PKI enabled e-Procurement with PG integration

National Conference on Digital Signature & Public Key Infrastructure (PKI)

PKI enabled e-Procurement with PG integration

Srinivasa Raghavan K

National Informatics Centre

17th June 2016

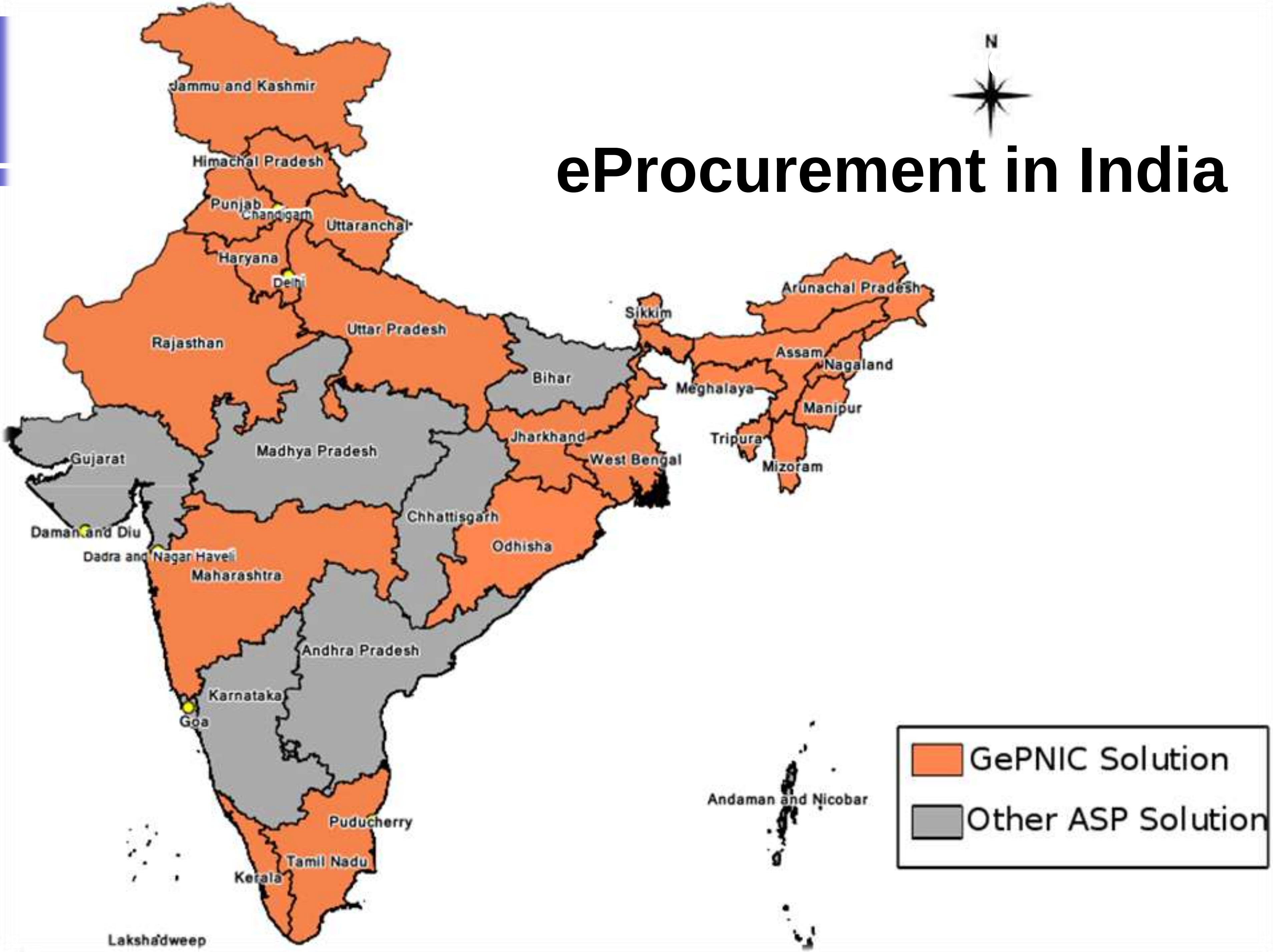
Procurement Background of India

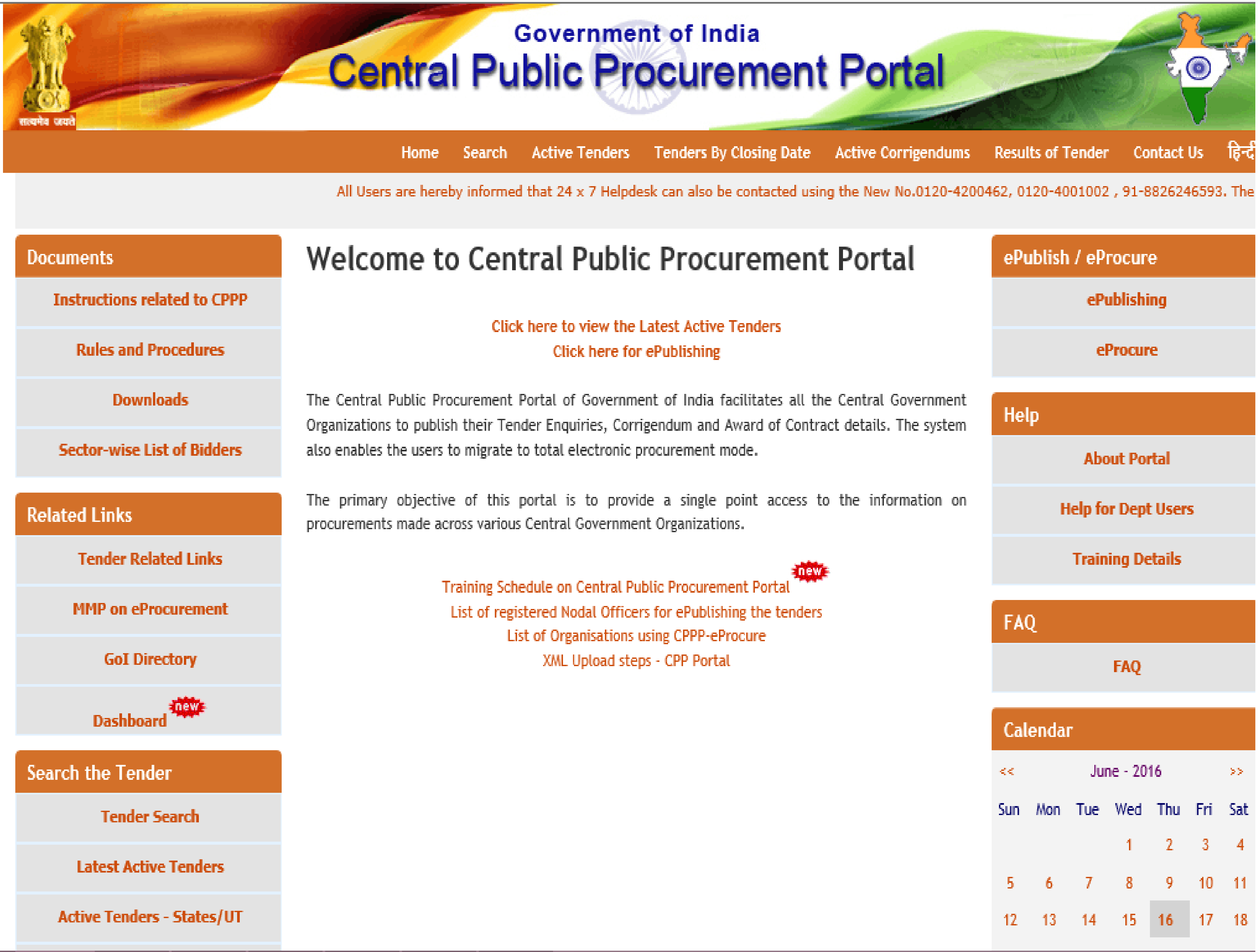
- Defined by the Principles of General Financial Rules(GFR) of the Government of India
- Process Guidelines enforced by Central Vigilance Commission (CVC) to ensure that free and fair procurement process is in place
- eProcurement Initiated from– Govt of Andhra Pradesh (2003), Indian Railways (2005), Govt of Karnataka (2007), National Informatics Centre, Deity (2008).
- Procurement is one area where large percentage of money is spent across Central / State Government.

