# Protecting Transactions and Data in Virtual World using PKI [ DSC ]

National Conference on DSC & PKI

Mumbai, June 17th, 2016

Presented By Girdhar Varliani

**(n)Code Solutions - A Division of Gujarat Narmada Valley Fertilizers & Chemicals Limited**

14th Floor, Tower One, Road 5C, Zone 5, GIFT City, Gandhinagar - 382 355. Phone : +91 79 6674 3300 / +91 79 6674 3200

403, 4th Floor, GNFC Infotower, S.G.Road, Bodakdev, Ahmedabad – 380054. Phone : +91 79 4000 7300 | Fax : +91 79 2685 7321

www.ncode.in | www.ncodesolutions.com | www.nprocure.com

# (n)Code Solutions

- (n)Code Solutions - IT Division of GNFC Ltd, a 4600+ Cr Organization
- Licensed Certifying Authority since 2004 to issue Digital Signatures
- Empanelled to provide eSign Services
- PAN presence with 15 offices
- IT framework provided to Customers in African Countries
- Esteemed Clientele : From National Level Banks to Forbes 500 Companies, with many Central and State Government Departments
- NICSI Empanelled for DSC Issuances
- CMMi Level 5, ISO 9000:2008, ISO 20000-1 and ISO 27001:2005

