सत्यमेव जयते

eDistrict

Mission Mode Project

Under the

National eGovernance Plan

Implementation Guidelines

DEPARTMENT OF INFORMATION TECHNOLOGY

GOVERNMENT OF INDIA

TABLE OF CONTENTS

1. Terms & Definitions

2.1 National e- Governance Plan (NeGP): Although, a number of e-Governance projects have been undertaken through individual initiatives, for the first time a programmatic approach is being adopted while implementing various e governance initiatives at the Central, State and Local Government level under the National e Governance Plan (NeGP). The NeGP , which was approved by the Government in May 2006 consists of 27 Mission Mode Projects (MMPs) and 8 components Implementation of such a Plan requires buy-in from diverse stakeholders such as central ministries/departments, state governments, local government bodies, private sector agencies and citizens. The focus of the NeGP is on delivery of services to citizens in an efficient and transparent manner at affordable cost to the citizens. The NeGP envisages the creation of certain core and support infrastructure which would web enable services for anytime anywhere access and thereby radically change the way Government delivers services. The support and core infrastructure are:

2.2 Common Services Centres (CSC): The CSCs would be the physical front ends for delivery of services to citizens. The Government has already approved a Scheme for facilitating the eestablishment of 100,000+ broadband Internet enabled Common Service Centers predominantly in rural areas, with an equitable geographical spread. These centers would enable rural citizens to access the various e- government & private e-services at their doorstep and the Scheme is currently being implemented through a Public Private Partnership. Setting up such a huge delivery mechanism requires unprecedented network and application/data support.

2.3 State Wide Area Networks (SWAN): State Wide Area Networks are being setup to provide 2 Mbps connectivity up to block level with provision for wireless connectivity from the block level to the village level.

2.4 State Data Centers (SDC): State Data Centre (SDC) has been identified as one of the important element of the core infrastructure for supporting e-Governance initiatives of National governance Plan (NeGP). SDC would help States to consolidate services, applications and infrastructure to provide efficient electronic delivery of G2G, G2C and G2B services and would provide better operation & management control

National E-Governance Service Delivery Gateway

This mission project aims at setting up a National gateway called NSDG for standards based messaging between heterogeneous applications. A cluster of Gateways would be setup across the country which will be an integral part of the SDCs to ensure standards-based interoperability between the various departmental applications at the back end and connect the CSCs or other delivery channels at the front end. Acting as a nerve centre, the gateways would handle large number of transactions across the entire network; provide a common set of specifications and a single point access for departments. Such an infrastructure would also help inter-departmental working in a co-ordinated and synchronized manner. As a central message processing mechanism it would also help in tracking all transactions of the Government.

.**2.5 Mission Mode Project (MMP):** Under the NeGP 27 projects, have been identified which are to be implemented in a mission mode. Implementation in Mission Mode implies that the objective and scope of the projects would be clearly defined, they would have measurable outcomes (service levels) and they would have well defined milestones and timelines for implementation.

2.6 State MMPs: State MMP under NeGP refers to those MMPs for which the Nodal Central Line Ministry/ Department would frame the broad policy guidelines and facilitate project formulation but the actual implementation would be done at the State level and the State would be the ultimate owner of the project.

3. e-District

3.1 e-District is a State Mission Mode Project under the National e-Governance Plan. The Project aims to target certain high volume services currently not covered by any MMP under the NeGP and undertake backend computerization to e enable the delivery of these services through Common Service Centers. The implementation strategy of e District would suitably take into account the infrastructure currently being created under NeGP such as the SWANs, SDCs, CSCs and State Gateways

Services

Citizen centric services listed by the State under the Project, whose backend is to be taken up for enabling content development for delivery through the CSCs.

District Administration

District Administration in the context of eDistrict refers to the administration set-up led or coordinated by the District Collector / Magistrate including Subdivision / Tehsil / Block / Village level units responsible for delivery of services and information. For the purpose of services coverage under eDistrict, government services like passport etc which are purely and exclusively administered through the line department directly, should not be considered.

Back-end

The departments, which are involved in delivering a particular service, form the back end for the service. In case where the backend is partly digitized and electronically enabled with a combination of manual intervention, such a backend would be a Hybrid Back-end.

Business Process Reengineering (BPR)

Business Process Re-engineering is a critical content of the Project. In addition to delivering the services electronically (which are presently delivered physically and manually), the project aims to add value to the services by ensuring service levels. Adherence to service levels will be enabled through a detailed assessment of the present systems and processes, and redesigning of the same through BPR. The redesigning may or may not involve legislative amendments to the present set of rules and processes. The extent and feasibility of BPR will have to be decided by the State. The BPR Model adopted in the pilot district subject to refinement shall be uniformly applicable across the State.

Service level

The service level is defined as the time taken in the delivery of a particular service. Defining the service level would entail stating the present time taken for the service to be delivered manually, and prescribing the time which would be taken for the service to be delivered either electronically or manually subsequent to the execution of the project. The State shall prescribe the service level for each of the services identified under the project.

Standardization and interoperability

The application development should be based upon open standards – the application should be capable of running in multiple operating system and database. All application development needs to support n-tier (thin/thick client) architecture and should be based upon service oriented architecture.

Please refer to the annexure X on the interim report on Standards for e-Governance.

1. BACKGROUND

1.1 Government of India has recently approved the National eGovernance Plan (NeGP) in pursuance of its policy of introducing e-Governance on a massive scale, as enunciated in the National Common Minimum Programme. The NeGP vision aims to "**Make all Government Services accessible to the common man in his locality, through common service delivery outlets and ensure efficiency, transparency and reliability of such services at affordable costs to realize the basic needs of the common man**".

1.2 To realize this vision, 27 Central, State and Integrated Mission Mode Project (MMPs) along with 8 support components have been identified and approved by Cabinet under NeGP, to enable and facilitate rapid introduction of e-Governance in the country, with focus on service delivery. As per the implementation strategy, an identified line Ministry/Department would define the service and service levels of their respective MMPs and develop detailed guidelines for achieving the same.

1.3 For delivery of "web-enabled" anytime anywhere access to information and service across the country, NeGP envisions 3 pillars of eGovernance infrastructure. These are **State Wide Area Networks** (SWAN), **State Data Centre** for secure and fail safe data storage, and **Common Service Centers** (CSCs) as the primary front-ends for service delivery. XML based middleware Gateway infrastructure at the SDCs is also critical for the delivery of e-services.

1.4 eDistrict, is 1 of the 27 Mission Mode Projects under NeGP under the Department of IT, GoI. eDistrict aims at providing support to the basic administrative unit i.e. "District Administration" to enable content development of G2C services, which would optimally leverage and utilize the three infrastructure pillars, to deliver services to the citizen at his doorstep.

2. EDISTRICT - OBJECTIVE

2.1 The objective of the MMP is to target certain high volume services delivered at the District level, but which are currently not covered by any MMP under the NeGP, and undertake backend computerization to e enable the delivery of these services through Common Service Centers in a sustainable manner, within a specific time frame.

2.2 The scheme has been formulated on the premise that

a. Districts are the primary unit for delivery of bulk of the citizen services

b. Quality and content of Government Service Delivery can significantly improve with an integrated approach to service delivery.

c. Capacity building of the district administrative functions and processes will enhance efficiency and accountability in service delivery.

d. The services which would be delivered would have automated work flow and would perforce involve significant process redesign.

e. A Central data repository would be created at the district level, wherein data and information would be collected, stored, retrieved, used and exchanged in an efficient manner at all levels.

f. Enabling backend computerization for delivery of G2C services will ensure optimal leveraging and utilization of the core and support infrastructure such as Common Service Centers, State Data Centre, Statewide Area Network and Service Delivery gateway at the SDCs.

3. EDISTRICT – COVERAGE AND SCOPE

3.1 The scope for the Project is to be defined with reference to the set of services of the district administration that would be taken up under the Project.

3.2 The eDistrict Scheme focuses on **e-enabling the delivery of majority of citizen centric services**, that are administered by the District Administration.

3.3 **Timelines**: The scheme will be implemented in two Phases:

a) In **Phase I** Pilots would be undertaken covering 1-2 Districts of a State and

b) In **Phase II** the Project would rolled out across the State subsequent to successful implementation of the pilot.

c) Phase I would be completed within 18 months from the date of approval of the pilot project report. Phase II will be completed within 2 years from the date of sanction of statewide roll out.

3.4 The first step in the implementation of the eDistrict MMP (Phase I) would be to identify the pilot district and finalize the list of services that are be taken up under the Project.

3.5 It is proposed that a minimum of six (6) services to a maximum of ten (10) services can be undertaken under this Project.

3.6 A core list of six services have been identified at the national level which shall be taken up for implementation by all States which agree to participate in the e District MMP. The State can also add a further 4 services, at its discretion, for implementation under the MMP. The list of core services may be seen at para 3.9.

3.7 An indicative list of services, from which the States can choose 4 additional services, is at **Annexure I.** It may be noted that the list of services at **Annexure I** is illustrative and not exhaustive and States would be free to add additional services other than those indicated in Annexure I, subject to their meeting the criterion indicated in these guidelines.

3.8 In States where all or part of the of the services in the core list (Para 3.9) have already been e-enabled (data for the same is substantially digitized, workflow automated and the services are provided through an IT front end) by the State, then to that extent, State may select other services, subject to a maximum of 10 service in all.

3.9 **List of Core Services relating to** :

a) **Issue of Certificates** including Domicile, Nativity, Caste, Marriage, Income, Employment ,etc

b) **Pensions –** Social welfare Pensions (Old age, Widow, Handicap, Destitute)

c) **Revenue Court** – including Case listing, Case adjournment, Stay orders, Final orders, Status of execution of orders: Information , Tracking ,filing of misc. applications..

d) **Government dues and recovery** as part of Land Revenue – including Issue of notices, Record payments, Track default processes, Updation of treasury receipts etc

e) **Public Distribution System**, Ration Card related services -including Registration, Change of address, Addition of members, Issue of duplicates etc.

f) **RTI services** including redressal of Grievances – (Application, tracking, monitoring, redressal, appeals etc.).(Education, Electricity, Drinking Water, Panchayats, Health, Police, Revenue, Road, Treasury, Social Welfare, Irrigation, Woman & Child, Public Distribution System, Transport, Disaster Relief….

