

Root Certifying Authority of India (RCAI)

PKI Outreach Programme (POP)
Nationwide Awareness Programme,
Centre for Development of Advanced Computing (C-DAC)
Electronics City, Bangalore.

Overview

- Role of RCAI
- Licensed CA's
- PKI Implementation in India
- India PKI Forum
- End Entities, subscribers and relying parties

Role of RCAI

- The IT Act provides the Controller for Certifying Authorities (CCA) to license and regulate the working of CA.
- The CCA operates RCAI for certifying the public keys of CA's using its private key

- The CCA has established the RCAI under section 18(b) of the IT Act to digitally sign the public keys of CAs in the country
- The requirements fulfilled by the RCAI include the following
 - The license issued to the CA is digitally signed by the CA
 - All public keys corresponding to the signing private key of a CA are digitally signed by the CCA
 - Relying parties can verify the CAs public key signed by CCA through the CCA's website

- The CCA performs the Root CA functions in accordance with the CPS of RCAI
- The RCAI root certificate is the highest level of certification in India
- It is used to sign the public keys of the licensed CAs.
- The RCAI certificate is the self-signed certificate

Licensed CAs

- Safescrypt
 - Private Certifying Authority
 - <http://www.safescrypt.com/>
- NIC
 - An organization of Government of India, issuing Certificates to Government organizations for G2G transactions
 - <https://nicca.nic.in/>
- IDRBT
 - Established by Reserve Bank of India, issuing Certificates to Banking industry for INFINET transactions
 - <http://idrbtca.org.in/>

Licensed CAs

- TCS
 - Private Certifying Authority to issue Certificates to Individuals, Company and Government users
 - <http://www.tcs-ca.tcs.co.in/>
- MTNL
 - <http://www.mtnltrustline.com/>
- Customs & Central Excise
 - <https://www.icert.gov.in/>
- (n)Code Solutions CA (GNFC)
 - <https://www.ncodesolutions.com/>

PKI Implementation in India

PKI in India: Current Status



- 7 CAs Licensied by RCAI
- Total Number of Certificates issued by all CAs in India

Key Industry Segment

- Government
 - G2G
 - G2C
- Banking
 - Inter/Intra Banking transactions
 - Corporate Internet Banking
 - Retail Banking
- Financial Services & Broking
- B2B
- Healthcare
 - Telemedicine

- Government
 - Filing Tax Returns online by taxpayers
 - Citizen ID card
 - Issuing forms and licenses
 - Reservations & ticketing
- Banking
 - Inter/ Intra bank messaging systems
 - Corporate Internet Banking applications
 - Internet Banking
- Financial Services/ Broking
 - Online Trading
 - Electronic Contract Notes

- B2B
 - Online Tendering
 - e-Procurement
- Healthcare
 - Healthcare Management System (HMS)
 - Electronic Medical Recording (EMR)
 - Electronic Prescriptions

Existing Implementation

- Government
 - Ministry of Commerce and Industry
 - Electronic applications and approvals of Special Economic zones and Export Oriented Units
 - Online Applications for licenses by the EXIM community
 - Income Tax Department
 - Online Tax returns through e-Intermediaries

Existing Implementation

- Banking
 - Securing Inter/Intra bank messaging system (SFMS)
 - PKI enabling Corporate Internet Banking application by banks like ICICI Bank, Punjab National Bank

Existing Implementation

- Financial Services & Broking
 - Two major depositories in India have their applications PKI enabled
 - NSDL (National Securities Depositories Limited)
 - CDSL (Central Depository services (India) Ltd.)
 - Two major Stock Exchanges in India have secured their transactions with PKI
 - BSE
 - NSE
- B2B
 - E-Procurement and e-Tendering applications

India PKI Forum

- Is an Association of organization that are interested in promotion of PKI
- Primary members are the CCA and all the licensed CA. Any organization with interest can be associate member

- Some broad objective
 - To promote use of PKI and facilitate the penetration electronic transactions in society
 - To interact with other national and International PKI forums
 - To sponsor, conduct or organize training on subjects of interest
 - To disseminate information about electronic transactions

References

- www.cca.gov.in
- PKI in India, by M. Vidyasagar, TCS
- Current PKI Scenario in India, by Dr. Sudeep Oberoi, India PKI Forum