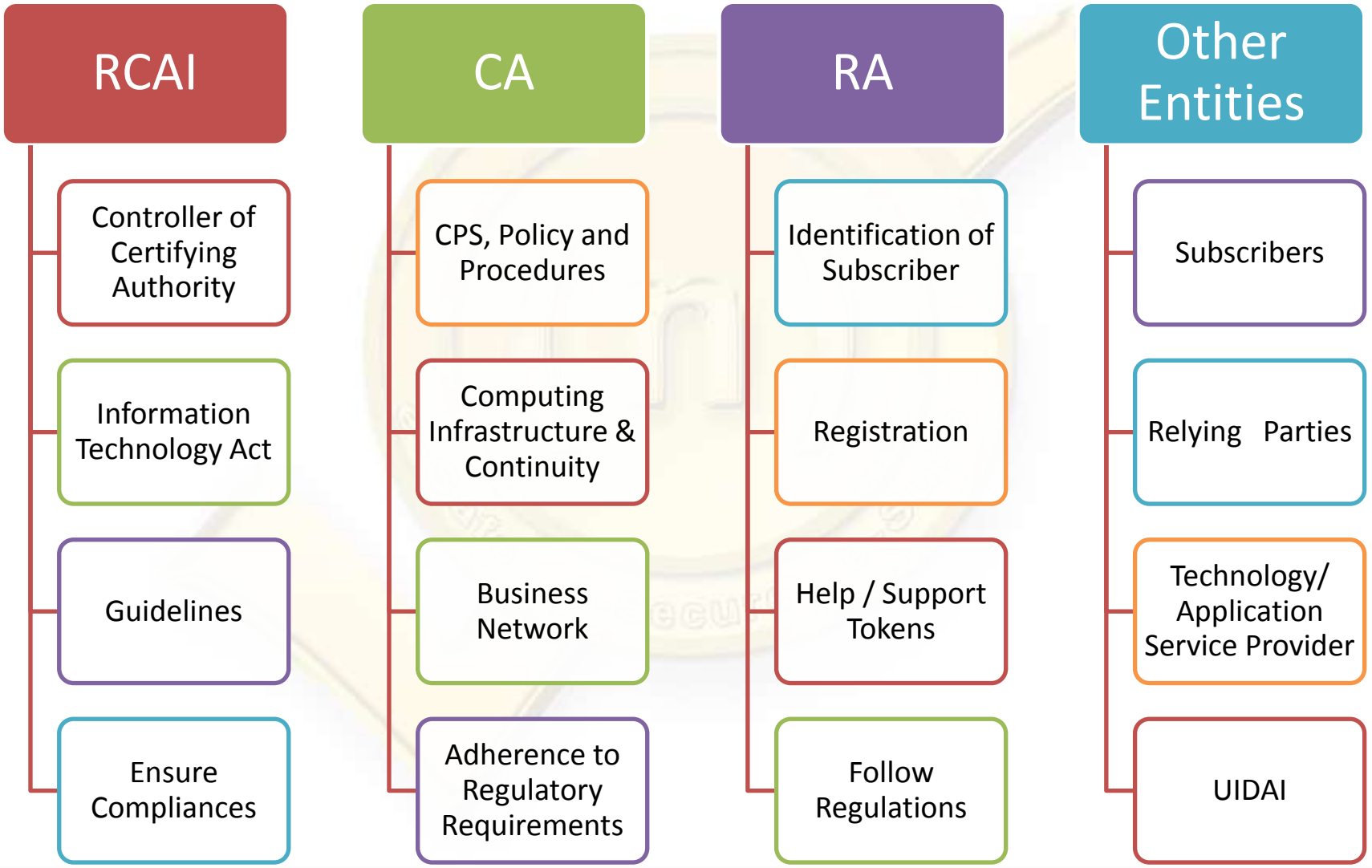
# (n)Code Solutions – As a CA

- **Public Key Infrastructure**
  - Digital Signature Certificates (DSC) as per IT Act
  - eSign
  - PKI Enabled Applications and Components
  - Time Stamping & OCSP services for SSL certificates
- **e-Tendering and e-Auctioning**
- **Projects and Consulting for**
  - e-Security and e-Surveillance
  - Comprehensive e-Governance Solutions
- **Others**
  - Software Applications
  - IT / ERP Consultancy, Implementation and Audits
  - Datacenters Creation and Operations

# Protecting Transactions using PKI

- **Public Key Infrastructure**
  - IT Act exists in India since 2000 and Technological Support for PKI
  - Over a period, Secure DSC issuance process is in place
  - Inter operating Guidelines help standardizing PKI enablement of applications
  - It is mostly end user who pays for procuring DSC benefitting Relying Parties
  - With introduction of e-Sign Relying party may start paying for transaction security
  - ECC Signature will process transactions faster and need lower storage
- **Relying Party Advantages**
  - Relying parties provides PKI enabled application to accept data with authentication
  - Use SSL for secure tunnel from Server to Client
  - Use Code Signing certificate to download PKI component or S/w version
  - Stores data in a secure method and ease of Audits
- **Information**
  - Eco system exists for PKI enablement including end users
  - Normal certificates are stored on FIPS certified devices (HSM, Crypto Token, Smart card)
  - Most common format used for documents is PDF and it supports e-Sign, Time Stamping

# PKI Ecosystem



# Certificate Details

**DSC**

- Class 0 Issued for Testing, Class 1 Issued for e-Mail Security
- Class 2 Issued w/o physical presence, less assurance
- Class 3 Issued with physical presence, higher assurance
- Class 2 and Class 3 DSC are issued on FIPS certified Crypto Devices
- Certificate validity can be for 1, 2 or 3 years [Separate Sign & Encryption DSC]