Background of NIC eProcurement

- National Informatics Centre developed **e-Procurement system (GePNIC)** to facilitate electronic tendering by any Central /State Government / Public Sector Units of India.
- Standardized templates, Configurable workflows, Item Codification, XML interchange of data, Role based access.
- **Completely on Open Source technology** i.e Linux , Apache Tomcat, Postgres SQL Database, Front end-Java Enterprise Environment (JEE) etc
- **Presently deployed in 40 instances and used by -**
  - 27 States / Union Territories under Mission Mode Project
  - 200+ Central Government Organisations
  - Total of around **13,94,547 e-tenders** worth **Rs 19,85,196 Cr**. Processed till May 2016.

eProcurement in India





All Users are hereby informed that 24 x 7 Helpdesk can also be contacted using the New No.0120-4200462, 0120-4001002 , 91-8826246593. The

Welcome to Central Public Procurement Portal

Click here to view the Latest Active Tenders
Click here for ePublishing

The Central Public Procurement Portal of Government of India facilitates all the Central Government Organizations to publish their Tender Enquiries, Corrigendum and Award of Contract details. The system also enables the users to migrate to total electronic procurement mode.

The primary objective of this portal is to provide a single point access to the information on procurements made across various Central Government Organizations.

Training Schedule on Central Public Procurement Portal new
List of registered Nodal Officers for ePublishing the tenders
List of Organisations using CPPP-eProcure
XML Upload steps - CPP Portal

<< June - 2016 >>

Sun	Mon	Tue	Wed	Thu	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18

Benefits for Procuring Entities

- Induces Greater Transparency
- Shortens Procurement Cycle
- Economical / Saves money
- System aided Evaluation process
- Automated Process to a greater extent
- On the fly Reports / Comparative statement
- Integrity and Authenticity ensured due to Digital Signing of all docs
- Improvement in work culture in the departments
- Reduces Litigation / Complaints

Benefits for Suppliers / Contractors / Bidders

- Free of cost registration & participation
- Anytime & Anywhere Bidding – Anonymity ensured
- Fully Secured and Standardized process
- Automatic Tender alerts and Status alerts
- Zero Administrative hassles
- Can carry out all activities from any computer
- Economical – savings on cost of bidding
- Reduces efforts in bid preparation
- Can submit / resubmit bid till last minute
- Transparency at each stage

Product Features -NIC eProcurement System

- Adhering to PKCS 7 format standards as per CVC Guidelines
- Scalable infrastructure, can address dynamic growth
- Web Based & Easy to Use
- Secured Hosting facility , Web security- SSL technology
- Audit trail of each activity, Time stamping of all events.
- Replication of data & backup facility with Disaster Recovery
- Completely Role based Access implemented
- SaaS Model
- Security audited by Standardization Testing & Quality certification (STQC) and various other CERT-IN agencies

Authentication Mechanism in GePNIC

- User registration - Bidder and Department Users.
- Two factor Authentication including PKI.
- During registration the login ID is checked for uniqueness
- Valid Class 2 or Class 3 DSC under CCA India needed
- One User – ID - One DSC
- Once the DSC is attached, the Public Key details of the DSC is stored against this user.
- Signing certificate is registered first then encryption.
- Can be procured from any CAs – all are integrated

Secured Bid encryption

System extends **Public Key Infrastructure** (’PKI’) at its very core for making secured bidding process compliant with Indian Information Technology Act 2000.

- The *signed bid* document is encrypted by random symmetric key and equivalent hash value is generated.
- This random key is encrypted using bid openers public keys.
- This will ensure such that these keys can be decrypted only with the bid openers private key which resides on their tokens.
- To make it tamper-evident, system generates hash values against each stage and verifies before decryption.
- This will ensure an accidental or intentional change to the bid document, including opening/viewing the data, will change the hash value.

This "hash value" is analogous to a fingerprint of an individual being unique to that person.

Online PG Integration

Organisation	Online PG
Mahanadi Coalfields Ltd	Axis Bank with NEFT
Govt. of Kerala	SBT with NEFT
Govt. of Maharashtra	SBI with 55 Banks
Indian Oil Corp Ltd	ICICI with 50 Banks & NEFT
Govt. of West Bengal	ICICI with 50 Banks & NEFT
Govt. of Puducherry	SBI with 40 Banks
Govt. of Uttar Pradesh	SBI with 55 Banks
Govt. of Punjab (PWD)	SBI with 55 Banks
Coal India Limited	Axis Bank with 55 banks

Whats Is Unique in eProcurement PG

Unlike Other Utility Payments, the difference in eProcurement Payment is vast.

