E-Procurement

Technological Challenges In Implementation of

e-Procurement

It is a continuous process as

With time we have to cope up with the technological changes

The Greatest Challenge

Difference between

- Few Zeros with enabled one (AP Case)
- Many Zeros with disabled one

“Clarity in leadership and vision will overcome all the challenges including technological.”

Technological Challenges

- eProcurement comprises of
  - Supplier Registration
  - Indent Management
  - E-Tendering
  - Catalogue Management
  - Contract Management
  - E-Auction
  - E-Payment
  - Accounting
  - Management Information System

eProcurement Users

For a successful implementation of project it will be mandatory to address the requirements of following

- Supplier
- Government Departments
- IT People within department
- System Solution Providers
- Banks/ Payment Gateways
- Citizens
- Cyber Cafe

Sources of Challenges

- Various users of the system
- Hackers
- Threat from Within the System
- Continuous Change in Technology (Obsolete resources)
- Threat from Disasters

Source of Challenge	Objective	Mechanism	Possible Challenges
Supplier	To Place Bid	Own PC Cyber Café	▪IT Literacy ▪IT Infrastructure ▪Connectivity ▪Virus Infection ▪Digital Certificate
Government Department	Transparency & Integrity of the Transactions and Process	Solution chosen (PPP, In-house, Hybrid etc.)	▪Resistance to Change ▪Lack of Policy and Procedures ▪Lack of involvement from all corners ▪Lack of Trust in the system ▪Integrity of individuals involved in the system.

Source of Challenge	Objective	Mechanism	Possible Challenges
IT People Within Department	Smooth running of entire eProcurement system	Data base and audit trail management	▪Compromise with Data Integrity
System Solution Provider	Provide solution/ support	Development of application	▪Bugs in application ▪Platform dependence ▪Support limited users ▪Continuous support

Source of Challenge	Objective	Mechanism	Possible Challenges
Threat from Hackers	To sabotage the system with malified intensions	Continuous R & D to break the system using SQL injections etc.	▪Vulnerability in OS & Protocols ▪Improper network implementation ▪No regular security audit of network and application
Change in Technology	Switch to latest technology if required	Replacement/ up gradation	▪Obsolete technology ▪No Support for existing technology ▪Scalability
Threat from Disaster	Unavoidable circumstances	Natural Calamity	▪Lack of alternate solution

Addressing Challenges

Strengthening Infrastructure

- Penetration of PC’s down to Panchayat level
- Connectivity down to Panchayat level
- Computer Awareness among people/Expected Users
- Conduct training on product and technologies

Authentication and Security

- Maintenance of Data Integrity
  - Audit Trail Log should be different from OS logs
  - Access control log should reside at different locations
  - All actions and system events should be logged and monitored continuously in order to keep track of changes, in terms of security and in order to provide statistical report to concerned authorities.
  - Access control logs should be accessible to 2-3 representatives of Government
  - Bid Process Committee should have multiple encryption keys with different committee members
- Authentic Audit Trails
  - Network Time Protocol – Should use some global server for time stamps.
- Use of digital signatures to ensure Non Repudiation
- Bid encryption at database level

Digital Signature

Timely availability of Digital Signatures

- Keeping in mind the demographic conditions of HP, support for Class 2 in addition to Class 3 certificate should be admissible

- Being a smaller state maximum 2 Sub CA's in a State – One to cater major department like PWD and the other for all other miscellaneous departments

Technology to be adopted for Digital Certificate Issuance

- USB token should be provided to the applicant so that he apply from any where without installing certificate on m/c

Interoperability

- Application should be platform independent (at client end)
  - Microsoft is used widely but prone to security threats
  - Open source is more secure but application becomes kernel dependent
  - Open source has support related issues
- Solution provider should take care of heterogeneous environment at client end
- PKI control should be made available all platforms i.e. Linux, Windows etc.

Other Challenges

- Multiple Payment gateway option (2 to 3 different channels).
- Should support certificates issued by Multiple CCA’s
- The application should be scalable.
- Off Site backup to take care of Disaster
- Stand By servers to cater breakdown