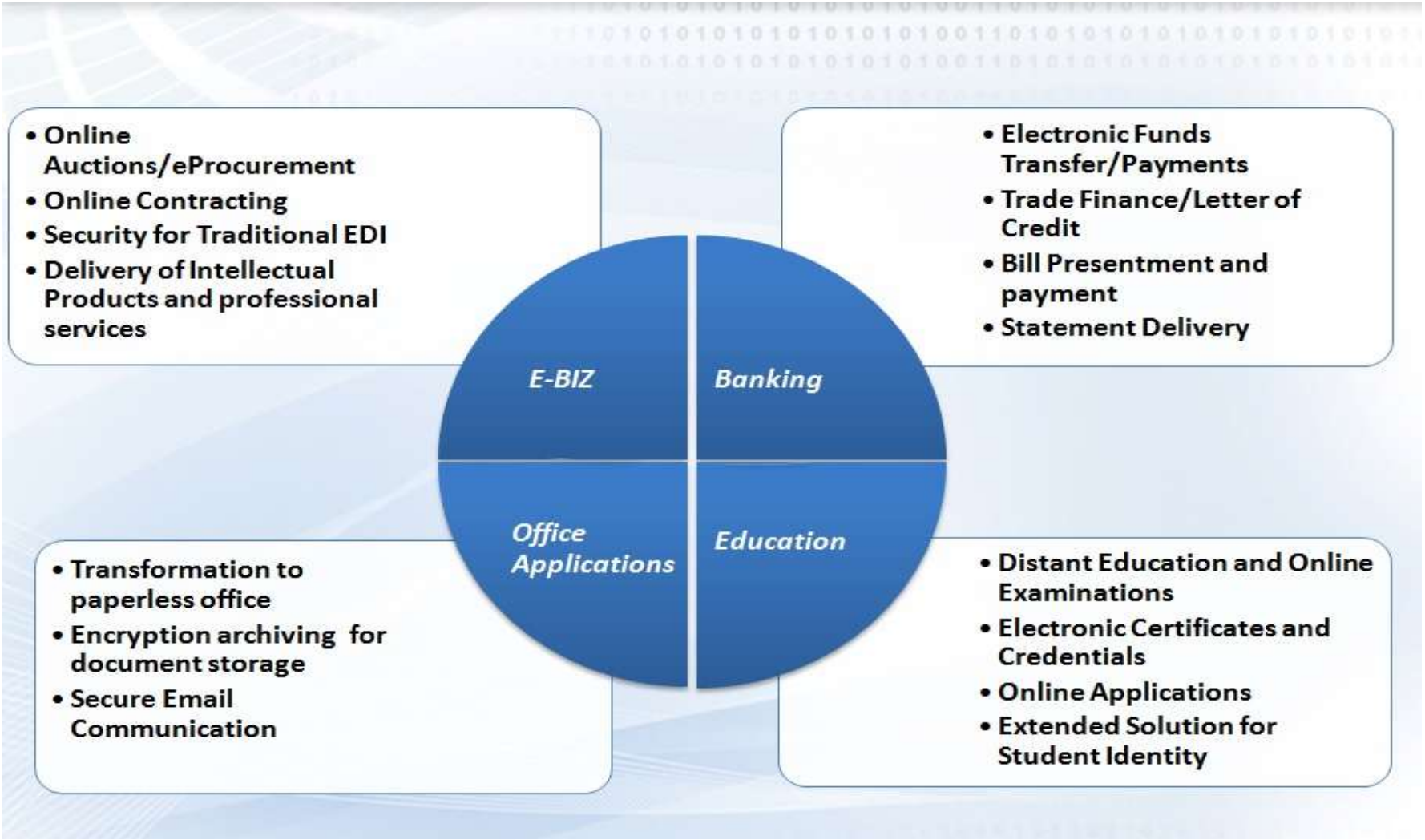
**SSL**

- Class 2 Certificate issued in soft form
- Class 3 Certificates Issued on Hardware Security Module
- OCSP services