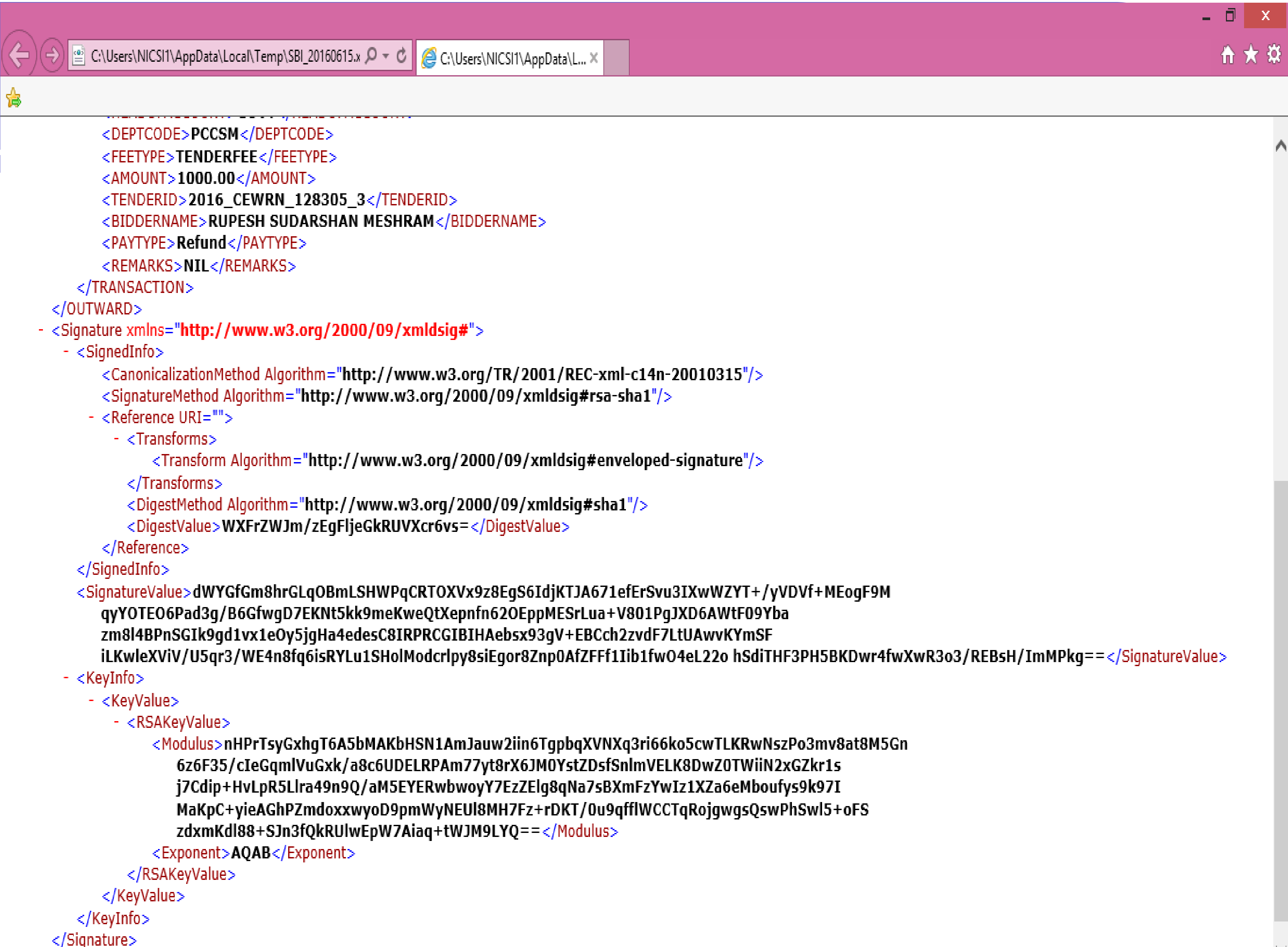
- Complete Secrecy of the Bidder and the participating tender to be maintained till Bid Opening.
- The Fee Collected include Tender Fee and Earnest Money Deposit (EMD) and other fees if any.
- The Tender Fee is deposited in to the Government Account. .
- The EMD is pooled and managed as per the Acceptance / Rejections of the Bid.
- If rejected, the EMD is refunded automatically to the bidder. Otherwise deposited in Govt. Treasury / Account
- The Entire transaction between banks are completely encrypted to reassure secrecy of the Process.