3.10**Financial**: An approximate amount of Rs.4.00 Crores per pilot district has been earmarked under the scheme. An indicative list of the major heads and their expenditure envisaged is at **Annexure II.**

4. SELECTION OF SERVICES BY THE STATE

4.1 For the eDistrict MMP, the State should consider the following during the process of selection of services under the Project. This would include:

a) **IDENTIFICATION-** identifying exhaustively the services that are rendered at the district level.

b) **LISTING –** Having identified all the services at the district level, listing of these services in order of the demand/volume generated. For this the State may make use of already existing surveys by independent agencies (IL&FS CSC's report, PricewaterhouseCoopers Study on eReadiness, etc.)

c) **AUTOMATION OF BACKEND:**

(i) The selected services are to be classified with reference to the number of line departments involved in delivering the selected service and whether the line department/s is covered under any other MMP under the NeGP such as panchayats, police etc

(ii) High volume services where a single line department is involved in the delivery of the service should be taken up first , preferably for an end-to-end digitization & workflow automation (covering all process points) for effective online delivery of service. In any case, minimally, the service offered under the project must be enabled, to receive requests ,track status and deliver the service online. The backend processes to the extent feasible may be taken up for e enablement.

(iii)For services which involve more than a single department at the backend, the extent of backend digitization and automation may be worked out by the State, taking into account the present e-readiness of the backends, the feasibility of digitization within the project timeline of 18 months and the financial implications of such an effort keeping in mind the total funding available for the Project, as indicated at Para 4.10.

(iv)For services which at the backend would involve computerization of a line department being covered under another MMP of National e-Governance plan, funding under eDistrict would only be made available for providing a minimum interface to the line department with the district administration for activities such as receipt of requests, status tracking and delivery, and general information. *In such cases the backend processing and infrastructure shall be beyond the scope of the present scheme*.

(v) For services that are taken up under eDistrict but where the backend and infrastructure in being funded out of an other project (NeGP or otherwise), it must be ensured that the entire workflow at the point of service fulfillment "citizen end" is automated – and can be integrated with the backend as and when the same is ready.

d) **SELECTION –** From the list so drawn, services to be included in the scope of the e district MMP would be identified by the State based on an analysis of each identified service. The analysis would include considerations such as :

(i) Importance – How important is the service from the citizen's point of view and how sustainable the service would be in the long run, in terms of revenue generation through user charges.

(ii) Potential benefit to Citizen/Government from computerization.

(iii) Ease with which service levels (time bound) for each service can be defined and ease of replication through out the state

(iv) Degree of changes required in existing processes to meet the service level requirements of each of the service (BPR). **[Annexure III** provides an overview of the concept of BPR and the potential benefit from the same].

(v) Ease with which such changes can be introduced, including legal reforms,

(vi) Availability and quality of existing manual/digital data that can be used for online service delivery within a period of 18 months

(vii) Extent of coordination with multiple offices of the State for provision of the service online

(viii) Potential for levying user charges for sustainability of the initiative

5. IMPLEMENTATION STEPS

Listed below are the sequences of steps to be followed in the implementation of the eDistrict MMP.

5.1 Selection of Pilot District

a) The State shall initiate the eDistrict MMP by identifying a pilot district in the State (Phase I)

b) One pilot district in a State would be covered in the Phase I. (In exceptional cases and with proper justification, a maximum of two districts in a state may be considered).

c) Phase I district should be taken up keeping in mind the ultimate objective of State wide roll out.

d) The pilot district/s should ideally represent critical aspects of the State .viz...

(i) Population profile – rural / urban /tribal

(ii) Socio-economic/demographic profile

(iii) Likely stability of district collector and nodal officer during Project phase of 18 Months

(iv) eReadiness of the District (quality of resources available, quality of data, etc) for implementation

5.2 Identification/Notification of State Agencies.

a) Identification of a Nodal Department which would be the Project owner at the state level (IT/Revenue Department).

b) Notification of a State Designated Agency (SDA) and a State Nodal Officer to represent the State and provide all State level support for smooth implementation of the Project. It is preferable that the State eGovernance Society, if in existence, be identified as the SDA for the project.

c) In the event that a State e Governance Society is not in existence, for the Pilot, the State may notify an appropriate Agency as a SDA, however, for the rollout, the State would need to establish a State e governance Society.

d) The State Designated Agency should ideally be a suitable PSU/Society of the State Government. In any event the SDA would have to be empowered to open a separate Bank account and operate the same for the implementation of the e District Project.

e) Formation/Notification of District e-Governance Society (DeGS) as implementation agency in the District/s.

5.3 Preparation of the Project Report (PR)

a) Following the selection of the pilot district(s), and identification of the implementation agency, the State is required to prepare a Project Report (PR) for the selected pilot district/s as per the template enclosed in **Annexure IV.**

b) The State shall have the option to prepare PR on its own or through their own consultants. The DIT has empanelled a set of 5 consultants (list attached at Annexure V) for the e District Project and the State Government may request DIT to assign one of the said five consultants to assist the State in preparing the PR.

c) The PR so submitted by the State would be appraised technically and financially by DIT for approval. For the purpose of the appraisal a soft copy of the project proposal should also be sent to DIT.

5.4 Approval by DIT, GoI

a) Following the submission of the project report to DIT, GoI, the same would be appraised for conformance to the eDistrict MMP guidelines/scheme. Following the appraisal, the pilot project (Phase I) would be accorded administrative and financial approval and the same would be communicated to the State / State Designated Agency for project initiation

b) The issue of administrative approval would be accompanied by release of first installment, which would include an amount of Rs. 10.00 Lakh, as seed money, for activities relating to setting up the DeGS

5.5 Selection of the Implementation Support Agency(ISA)

a) Following the approval of the eDistrict MMP (Phase I), the SDA needs to identify an agency for providing day to day implementation support to the DeGS for undertaking the project.

b) For the purpose of providing implementation support, the DIT, GoI has empanelled five national consulting firms for supporting and conducting BPR and providing end-to-end project implementation consultancy. The list of consultants and Terms-of-reference for Implementation support is given at **Annexure V.**

c) The State may choose any one of the above empanelled consultants who would be assigned by DIT, GoI for the estimated Project period of 18 months.

d) Alternatively, the State may choose to undertake the task of BPR and project monitoring through existing resources/ state agency capable of providing such support for the entire duration of the project i.e. 18 months. In this case the funds for consultants earmarked for the project can be used for engaging its own team and also towards the physical implementation apportioned across funding heads (refer Para 8).

5.6 Finalization of Service Levels and Business Process Reengineering (BPR)

a) In line with the philosophy of NeGP i.e. focus on service delivery with assured service levels, it is mandatory that prior to the start of the actual implementation, the State undertake a comprehensive study of the existing processes for service delivery, to identify areas for improvement across the selected services. (Minimum of six and maximum of 10 – refer to Para 3.5).

b) This improvement would be aimed at achieving service levels for each of the service, to be approved by the State as a standard prior to the actual implementation of the pilot.

c) Irrespective of the choice of implementation support agency as part of the project, the following documents need to be prepared and submitted:

(i) Documentation of the existing process of service delivery across the eDistrict Services

(ii) Existing Services Levels

(iii) Proposed Service Levels, based upon benchmarking / opportunities for improvement

(iv) Identification of Business Process Reengineering requirement to achieve the proposed service levels, including areas where legal changes would be required.

(v) Documentation of To-Be Process maps in line with the BPR proposed

(vi) Cost Benefit Analysis of the proposed changes

d) Implementation of BPR and Change Management are the key components in ensuring the success of eDistrict MMP.

5.7 **Project Implementation**

a) Following the State approval of the service levels and BPR required for implementing , the DeGS would initiate the development of the following documents:

(i) BPR and Change Management Plan

(ii) IT Infrastructure Up gradation Plan

(iii) Procurement and Financial Management Plan

(iv) Site Preparation Plan

(v) Functional Requirement Specifications for the re-engineered Processes

(vi) System Design Document and SRS

(vii) Training Requirement

b) At the same time the SDA would also initiate steps for the identification of a technical partner as the Application Developer, which may be NIC or any other organization – Government or Private.

c) The activities relating to procurement, site identification, preparation, and installation of hardware would have to be simultaneously coordinated by the implementing agencies both at the State and district level.

d) The SDA/DeGS would ensure data digitization of requisite records by within the agreed time frame.

e) The SDA/DeGS would ensure development, completion and successful testing of application software by the Application Developer

f) The SDA/DeGS would ensure end-to-end implementation of the project within the project timeline and cost.

5.8 Independent **Outcome Assessment**

g) Following the total / partial implementation of the pilot project, DIT may appoint a third party to independently assess the outcome of the project in line with the outcome envisaged – detailed in Para 10 of this note.

6. THE IMPLEMENTATION STRUCTURE

6.1 Undertaking eDistrict calls for active participation and close interaction amongst various stakeholders such as State Governments, District Administration, District Level officers (DLOs) of Citizen Centric Service Oriented Line Departments, Field Functionaries, and Local bodies and implementation consultants.

6.2 The 'e-District' Scheme has a 4-tier implementation structure:

a) **Department of Information Technology, Government of India –** to provide funding, enable synergy with MMPs, Empanelment of project consultants, Aggregation and sharing of best practices, provide suggestions on BPR at an all India level, and facilitate the pan-India rollout.

b) **State Government**, the owner of the project would closely work with Department of Information Technology, GoI to provide over all guidance in implementation and monitoring of Project across the State.

The State Government would appoint a high level State Project Committee which would oversee the implementation of the Project at the State level.

c) **The State Project Committee** shall be duly empowered to take decisions on the implementation strategy, process reengineering requirements and make all policy level decisions needed for ensuring the successful implementation of the Project.

d) **State Designated Agency** (SDA) shall be the authority responsible for implementing the Project at the State level.

e) At the core of the implementation structure is the **DeGS**, led by the Collector, which would be responsible for implementing the project supported by the ISA and the Application Developer.

7. ROLES AND RESPONSIBILITIES

7.1 Department of Information Technology (DIT), GoI

a) Frame and Issue Guidelines to the State Governments and District Administration for implementation of ‘e-District’ in the Pilot Districts and State-wide roll out

b) Receive and appraise proposals from the State for Pilot ‘e-District’ implementation

c) To form eDistrict Project Management Group (EPMG) for monitoring the program at national level

d) Provide technical assistance to the State for effective implementation of the MMP

e) Provide empanelled list of consultants for BPR and project monitoring to the State Governments

f) Organizational capacity building

g) Monitoring implementation’, consolidation of BPR, Products, Case studies and etc.