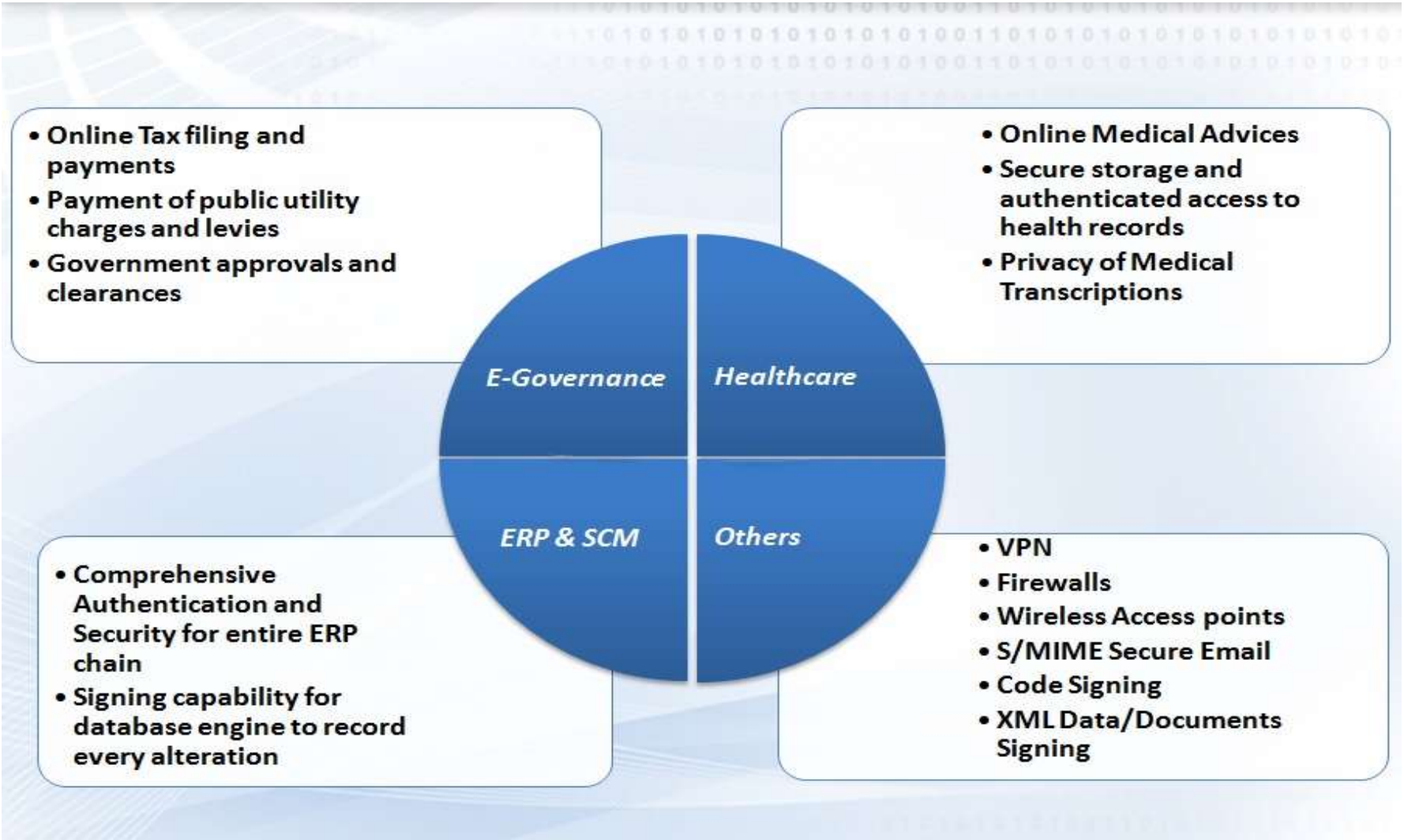
**Special Certificates**

- Code Signing Certificates
- Document Signer Certificates
- Time Stamping

# PKI - Potential Usages



# PKI - Potential Usages



# Challenges

- India PKI is still at a fledgling stage
- To reach at paperless computing more efforts and initiatives are required by
  - Governments, Financial Institutes, Corporates
- UIDAI to improve authentication services
- Mobile PKI is still out of reach
- RCAI to get listed in major browsers
- Lack of Awareness & fear among the end users
- Low understanding on Judiciary processes for PKI

# PKI Enablement

- Basic Requirements
  - Identify toolkits, API as per platform requirements
  - Download Trust Chain and Verify Thumbprints
  - Identify allowable OID and build assurance level
  - Verify Trust Chain
  - Schedule CRL download, thumbprint verification
  - Storage of CRL, Hash, Thumbprints, logs, TimeStamp, for records, archival and Audit

# PKI Enablement …

- DSC Validation Requirements
  - Start Upward from End Entity Certificate in Chain
  - Validate thumbprint of all Certificates in the chain
  - Validate all certificate attributes Published by CCA
  - Validate Issuer Name and Subject in Trust Chain
  - Validate Server Time within validity of certificates
  - Validate Certificate Revocation Status using on-line CRL, OCSP as appropriate

# PKI Enablement …

- Application Architecture
  - Segregate Modules / Programs / Data
  - Provide for Administrative interface
  - Calculate database space and computing power
  - Identify Critical Data / Requirements for Signing and Encryption
  - Generate appropriate logs and ensure security
  - Test implementation prior to shifting the solution to production environment