eProcurement Business Requirement

- EProcurement system will refund both tender fee and EMD fee if tender has been cancelled / retendered before technical opening.
- EProcurement system provides option to forfeit EMD as a settlement process for defaulting bidders.
- EProcurement system generates a consolidated refund & settlement XML file as an EOD activity.

eProcurement Business Requirement

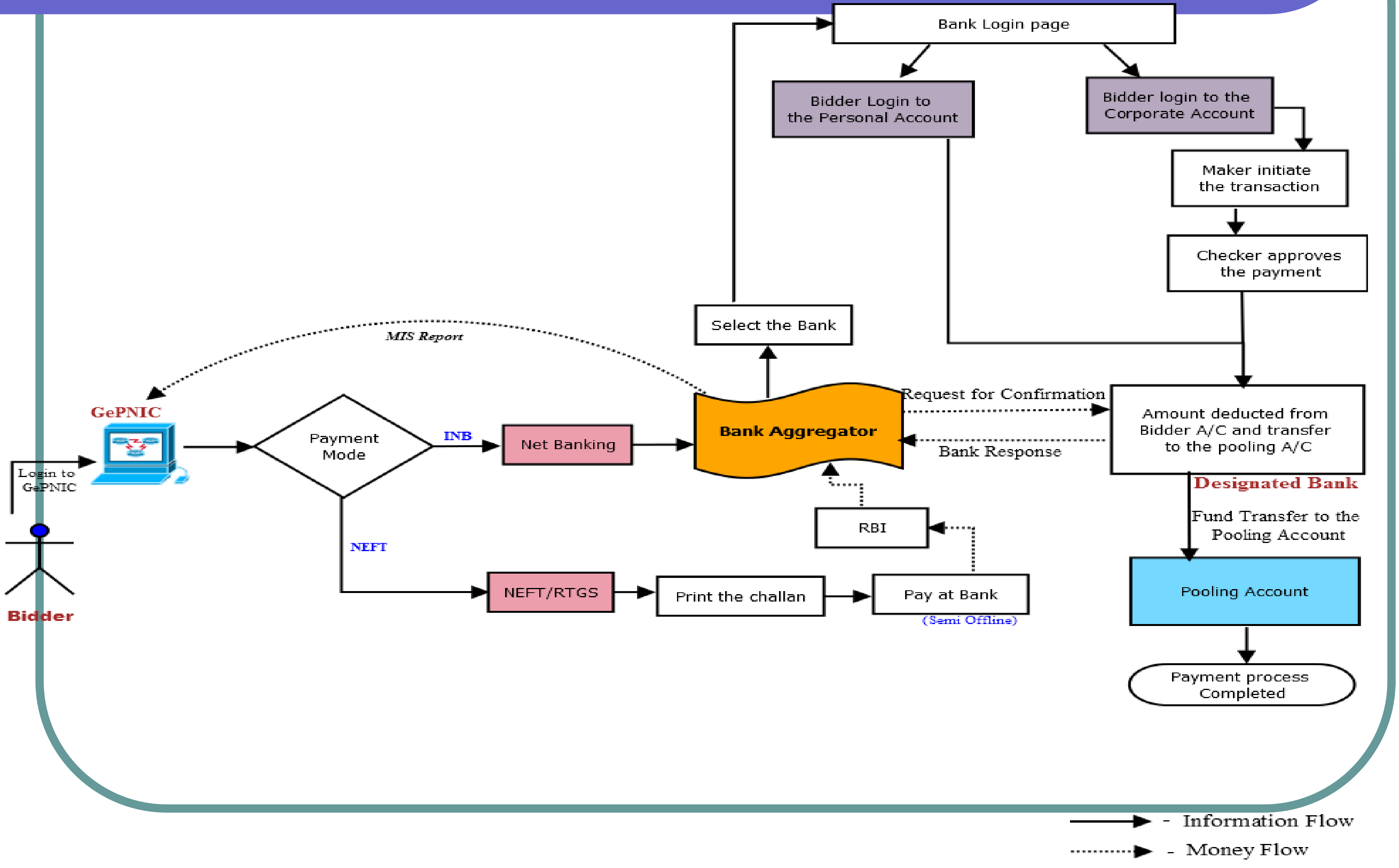
- This file will have the list of transactions with breakup of tender fee, department ref. no. in case of settlement and transaction ref. No. in case of refund (Bank system identifies the source and destination with this eprocurement reference number) the same will be hashed / encrypted.
- In case of settlement, bank system will credit tender fee in concerned Department account.
- Forfeited EMD will be transferred to concerned department account.