7.2 The State Government

a) The State Government will need to set up a State Project Committee, identify a State Designated Agency (SDA) and a State Nodal Officer to represent the State and provide all State level support for smooth implementation of the 'e-District' Project. A suitable SDA may be appointed, keeping in mind Para 5.2 of these guidelines.

b) Identify the pilot district and approve the project report for taking up the Phase I of the eDistrict MMP

c) Define the services for Pilot 'e-District' implementation as prescribed in the selection criteria

d) Set up a duly empowered State Project Committee (SPC) for overseeing the implementation of the 'e-District' Project.

e) To enter into necessary MoUs/agreements with DIT/other central agencies/service providers for funding, defining service levels for identified services, ensuring service level adherence, implementation and sustainability of the pilot project and subsequent state wide rollout.

f) To identify and nominate the project champion at State (IT/ revenue department) and District level and ensuring complete involvement of the project champion from start to finish of the Project

g) Issue instructions and ensure formation of District e-Governance Society with a District Implementation Committee in the Districts.

h) Provide State Financial Support as per the project report

i) Provide Infrastructure and other support to the State Designated Agency (SDA)

7.3 State Project Committee

a) The SPC would oversee the (creation) and functioning of the District e-Governance Society and the SDA with reference to the 'e-District' Project, including taking decisions on the implementation strategy and oversee the process of selection of the agency for software development.

b) It would be the driver for policy, regulatory and other relevant changes and would take decisions on issues relating to the BPR needs for the Project.

c) It would take an appropriate decision on the mode and degree of integration of the existing physical, digital and institutional infrastructure of various Government Departments as well as the infrastructure created under ‘e-District’, to ensure service delivery through CSCs.

d) Review and approve the sustainability (revenue) model for pilot project and the replication of the same for State wide rollout. This would include decision on fixing of user charges and the sharing of revenue between the District e Governance Society and State e Governance Society etc.

e) Propose the State wide rollout based upon common software, approach and financial model following the completion of the pilot project.

7.3 State Designated Agency

The role of the SDA would primarily be to:

a) Extend necessary policy level support to develop a sustainable framework for regulation, promotion and ramp up of e-platform for G2G and G2C Systems of the District.

b) Synchronize roll out of ‘e-District’ with CSC, SWAN, SDC

c) Detail out implementation strategies, in case of time lag between SDC/SWAN and eDistrict implementation.

d) Coordinate and facilitate interactions between the project implementation partners/consultants, State Government Departments, District Administration

e) Enable creation of a comprehensive State package for ‘e-District’ and other technical support. Facilitate integration of the existing ICT enabled and other Government Schemes into the ‘e-District’

f) Facilitate administrative readiness and e-readiness of the District

g) Facilitate selection of ISA and application Developer under the guidance of State Project Committee / Apex Committee

h) Facilitate fund transfer to the District Authorities in case funds for the pilot project are allocated to the SDA

i) Draw up a comprehensive user charges policy and a sustainable road map for the e district project for approval of the State Government.

7.4 District e Governance Society (DeGS)

a) The DeGS would provide close tie-ups with all the stakeholders in the Project at field level. The stakeholder from the district government would include Collector/Deputy Commissioner, Sub Divisional Officer / Magistrate, Tehsildar / Patwari, Block development officer, and field functionaries

b) Provide commitment and support to bring-in the process changes

c) Provide overall guidance to the Project at District level

d) Work closely with the ISA and Application Developer to undertake the field work, comprehend the requirements, document the observations, prepare roadmap, redesign the processes

e) Build capacity of the staff and executive resources of the district administration. DeGS and ISA would also work closely with the technical solution provider for developing and customizing the software, implement the technical solution

f) To implement guidelines of State Government and Government of India for ‘e-District’, CSC, SWAN, SDC and any other e-Governance Programmes in the District.

g) To manage, supervise and implement backend computerization of Government Departments with long term vision of Government.

h) Coordinate, manage & monitor the receipt & utilization of financial support received from the State Government / Government of India

i) Support the Common Services Centers (CSCs), throughout the District for providing G2C services as per the Service Level Agreements between Departments/ SDA for CSCs and the Service Center Agency. It would identify and recommend the Citizen Services which can be provided in consultation and co-ordination with the concerned departments on priority and assist SCA in roll out of G2C services in CSCs.

j) Collect user charges as fixed by the State Government and keep audited accounts of the same.

k) Take all publicity measures and campaigning through media like TV, radio, newspaper, conferences, seminars, public meetings, banners and posters etc for creating awareness about transformation through e-Governance for the benefit of the rural masses.

l) Initial seed money of Rs 10.0 Lakhs would be provided for the smooth establishment and functioning of the society by way of contribution from Government of India.

m) Explore revenue streams for the sustenance of the District eGovernance Society and assist SDA in formulating policies accordingly.

- .

7.5 National Informatics Centre (NIC)

a) NIC has been providing considerable support to State and District Administration in the design and implementation of eGovernance Initiatives.

b) Given the experience and presence of NIC personnel at District Level, the State/District Administration may choose the services of the NIC in development of the software solution required for online provision of the services selected under the eDistrict Pilot Project. However, the decision on the same is left to the State Government/District Administration taking into account local factors such as:

i. Availability of manpower

ii. Ease of integration with existing initiatives

iii. Availability of existing application for services proposed

iv. Prior experience

v. Ease of implementation for State

c) *In the event the State / District Administration chooses to utilize the services of any external agency for application development and deployment, NIC should be part of the implementation committee overseeing the implementation of the Project at the State and District level so that the project benefits from the knowledge of the NIC of the existing applications and facilitates integration of various legacy applications.*

7.6 Implementation Support Agency (ISA)

a) As indicated in Para 5.3.2, DIT has created a list of empanelled consultant for providing implementation support to the District Administration. In case the State / District Administration chooses to avail the services of the empanelled consultants, they would be responsible for:

i. Preparing the PR

ii. Recommend the service levels

iii. Recommend redesign of the Business Processes (BPR)

iv. Carry out the field study in order to understand the requirements of the citizens, Existing delivery mechanism, levels of interfaces with the Governments, the impediments and difficulties in the accessing the services and information

v. Design an efficient and effective end to end service delivery process

vi. Understand the capacity building requirements and help create a facility for development of capacity

vii. Suggest the functional requirements for the application , based on the BPR

The support of implementation support agency would be segregated across two stages

b) **Stage I:** Design Phase

i. Documentation of the existing process of service delivery across the eDistrict Services

ii. Existing Services Levels

iii. Proposed Service Levels, based upon benchmarking / opportunities for improvement

iv. Identification of Business Process Reengineering requirement to achieve the proposed service levels, including legal changes required.

v. Documentation of To-Be Process maps in line with the BPR proposed

vi. Cost Benefit Analysis of the proposed changes

vii. Design the Functional Requirements of the e-district application

viii. Prepare the Project plan and budget for implementation

ix. Capacity Building / Training Plan

c) **Stage II:** Implementation Phase

i. Design the Change Management Plan

ii. Prepare System Requirement Specification (SRS) for application development

iii. RFP for data entry Vendor

iv. Design the site Layout

v. Project monitoring and reporting to the District administration

vi. Designing the PPP options for providing services

vii. Project Management of the site preparation

viii. Review of the User Acceptance Test (UAT) procedures and review of test results

ix. RFP for Statewide rollout for Pilot e-district application

x. In case of States selecting its own ISA (other than the centrally empanelled consultants) similar terms may be prescribed.

7.7 Application Developer – Application Development and Digitization

a) In States where NIC is identified as the Application Developer, only the data digitization agency will have to selected, for which ISA shall assist in designing the RFP and the subsequent processes.

b) State where application development is preferred through a non NIC partner, the need would be to identify Application Developer for both software development and data digitization. If it is found feasible, the Application Developer could also be made responsible for Data digitization, apart from application development, and migration from legacy application.

c) The Application Developer would also be responsible for:

i) System Requirement Specification

ii) Software Development

iii) Development of UAT procedures and test cases

iv) User Training

v) Rollout in the District

vi) Interface with front end delivery centers for application go live

8. FUND MANAGEMENT

8.1 All funds under the 'e-District' Project for Pilot implementation would be released directly to the State Designated Agency identified by the State Government in the project proposal. As per the States request funds may even be released directly to the District e-Governance Society for the pilot project. However for the rollout, the funds would be released to the SDA only.

8.2 The funds would be released in installments on accomplishment of prescribed milestones, and the State Government certifying the utilization. The prescribed milestones are listed below.

8.3 The phase I (Pilot) funding would be given as grant-in-aid by DIT. However for the phase II (State wide roll out) the funding is proposed to be in the ratio of 75: 25 between DIT and State respectively.

8.4 The first installment would be released subsequent to administrative and financial approval by DIT of the pilot proposal. This would be 30% of the project cost which would include seed money of Rs 10.00 Lakhs for the District e Governance Societies.

8.5 The second and third installment would be 60 % and 10 % respectively on utilization of released funds.

8.6 The funding plan over the eighteen (18) months period is shown in **Annexure VI.**

8.7 The funds for State-wide roll out of 'e-District' would be released only to those States that have implemented the pilot districts successfully as per the guidelines.

8.8 All subsequent releases would be subject to submission of utilisation certificate by the SDA & release of State Government Commitment & utilisation of the same. In case the actual utilized amount works out to be different from the amount sanctioned by the DIT for the said Scheme for a State, the Designated Agency would be required to submit a revised sanction proposal for the 'e-District' Project, prior to release of next instalment.

8.9 The service delivery would be based on a PPP model and user charges would be levied. The recurring expenses could be covered through the users' charges recovered from service delivery. The State must ensure financial sustainability by at least covering the operating expenses.

