓	✓	
Block Chain	✓	✗	✗	✗

Summary

- PKI applications are ever increasing
  - Thanks to Cloud and IoT
- Emerging Technology Influence
  - Blockchain
    - PKI can absorb Blockchain in various processes of the PKI Ecosystem
      - Eg: Certificate Transparency
- PKI's Motto:
  - Making transactions secure, easier, faster, and reliable - (SEFR)



Public Key Infrastructure

www.facebook.com/pkiindia

@pkiindia

PKIIndia

Internet Protocols

/iiref

/iiref.in

@iirnef

Thank You!

balajirajendran@gmail.com