C:\Users\NICSI1\AppData\Local\Temp\SBI_20160615.x
C:\Users\NICSI1\AppData\L...

```
      <DEPTCODE>PCCSM</DEPTCODE>
      <FEETYPE>TENDERFEE</FEETYPE>
      <AMOUNT>1000.00</AMOUNT>
      <TENDERID>2016_CEWRN_128305_3</TENDERID>
      <BIDDERNAME>RUPESH SUDARSHAN MESHRAM</BIDDERNAME>
      <PAYTYPE>Refund</PAYTYPE>
      <REMARKS>NIL</REMARKS>
    </TRANSACTION>
  </OUTWARD>
- <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  - <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    - <Reference URI="">
      - <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>WXFrZWJm/zEgFljeGkRUVXcr6vs=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>dWYGfGm8hrGLqOBmLSHWPqCRTOXVx9z8EgS6IdjKTJA671efErSvu3IXwWZYT+/yVDVf+MEogF9M
      qyYOTEO6Pad3g/B6GfwgD7EKNt5kk9meKweQtXepnfn62OEppMESrLua+V801PgJXD6AWtF09Yba
      zm8l4BPnSGIk9gd1vx1eOy5jgHa4edesC8IRPRCGIBIHAebsx93gV+EBCch2zvdF7LtUAwvKYmSF
      iLKwleXViV/U5qr3/WE4n8fq6isRYLu1SHolModcrlpy8siEgor8Znp0AfZFFf1Iib1fwO4eL22o hSdiTHF3PH5BKDwr4fwXwR3o3/REBsH/ImMPkg==</SignatureValue>
  - <KeyInfo>
    - <KeyValue>
      - <RSAKeyValue>
          <Modulus>nHPrTsyGxhgT6A5bMAKbHSN1AmJauw2iin6TgpbqXVNXq3ri66ko5cwTLKRwNszPo3mv8at8M5Gn
            6z6F35/cIeGqmlVuGxk/a8c6UDELRPAm77yt8rX6JM0YstZDsfSnlmVELK8DwZ0TWiiN2xGZkr1s
            j7Cdip+HvLpR5Llra49n9Q/aM5EYERwbwoyY7EzZElg8qNa7sBXmFzYwIz1XZa6eMboufys9k97I
            MaKpC+yieAGhPZmdoxxwyoD9pmWyNEUl8MH7Fz+rDKT/0u9qfflWCCTqRojgwgsQswPhSwl5+oFS
            zdxmKdl88+SJn3fQkRUlwEpW7Aiaq+tWJM9LYQ==</Modulus>
          <Exponent>AQAB</Exponent>
        </RSAKeyValue>
      </KeyValue>
    </KeyInfo>
  </Signature>
```

Payment Flow – Online PG



Challenges faced……..

- ✓ **e-Payment Related :**
  - Adoption in Government – Issues in Wide scale and uniform adoption of e-Receipts/ e-Payments in Government
  - Gateway Integration – Diverse Gateway Interfacing Requirements. No off the shelf software to meet the eProcurement need.
- ✓ Digital Certificates (DSCs) Related:
  - ✓ Applet Support for DSCs from Browsers includes security vulnerabilities. To over come this, Signed Applets are used.
  - ✓ Implementation related – CCA has issued instructions to issue DSC only in Hard tokens which will be supporting to better secured use of the system

Way Forward

- Inclusion of eSign for Signing of Documents
- Provision of Multiple Aggregators in ePayment
- Mobile App for instant Status updates

Thank you