9. KEY CHALLENGES IN 'E-DISTRICT'

9.1 Some of the key challenges that State Government / District Administration need to consider while developing the project proposals and during implementation of the pilots are

a) Time Bound Project : Project needs to be completed in 18 months

b) Service levels need to be defined, which would require BPR including possible Legal and regulatory changes

c) The pilot project needs to be synchronized with the rollout of the core and support infrastructure for NeGP - SWAN, CSC and SDC.

d) Ensuring administrative stability of e-Champions for ensuring time bound implementation and responsibility

e) Resolve issues and conflicts related to existence of Paper and Paperless system in parallel

f) Standardization of financials, technology and applications

g) Integration with existing applications with e District

h) Absence of IT organization structure at the District except limited 1-2 technical personnel of NIC

i) Process reforms and Change management

j) Development of sustainable financial model

9.2 Awareness among the Government Departments

a) The SDA for implementing the scheme in the State needs to take appropriate steps to ensure all the State Departments are cognizant about the ‘e-District’ Project, its implementing structure and the support required from each department.

b) SDA may organize seminars for the concerned State and District Administration officials.

9.3 Monitoring

a) The eDistrict Project management Group (EPMG) at DIT would monitor the program at national Level.

b) The State Government would need to set up a State Project Committee (SPC) at the State level to coordinate with functionaries of various concerned District Administration and Government Departments as well as district level officers for ensuring smooth implementation of the ‘e-District’ Vision, Mission and Objectives.

c) It is expected that the Monitoring Committee would meet on a regular basis to review the implementation progress of ‘e-District’ at Pilot District locations

d) DIT will stipulate and put in place a mechanism for monitoring of all ‘e-District’ on a continuous basis during Pilot implementation phase and Pan-India roll out phase. All States would be required to comply with such stipulation in order to receive funds under the MMP.

9.4 Service Level Agreements

a) The State Government would need to define specific service levels for each of the services proposed under the pilot district and Service Level Agreement (SLA) will need to be entered with service providers in case an outsourced model for implementation is proposed.

9.5 Modifications/ Addendum

a) DIT, Government of India may issue any future instruction/ clarification from time to time regarding implementation of the ‘e-District’ National

Mission Mode Project. Such instruction/ clarification/ modification would form the Addendum for the instant Guidelines and shall be binding on all concerned.

9.6 Deployment Architecture / Technology Solution

a. **Annexure VII and Annexure VIII** to this document provides guidelines for defining solution architecture for the eDistrict application and the same should be considered for deployment.

b. The application development should be based upon open standards – the application should be capable of running in multiple operating system and database.

c) All application development needs to support n-tier (thin/thick client) architecture and should be based upon service oriented architecture.

d) The software development should follow a SLDC in line with the relevant ISO guidelines.

Additionally, DIT has set up a committee on standards and the application would need to ensure compliance to the same, in case these are finalized before start of the development. Annexure X may be referred for the interim report on Standards.

10 DEFINITION OF SUCCESSFUL OUTCOME

For the project to be considered successful, the following outcome would be measured:

10.1 Phase I

a) Working solution for the district replicable across the State.

b) Successful implementation of Business Process Reengineering (BPR) leading to tangible value addition to services delivered.

c) Number of live notified ‘e-Services’, adhering to prescribed service levels.

d) ‘Institutionalized’ capacity to sustain e-enabled delivery on a consistent and regular mode. (Data updating.)

e) The 'E-District' Systems and solution should be live for at least six months with services being provided through CSCs and other front end systems

f) eDistrict should leverage the SWAN, SDC , CSC and State Gateways

g) Development and implementation of a financial sustainability model

h) Agreement by the State for undertaking a time bound Phase II of the project

10.2 Phase II

a. Number of live notified 'e-Services', adhering to prescribed service levels across the state.

b. Enhanced accountability of the governance structure to deliver efficiently and transparently.

c. Uniform 'e-District' Package in the State.

ANNEXURE I – CATEGORY OF SERVICES (INDICATIVE)

A-	CERTIFICATES
B-	REVENUE
C-	MARRIAGE SERVICES
D-	ELECTORAL SERVICES
E-	LICENSES
F-	COURT SERVICES
G-	UTILITY SERVICES
H-	COLLECTION OF PROPERTY TAX
I-	GRIEVANCES
K-	EDUCATION
L-	HEALTH
M-	EMPLOYMENT
N-	POLICE
O	TRAVEL/SERAI
P	GRANTS/ LOANS
Q	SOCIAL WELFARE
R	INDUSTRIES

Note: Detailed list of each category given in Annexure I-A separately.

ANNEXURE II – INDICATIVE PROJECT COST FOR ONE DISTRICT

S No	Description	Cost (Rs Lakhs)
1	Hardware	140.00
2	System Software	30.00
3	Application Software	30.00
4	Data Digitization	50.00
5	BPR and Consultancy	75.00
6	Site Preparation	15.00
7	Training	15.00
8	Connectivity	15.00
9	Administrative expenses	10.00
10	Seed money to e-Gov Society	10.00
9	Others	10.00
	TOTAL	400.00

ANNEXURE III – APPROACH TO SERVICE LEVELS AND BPR

A. Service Level Definition

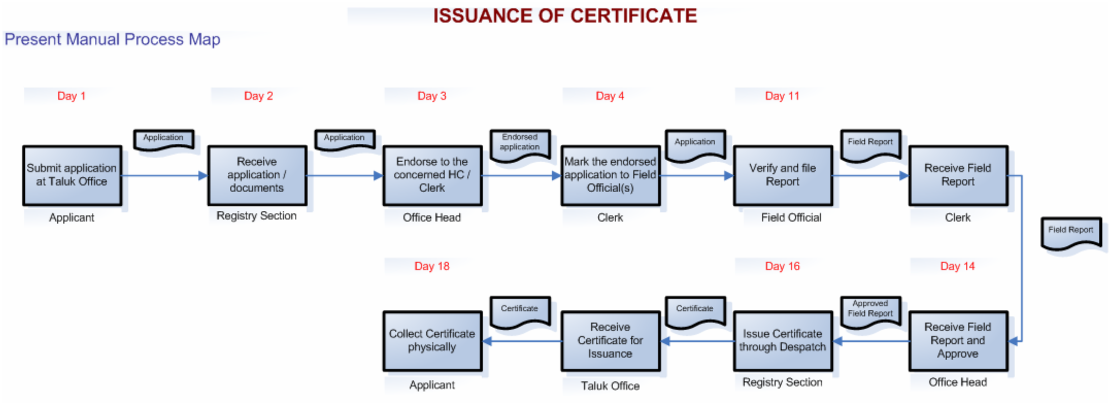
The objective of indicating common services and service levels is to provide consistent service levels to citizens and service oriented delivery in one of the corner stone for NeGP. The common services can be grouped into following categorizes and the State can use the following illustration to define service levels across all of the services proposed under eDistrict MMP.

Sl. No.	Category of Service	Possible Service Levels
1.	Information Availability / Dissemination	Online (Site to be updated at least every 7 days; Changes in existing information uploaded within 2 working days)
2.	Availability of Forms	Online 100% forms used in the department available
3.	Tracking of Application	Online (Status Change provided online within 2 working days)
4.	Transaction (w/o verification)	Online, through Payment Gateway <2 days, through Banks / Service Centres
5.	Transaction (requiring verification of documents)	< 5 working days
6.	Transaction (requiring personal interface/ field visits / verifications)	< 10 working days
7	Payment	Online, Through Payment Gateway
8	Availability of Transaction Service	Online, 24*7 99.9% uptime
9	Grievance Redressal System (including services under Right To Information)	Online, Immediate Acknowledgement / Reference No. Response Time < 2 working days Redressal of Complaint < 7 working days

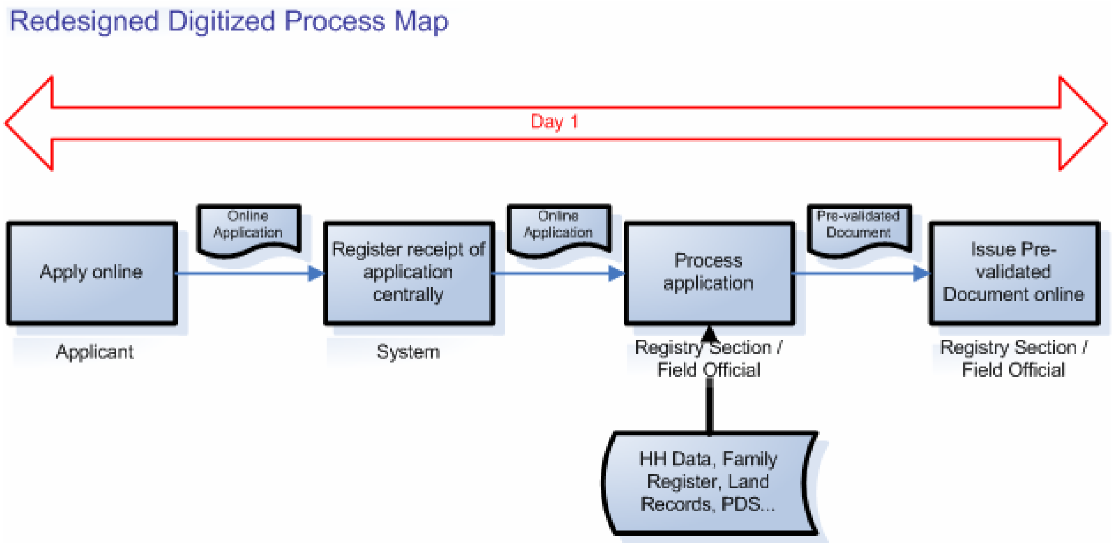
B. Business Process Reengineering

The importance of process redesign to facilitate and ensure best practices in the realm of e-Governance cannot be over emphasized. It is vital that the Process Redesign, i.e. the critical analysis and radical redesign of workflows and processes within and between governmental departments, is undertaken if we are to achieve breakthrough improvements in performance. While deployment of IT solutions increases the efficiency of operations, it will not necessarily deliver the best results unless the processes are reconfigured appropriately to the demands of the specific circumstances. Otherwise, e governance would simply result in “computerization” and the duplication of manual processes by machine-based processes resulting in “automated” waste. Process Re-engineering ensures that processes are redesigned to ensure effectiveness thereby delivering the maximum value to the government, its employees and most importantly, the common citizen. The concept of BPR is best exemplified by the graphical representation below:

Before BPR



After BPR


Redesigned Digitized Process Map
Day 1
Apply online
Applicant
Online Application
Register receipt of application centrally
System
Online Application
Process application
Registry Section / Field Official
Pre-validated Document
Issue Pre-validated Document online
Registry Section / Field Official
HH Data, Family Register, Land Records, PDS...