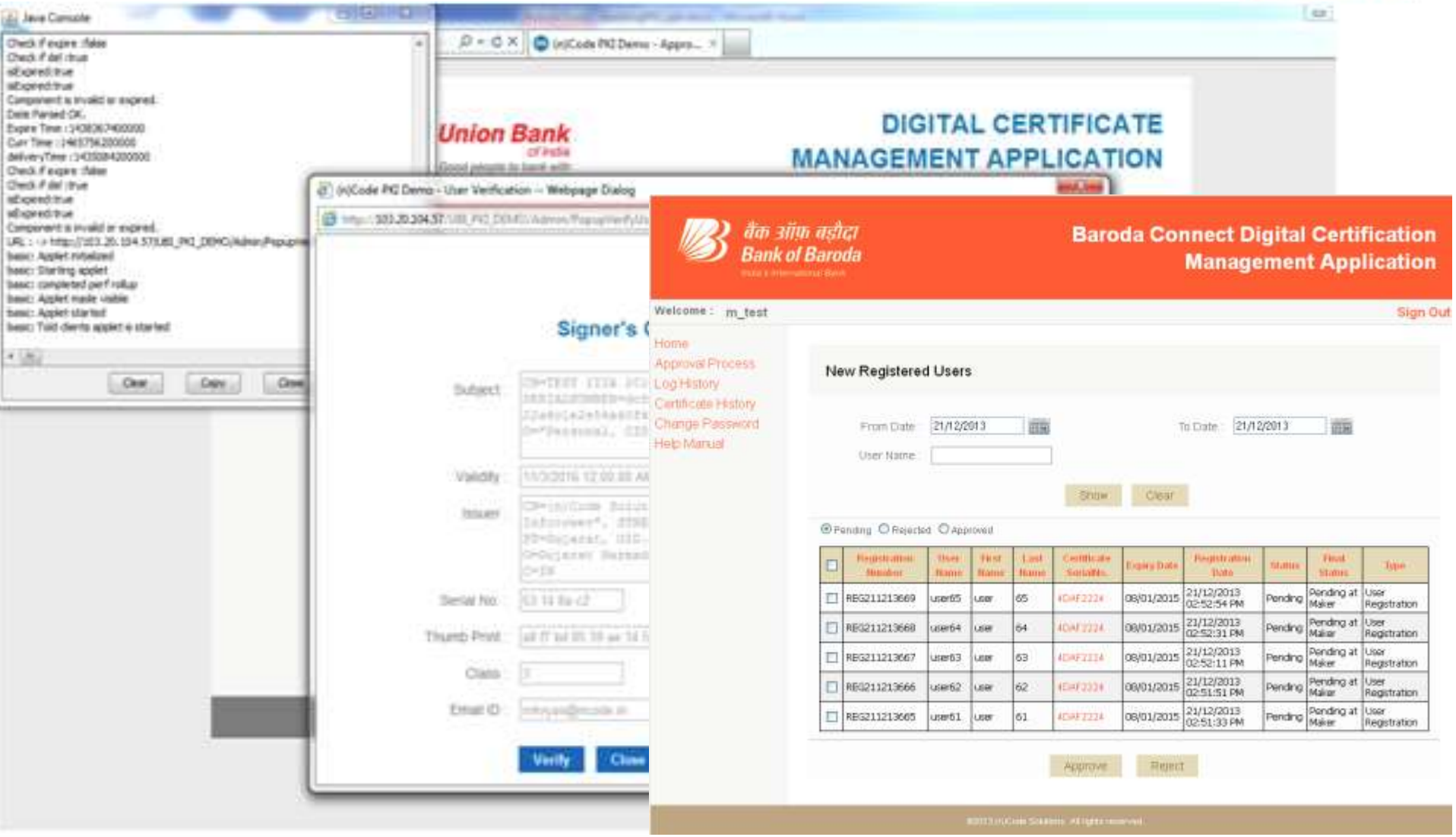
# PKI Enablement …

- **Best Practices**

Considering present guidelines issued by the office of CCA and validations done by Certifying Authorities while issuance of DSC :

  - Start using e-mail from the DSC and do not accept manual or separate e-mail id while registering users and communicate using such e-mail id
  - Take mobile No. from user and verify its hash available in the DSC instead of asking it separately and not validating
  - Validate or take Organization name from DSC instead of taking it separately
  - Take OCSP or CRL path from the certificate and validate on-line CRL instead of local CRL validations by applications and downloading CRLs periodically

# PKI Enablement …



# Applications

- PKI enablement in
  - e-Procurement
  - e-Auctions
  - Banking Applications
  - Work Flow
  - Form Signing
  - Citizen Centric Applications (e-Sign)
  - Server to Server authentication

# PKI Advantages - Banks

- Banks can act as RA for Certifying Authorities and issue DSC to atleast own customers
- 3 year validity certificates reduces per transaction costs
- Use SSL from Indian CA with OCSP services. India Root being trusted in many Browsers
- Complete DSC Authentication solutions are available, which requires least changes in present Application, allowing Banks to implement PKI easier and faster
- ECC signatures will process transactions faster, lower storage
- Use Time Stamping services as per IT Act
- Use e-Sign for; Opening New account, FD, 15G/15H forms
- Organizational e-Sign also available for ease of Net Banking
- Become associate member with India PKI Forum

GNFC

(n)Code Solutions
e-Safe . e-Secure . e-Sure .


# Thank you

Girdhar Varliani gmvarliani@ncode.in 9327056796