Approach (Illustrative)

Step 1: Review of the objective and performance metric (service level) of the service. Say the objective is issue of a certificate within 2 days of the receipt of request.

Step 2: Mapping of these performance metrics (outcomes) with current levels. Say currently it takes 15 days to issue.

Step 3: Assessment of whether deficiencies in service metrics can be met through changes in the current set-up, especially those relating to centralized data availability, process points- its spread physically and geographically, hierarchies involved and functions and tasks performed at each of these points, and delegation of power at each of these points and so on

Step 4: Prepare a case for the proposed change in rules/acts detailing the benefits to citizens/business (supported by examples of similar initiatives in other states/ departments)

Step 5: Enable and ensure implementation of the redesigned processes with appropriate changes by way of amendment to the, rules, acts ,administrative orders etc.. ; Adequate empowerment of the Agency responsible for executing the changes.

Step 6: Prepare a contingency plan for the next best option for undertaking process changes in case the proposed changes cannot be achieved.

ANNEXURE IV – FORMAT FOR SUBMITTING PROJECT PROPOSALS

Terms for preparation of Project Report (PR) for the e district pilot projects for a State (generally one district per State but note more than two districts per State)

3. 1 Introduction

- The PR must start with a brief on the district – its demography, topography, structure in terms of blocks/tehsils and other socio economic parameters. The brief must include the functions of district administration and the organization structure. PR should highlight the existing infrastructure, any back end computerization already completed and overall e readiness.

3. 2 Define project Objectives in line with NeGP mission and EGRM of the State

- PR must indicate which of the specific objectives of National e Governance Plan could be achieved by the project and in particular, how the project, if successful will influence the attainment of these objectives.

3.3 Define Project Outcomes envisaged

- The outcome(s) of the project should specify its impact on and benefits to a target beneficiaries that are anticipated on the achievement of project objectives. The identification project outcomes should help in deciding on which activities and services are required to be undertaken.

3. 4 Identify and detail out various services offered

3. 5 Define Target beneficiaries

3. 6 identify various stakeholders and define roles and responsibilities

- The stakeholders should include all sections such as Ministry, department, district, vendors, consultants, implementing agencies, monitoring agencies, citizens etc.

3. 7 End user consultation to understand stakeholders’ expectation

3. 8 Business Model

- The PR must provide details of the proposed business model of the project to ensure self-sustainability of the project in terms of continuity of the services to the beneficiaries without the dependence on external sources of funds. The demand for targeted services, estimated adoption rate and revenue must be estimated.

3. 9 Business Process Re-engineering

- The PR must indicate the requirement of process re engineering and a brief methodology to conduct the same.

3. 10 Service Levels and Measurement

- The PR must detail out the service levels for each offered service and propose a methodology for continuous measurement and reporting.

3.11 Capital Expenditure

- The PR must provide complete details of capital expenditure proposed for the project. The location wise numbers of each hardware, software, furniture, data digitization, project management cost etc required must be provided. The PR must indicate existing hardware/ software etc and identify its usage in the proposed project. The requirement of database and application server needs to be justified in the PR since it is expected that all the databases and application would be hosted in the State Data Centre (SDC) proposed by the Department of Information Technology (DIT).
- In case machines at client end and LAN, the same to be planned on the basis of requirement at each office (net of existing machines or machines planned under any other e Gov projects).

3.12 Operating expenses

- The PR must detailed out projected year wise operating expenses

3.13 Capacity Building

- The PR must indicate the proposed organizational structure of the project with clear reporting relationship. The detailed number of personnel at various levels required to be indicated. The training needs of the personnel to be highlighted with clear training plan, training modules and time frame for the training identified

3.14 Contracting Arrangements

- The PR must provide details of all contracts identified (even if not finalized) and the annual contract values.

3.15 Risk

- The PR must explain the various categories of risks which are most likely to impact on the performance on delivery of services. The PR must highlight the method to evaluate the overall chances of potential loss and the plan to control & monitor the same.

3.16 Cost Benefit Analysis

- The PR must show the results of cost benefit analysis

3.17 Service Delivery Mechanism

- The PR must clearly detail out the proposed channel for delivery of services and plan for integration with the CSC scheme.

3.18 Institutional Mechanism for Project Management

- The PR must indicate the Project Management and Monitoring structure proposed, in consultation with the Stakeholders.

ANNEXURE V – LIST OF CONSULTANTS EMPANALLED FOR IMPLEMENTATION SUPPORT AND TOR FOR THE BPR

LIST OF CONSULTANTS EMPANELLED FOR IMPLEMENTATION SUPPORT

1. Wipro Limited (Infotech Division)
Plot No 480-481, Udyog Vihar Phase III
Gurgaon 122 016
Telephone: 0124 30840000
Fax: 0124 3084349

2. PricewaterhouseCoopers Pvt Ltd
PwC Centre, Saidulajab, Opposite D Block, Saket
Mehrauli Badarpur Road,
New Delhi 110 030
Telephone: 011 41250000
Fax: 011 41250250

3. 3i Infotech Limited
14 Anand Lok,
Next to Ansal Plaza, Khelgaon Marg
New Delhi 110 049
Telephone: 011 51041222
Fax: 011 51041225

4. Telecommunications Consultants India Limited
TCIL Bhawan, Greater Kailash I,
New Delhi 110 048
Telephone: 011 26202633
Fax: 011 26241422

5. Intel Technology India Pvt Limited
Upper Ground Floor, Block E
International Trade Tower, Nehru Place,
New Delhi 110 019
Telephone: 011 41226000
Fax: 011 41226055

The empanelled project support consultant is expected to undertake the following tasks as part of the pilot project implementation:

- Conducting Requirement Analysis (analysis of the processes/situation as it exists and redesigning the same to achieve the targeted outcome)
- Identifying the BPR requirements and design the legal changes required to implement the process improvements.
- Designing functional requirements of e-district application with MIS requirements for assessing the impact keeping in view of unified technology architecture.
- Designing RFP for selection of Data entry vendor
- Designing the site layout of Administration Offices
- Support in implementation of the e-district applications at the sites
- Project Management with Status update and progress tracking of the project online
- Designing PPP options for sustainability of the Project
- Designing of the RFP for State-wide Rollout of the e-district Application
- Defining the current and proposed service levels

Details of task to be carried out

1) **Requirement Analysis:** In order to benefit from this initiative it is necessary to analyze and then redesign the current district administration system and its components to bring in effectiveness, efficiency and added value contribution to the objective of district administration. The BPR would comprise of following steps:

   ➢ **Planning:** This step would entail planning activities that would include the creation of a project scope document, and an examination of existing workflow system. The building blocks of the district administration identified to be covered under the study are as follows:

     - Information availability & access
     - Personal presence
     - Receipt & Validation of application with supporting documents
     - Lodgment
     - Receipt of Fee
     - Preparation of case file, noting & forwarding

- Maintenance of register (Statutory & control)
- Verification
- Release Payment
- Document storage & retrieval
- Decision / Approval / Authorization
- Delivery

- **As-Is Assessment:** This assessment would primarily comprise of examining the existing workflow processes and system used by the district administration. A business process map for the current process may be prepared. Subsequently, similar activities would be grouped for process normalization and redundant activities would be proposed for removal. The study would also identify the current services and service levels
- **Target Envisioning:** The target e-district would be envisioned after benchmarking of the current processes against relevant best *practices* to obtain ideas for improvement.
- **To-Be Process:** After the identification of potential improvements to the existing processes, the development of the proposed workflow system would be built on the research from the benchmarking and best practices activities. It would also be required to identify and document risks associated with implementation of the automated workflow processes. The resultant processes would be validated by the district administration officials and duly approved by the government before implementation.

Designing the functional and software requirements of the e-district Application: To design the functional requirements of a comprehensive workflow software system consisting of all the required modules for the district administration at various levels – District collector office, Additional District Magistrate, City Magistrate, Tehsildar, Revenue Inspector. Detailed study would require to be conducted for finalization of Software requirement specifications. The scope of SRS would be as under:

Micro level study of candidate systems of District Collectorate, Zila Parishad, Sub division, Tehsil, Block and other offices under the direct purview of District Administration

List out office wise systems for Software development

Describe the system as seen by its end users, analysts and testers.

Describe the design view of the system encompassing with broad classes/data bases, transaction layouts, integration/ interfaces for process transformation.

Describe the process view, addressing the processes involved in building the systems, interlinkages in process transformation, performance, scalability and throughput of the system.

Designing RFP for Data Entry vendors and Digitization of manual records and assisting the district during Bid process management: In order to enable the district administration to work on designed electronic workflow system, the concerned officials may require referring old records. Therefore, as per the requirement old manual records would be digitized using the data entry vendors. The RFP for selection of the Data entry vendors will be designed by the consultants.

Assist in Designing the Site Layout: The concerned offices of the district administration may also require modification in the existing infrastructure to implement the proposed system in an effective manner. The consultants will assist in designing the site layout.

Project Management of the Implementation of the e-district Application: Assist during: Monitor the progress of the project activities and deployment of the application in the district and testing with the end users. The consultants will track the progress of the projects and provide status update to the District administration/ State project committee on regular intervals. They will timely escalate the issue and plan for risk mitigation strategies

Change Management and communication plan – The consultants will design the project change management strategy and communication plan. Design training manual and the assist in conducting functional trainings

Designing PPP Options: The consultants will study the existing transaction volumes and the model for designing PPP options for sustainable implementation of the e-district. The consultants need to design a revenue model based on the user charges

Designing the RFP for Statewide Rollout: The consultants need to design a RFP for Statewide Rollout based on the Pilot e-district implementation.

ANNEXURE VI – FUNDING PLAN

	Start of Month						
	1	3	6	9	12	15	18
	Phase I			**Phase II**		**Phase III**	
Hardware			30%	30%	40%		
System software				50%	50%		
Application software				50%	50%		
Data digitization			25%	25%	25%	25%	
BPR and Consultancy	10%	20%	20%	20%	10%	10%	10%
Site Preparation		50%		50%			
Training				30%	30%	40%	
Connectivity						50%	50%
Administrative Expenses	30%			30%		40%	
Seed Money to e Gov Society	100%						
Others	10%	10%	10%	20%	20%	20%	10%
Total	5%	6%	18%	29%	28%	10%	4%
	Phase I = 30 %			**Phase II = 60 %**		**Phase III = 10 %**	

ANNEXURE VII – GUIDELINES DEFINING ARCHITECTURE FOR EDISTRICT APPLICATIONS

1.0 Introduction

Software Development and Deployment Framework for E-District Applications is worked out to aid the Stakeholders from States, IT System Development Agency and nominated Quality Ensure team. The suggested framework is inspired and built using three models – Spiral Model, Rationalized Unified Process Model and Iterative Model. The Framework is divided into number of steps which should be used to build interoperable and good quality E-District Applications. The Framework recommends that during various Iterations of Application Development life cycle, Hardware Sizing and Procurement of IT, IEEE Standards for development, ANSI SQL-2003 standards for RDBMS and Open Standards for hardware platforms should be used. Various parameters which can be utilized to estimate the number of processors/Server, hard disk storage space and RAM have been suggested. Emphasis is put to build redundancy in the hardware equipments to ensure high availability of System for E-District Application.

2.0 Framework Objective

This framework is developed to provide Software Solution Development and Deployment framework for E-District MMP

3.0 Scope

This framework for has been developed as a template to help State governments in the smooth operation, management, and oversight of the e-district application projects. This will also help the States in understanding the phases for software development and its architecture.

4.0 Software development and deployment disciplines

- Software Requirement Study and Planning
- Analysis and Design
- Development
- Application Testing
- Application Deployment
- Configuration and Change Management
- Software Project Management
- Resource Allocation Planning

Systems should be delivered through development of components since it will make it possible to assign well defined responsibility to a role, easier to maintain, and increasing the possibilities to reuse.

- **Assign clear cut responsibility to each Sub program/procedure**

If the number of lines in a subprogram is exceeding 500, then it should be taken as a signal that we are over loading responsibility to a sub program. Re-factor the subprogram/procedure.

- **Naming conventions for local variables and parameters of a procedure**

Give names of smaller length to local variables and more verbose names to parameters of a subprogram/procedure.

- **Avoid using Constant Literals**

The use of constant literals such as

if AmountWithdrawn > 15000 then printf(" Withdrawl not permitted in ATM);

should be avoided, instead meaningful names as ATMWithdrawlLimit should be used in place of Rs 15000.

- **Avoid using chains of Nested Statements**

Developers should avoid using chains of IF/Else and several cases in Swith Statement.

- **Use Logs inside the Code**

Logs should be put inside the code since it helps in debugging the code faster, understanding the thought process and structure of the program logic and tracking the execution of a program.

- **Put comments in Code**

Adequate comments inside the body of each program should be put, specially inside a sub program indicating the input arguments it accepts and output arguments it sends.

- **Use Defensive Style of Programming**

If a subprogram returns Null values they must be treated/checked inside the caller program to indicate that the action taken inside it is as per the agreed functional specifications.

Application Testing

Test discipline should be a part of Development Process and it should be done:

- To verify the interaction between objects.
- To verify the proper integration of all components of the software.
- To verify that all requirements have been correctly implemented.

- To identify and ensure that defects are addressed prior to the deployment of the software

Testing Documents:

Testing Document should describe:

- testing strategy,
- test cases,
- expected outcome and attributes of test process –
- quality, assessment,
- comparison and quality improvement,
- logs, incident reports (as per IEEE 829 Std -1998 Software Test Documentation) should be prepared and maintained.
- Penetration testing for security

Besides, the usual testing methods: Unit Testing, Module testing, integration, white-box, Black-box, load and stress testing, it is very important that we should carry out testing for **Web Interface** which includes:

- Testing that Forms run under all types of Browsers
- Impact of opening multiple windows
- Effect of using back option and situations responsible to denial of Services
- Impact of pressing Submit button next time while Credit Card Payment is being made.
- How to simulate the load on the application due to Web Users

Follow an iterative approach, which means testing should be done throughout the project as it allows to find defects as early as possible, which radically reduces the cost of fixing the defect. Tests should be carried out along four quality dimensions *reliability*, *functionality*, *application performance, and system performance*.

Application Deployment

The purpose of deployment should be to successfully produce product releases, and deliver the software to its end users. Following outcomes and the activities should be ensured:

- Producing external releases of the software
- Packaging the software
- Distributing the software
- Installing the software
- Providing help and assistance to users

Configuration and Change Management

The Change Management discipline should deal with:

- Configuration management
- Change request management
- Status & management of change requests

Configuration management

Configuration management means systematic structuring of the products. Artifacts such as documents and models need to be under version control and these changes must be visible. Dependencies between artifacts should be maintained so that all related articles are updated when changes are made.

Change request management

During the system development process several changes may come, track for them and artifacts corresponding to them should be kept.

Status & management of change requests

Change requests with states such as new, logged, approved, assigned and complete should be kept along with attributes such as root cause, or nature (like defect and enhancement), priority etc. in database so that useful reports about the progress of the project can be produced.

Software Project Management

This discipline should be used to focus mainly on the important aspects of an iterative development process:

- Risk management
- Planning an iterative project, through the lifecycle and for a particular iteration
- Monitoring progress of an iterative project, metrics

This discipline should be divided into two parts- Coarse Plan and Iterative Plan.

Coarse Plan

The coarse plan should focus on following items:

- The **Risk Management Plan** should detail out how to manage the risks associated with a project. Detail out the risk management tasks required to be carried out, responsibilities, and list of additional resources needed for the risk management activity.

- The **Risk list** should be prepared and sorted out in decreasing order of sensitivity including both known and open risks to the project along with contingency actions.
- The **Problem Resolution Plan** should be made describing the process used to report, analyze, and resolve problems that occur during the project.
- The **Product Acceptance Plan** should be prepared describing how the customer will evaluate the deliverable artifacts from a project to determine if they meet a predefined set of acceptance criteria. Detail out these acceptance criteria, and identify the product acceptance tasks, i.e., test cases and person and resources required for them.

Conformance Assessment Testing

STQC shall be undertaking all conformance testing of eGovernance applications/MMPs as per the deliverables given in the above framework.

5.0 Technology Guidelines for IT Infrastructure

The pilot may be developed keeping in mind the DIT initiatives such as SWAN, SDC, CSC, and NSDG being implemented under the NeGP for successfully deploying the various MMPs

Centralized Architecture Design Go in for 3 or more tier Centralized Architecture Design as it is cost-effective. Specific benefits include:

- A reduced total cost of ownership,
- Upgrades and new releases of the Application are to be done only at the central server, rather than having to be installed on several machines.
- Easier system maintenance and administration,
- The ability to manage and monitor the system from a single, central location
- Better management and administrative control
- Better deployment of security
- Economical to build redundancy at each level for business continuity and Disaster Recovery

Build Browser Based User Interface:

Build browser based interface for all types of clients – Internet users, Employees (Staff) and CSC (Common Service Centre) users.

Distributed Architecture for States with Poor Network Connectivity

States where network connectivity is poor and SWAN and State Data Centre (SDC) are likely to take some time to reach them, they may place Servers at District level but the flavour of production environment should be identical to 3 or more tier architecture so that at a later stage when SWAN and SDC Come up, the migration path is straight forward.

Option to choose Applications Already Available in Central Pool of NIC

The States which want to use applications already developed by NIC may use these applications and may start providing services to the citizens.

NIC to update and enhance the functionality of already developed Applications

NIC should incorporate the new functionality and update the applications already developed by it, on the request of State. Some of the applications may need migration from old technologies to new one, e.g., if some of the applications are developed under FOXPRO, they may require re-engineering; the same may be requested by the State.

Networking Guidelines

TCP/IP based communication protocol including IPv4/Ipv6 should be supported by the Application.

Security Policy and Guidelines

The Software and application development process should take appropriate measures for data privacy, confidentiality and access control issues while designing the software application strategy. The security initiatives may include PKI infrastructure, DMZ Policy, encryption, authentication, authorization and digital signature.

6.0 Strategy for doing Pilot Project

Option -I

States which want to do E-District pilot project in more than one District should divide the functionality /services in terms of Modules and assign them to two different teams working under the same Project Development Manager who is responsible to ensure the integration of the two independent module providing functionality of the application. This will help in faster development and deployment of application. This will also help in maintaining uniformity of development tools, hardware, system and application software at the State level and ensure better co-ordinations among the departments. It will help in avoiding duplication in development efforts.

Option –II

On the other hand, If some States want to get developed the same set of Services in two Districts through two different Vendors, due care must be taken to ensure that same set of tools, hardware, software and Application systems are used so that the environment for set of services remains homogeneous.

7.0 Features expected in RDBMS:

- Should support data base partitioning and parallel processing
- Should support Active-Active Configuration
- Allow users to connect and use the same database from multiple nodes by using resources of the individual node
- Should be available under maximum number of Operating Systems and supported under maximum number of Application Servers.
- Should have support for generation, consumption of XML data and XML based query capabilities.
- Allow multi dimensional OLAP capabilities for Data Warehousing

8.0 ANSI-SQL Standards for ensuring Interoperability

ANSI SQL-2003 can be used, while it should be kept in mind that bit data type is dropped from it. It is suggested that minimum SQL3 (SQL-1999) standards must be used for data types and developers should have the freedom to use features of SQL-2003. But if they are using features of SQL-2003 then proper documentation of the features used in the Application should be made so that the effort involved in backward migration of the data from SQL-2003 to SQL-1999 are known in advance to the Developers.

9.0 Hardware Sizing:

Following parameters should be included to arrive at – Number of Processors/machine required for Data Base Server and hard disk space requirements:

- Number of transactions done per minute
- load of reports
- resources required by concurrent number of users including DBA and other maintainers, database size
- data archival period
- TPMC of the Chip
- While deciding the size of RAM the requirements of Operating System, System and Application software should also be considered, besides the above parameters.
- Adequate redundancy should be built at Processor, Machine (or Server or Node) and Storage Space (Disk) level.
- Redundancy at Controller level for Storage Space should also be built.

- Disk should be configured in RAID 0, 1 or RAID 0, 5 level to avoid loss of data. In RAID 0, 1 the disk space required is double the size of actual data requirement but chances of loosing data become very low practically zero.
- Cluster environment should be built for critical applications with fail-over and fail back features.
- Similarly, the configuration of Application Server and Web Server should be worked out. Generally Application Server is lighter than Data Base Server and Web Server is kept lighter than the Application Server. But Redundancy and load balancing features must be built in them to achieve over all highly available system.

10.0 Application Server Software

Select Application Server:

- Supported under maximum number of Operating System
- Gives Driver support for accessing and storing information in maximum number of databases
- Provides capabilities for Centralized configuration and control

11.0 Procurement of IT Infrastructure

- Assessment of existing IT infrastructure
- Requirement analysis for additional IT infrastructure and procurement
- Data entry/migration
- Installation of hardware and system software
- Porting of Solution Software
- Release of Installation Certificate

ANNEXURE VIII - POSITIONING NATIONAL E-GOVERNANCE SERVICE DELIVERY GATEWAY (NSDG) - XML BASED MESSAGING MIDDLEWARE

Introduction

This mission project aims at setting up a National gateway called NSDG for standards based messaging between heterogeneous applications. A cluster of Gateways would be setup across the country which will be an integral part of the SDCs to ensure standards-based interoperability between the various departmental applications at the back end and connect the CSCs or other delivery channels at the front end. Acting as a nerve centre, the gateways would handle large number of transactions across the entire network; provide a common set of specifications and a single point access for departments. Such an infrastructure would also help inter-departmental working in a co-ordinated and synchronized manner. As a central message processing mechanism it would also help in tracking all transactions of the Government.

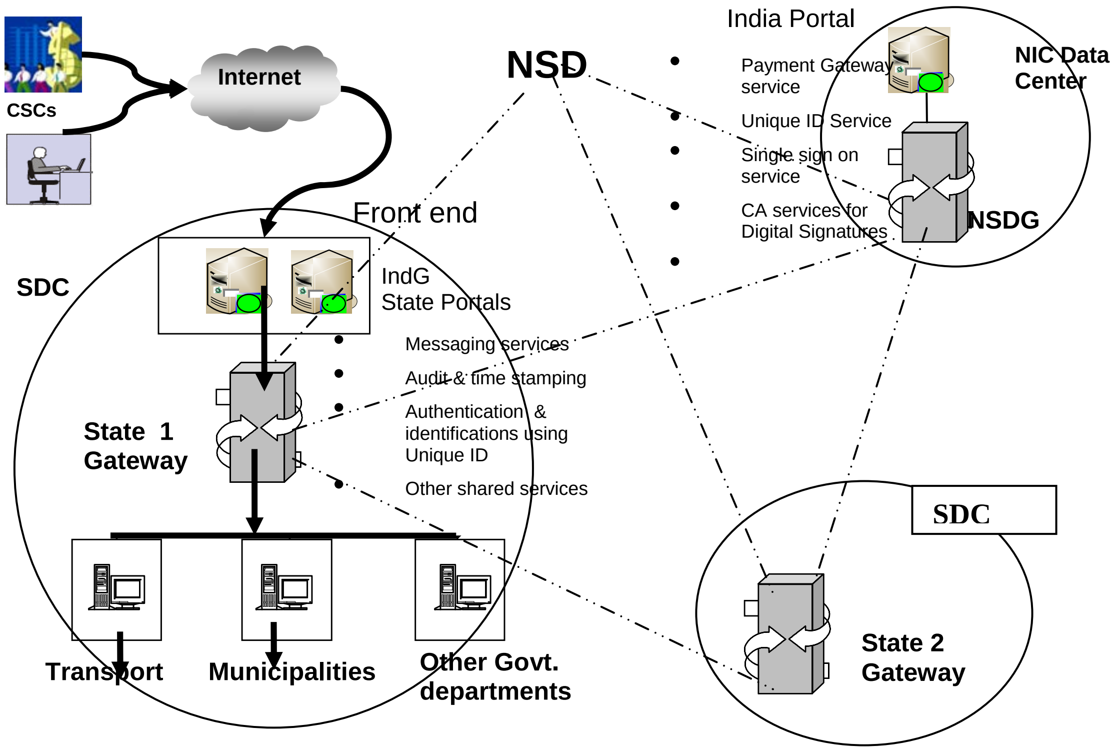
As a part of this project, a National Service Directory (NSD) to resolve the address and service resolution between the Gateways is also being set up. The NSD will publish all the departmental services across the country available through the gateways

With the CSCs, and E-District project in the pipeline, this soft infrastructure is a critical component in the SDCs. This infrastructure will facilitate:

1. Standards based messaging and routing switch ensuring secure and guaranteed delivery of services between the front end portals and the back end departments and between departments. It will de-link the backend departments from the front end service delivery mechanisms like CSCs.
2. This infrastructure will eliminate the need for the departments to have multiple linkages with the various SCAs providing citizen services through the CSCs. Rather a department will connect only once to the Gateway and transact with multiple CSCs. Hence the Gateway will Simplify the view of the external world to the departments and also ensure better security
3. Complete audit logs & time stamping of transactions going through it.
4. The Gateway will also help the Departments backend work flow evolve gradually as the Gateway acts as a middleware de-linking the backends from the front end. This means that even the Departments which do not have the a complete automation or work flow at the back can still deliver e-Service to the citizens in a limited manner through the Gateway. To cite as an example, a server may be put up at the department for message exchange with Gateway in absence of readily available infrastructure at the department.

5. In future, Gateway has the capability to add additional functionality to support shared common services like Authentication, payment gateway interface, etc
6. Use of common language viz XML for message exchange between applications and business processes within and outside Government

Positioning Gateway at the State data Center



Network Architecture with SDCs, CSCs, Gateway, NSD infrastructure in place

Positioning of Gateway

1. The Gateway is Core standards based messaging & routing middleware based on XML and SOAP envisaged as a cluster at the National level & SDCs. CSCs are the front-end access channels delivering various Government and private services. The SCAs setting up these CSCs could either have their own portal based on the Content Management framework guidelines issued by the government or use the common National SPV portal to publish the contents and services to the citizens. While convergence on either of these options is under way, as far as the access to Government contents and services is concerned, following possible options for user interface/access at CSCs are being considered:

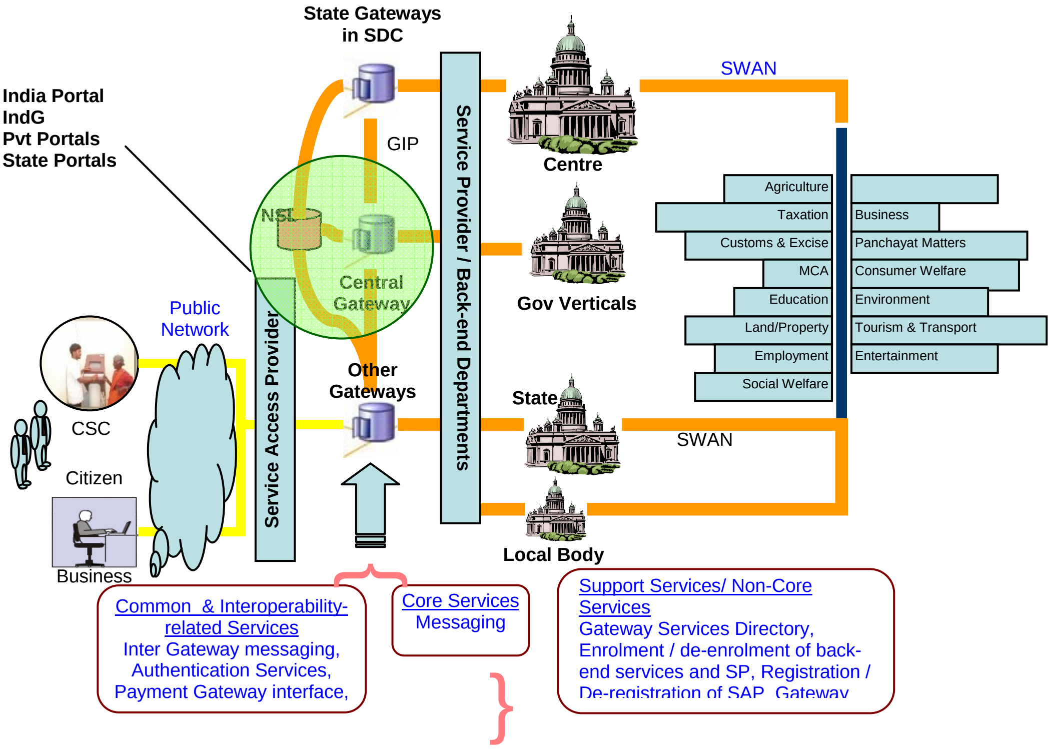
    1. Through the National India Portal
    2. Through State Portals (State Portal can be an instance of the India Portal i.e., the State specific contents and services from the India Portal are made available on the State Portal)
    3. Any other portal

2. In either of the options, the Portal will connect to the State Gateway residing at the State Data Centre. This would mean implementation of connectors using the APIs and the Message exchange behavior of the Gateway at the SCA portal if they are directly accessing the departmental services. If the SCA portal is only forwarding the service request of the citizen to the State Portal,

then it is the State Portal, which will build the requisite connector interface with the Gateway. In either case, the request is sent to the State Gateway.

3. The State Gateway will have all the intelligence as to how to route each request to the respective departmental Server offering the service, for example, Birth/Death or other Certificate related requests will be routed to Municipality Server and property tax related requests will be routed to Land Record Server. Each Department will have a Departmental Interface Connector (DIS) of State Gateway installed on a server. The response from these servers will be returned to the State Gateway Server which in turn will give it back to the SCA portal or the State Portal.

Role of Gateway in e-Gov Service Delivery



System Architecture for Gateway as the Middleware

1. New Services which are at the conceptualization stage

The services for which the architecture design is underway or yet to start must incorporate the Gateway functionality in the design. The message exchange behavior and the specifications of APIs to avail the gateway functionality will be made available shortly. However, this is assuming that the SDC is up and the gateway is in place in the SDC. But in cases where the SDC is not up and the application design is underway, the core gateway messaging functionality can be incorporated as a module, which can be, replaced once the State gateway is up. The development of this Gateway code can be undertaken under the guidance of CDAC, which is implementing the gateway.

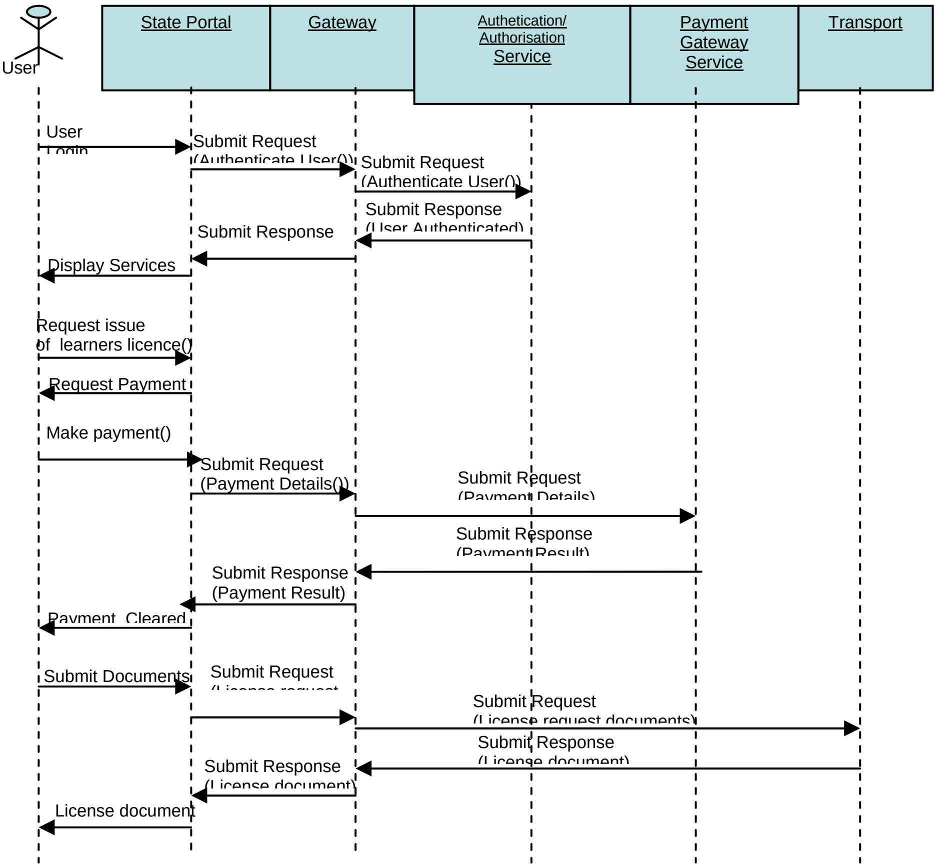
.

2. Existing Applications to use the Gateway architecture in Design

For services, which are already e-enabled, connectors will have to be built to connect and route messages through the Gateway. As one of the possible options the connectors can be built by the State government with the support of CDAC and the service provider who had initially developed the application.

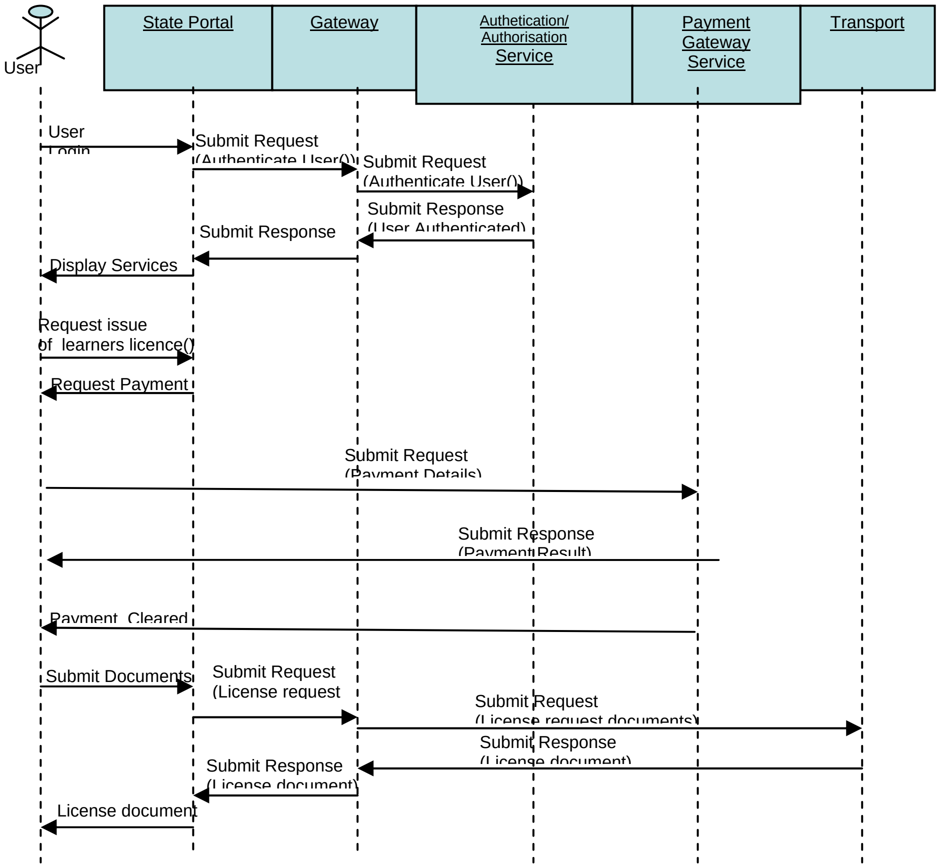
Option 1: Gateway is used for messaging and establishing interface with the 3rd party authentication services and payment gateway services.

Sequence Diagram showing messaging with Gateway for a sample service –Issue of Learners Driving Licence-for Internet User. User can be replaced by CSC.Digital Signing/Photo facility ,etc not included.Assumed visit to RTO not required except for collecting Licence.
(Note: Submit Request and Submit Response as indicated must be taken as conceptual representation of message interaction behavior of IIP, GCS protocol. Please do not treat Submit Request and Submit Response as any API representation.)



Option 2: Payment is made directly to the Payment Gateway

Sequence Diagram showing messaging with Gateway for a sample service –Issue of Learners Driving Licence-for Internet User. User can be replaced by CSC.Digital Signing/Photo facility ,etc not included.Assumed visit to RTO not required except for collecting Licence.
(Note: Submit Request and Submit Response as indicated must be taken as conceptual representation of message interaction behavior of IIP, GCS protocol. Please do not treat Submit Request and Submit Response as any API representation.)


User
State Portal
Gateway
Authetication/ Authorisation Service
Payment Gateway Service
Transport
User Login
Submit Request (Authenticate User())
Submit Request (Authenticate User())
Submit Response (User Authenticated)
Submit Response
Display Services
Request issue of learners licence()
Request Payment
Submit Request (Payment Details)
Submit Response (Payment Result)
Payment Cleared
Submit Documents
Submit Request (License request
Submit Request (License request documents)
Submit Response (License document)
Submit Response (License document)
License document

This is a preferred option to start with. Though the gateway implementation will have provision for the Payment gateway interface to establish connection with any payment gateway service, it is recommended that in the first phase, the payment is directly done with the payment gateway of the bank. Also, the authentication interface is to be used if there are any 3rd party authentication services being availed.

2. Implementing Agency for NSDG

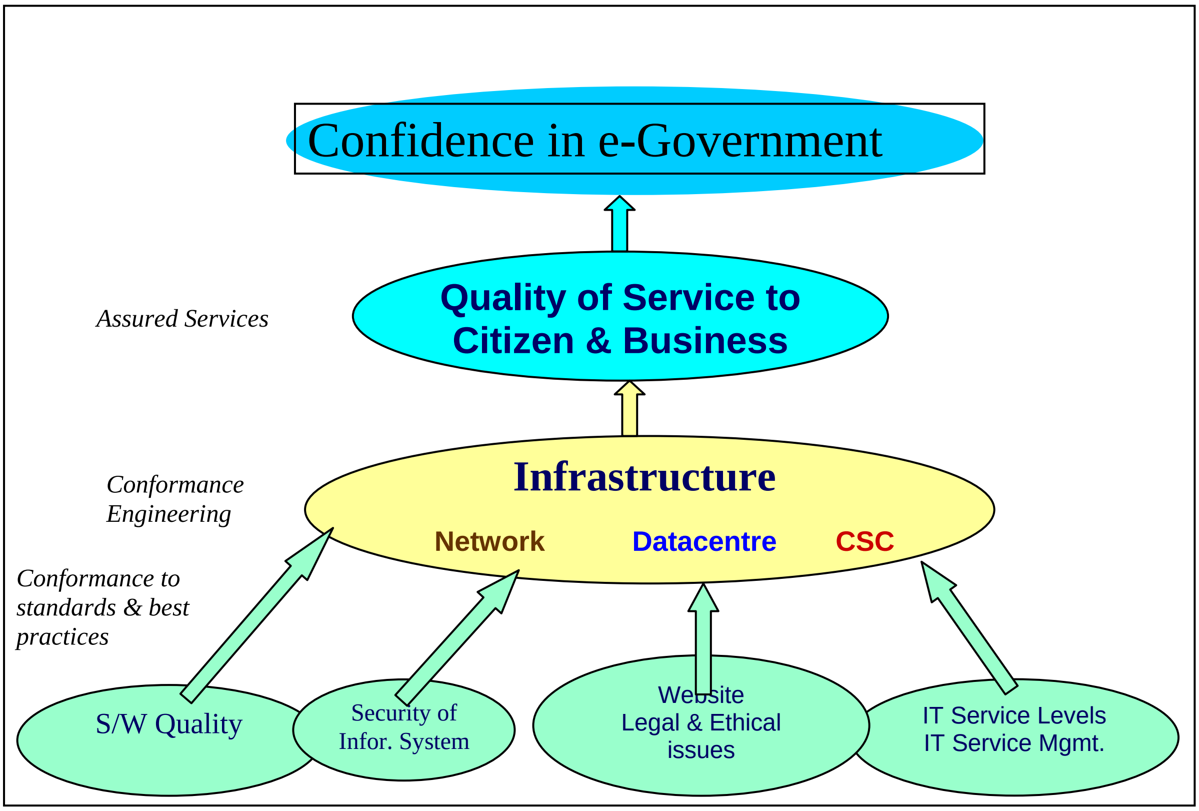
As part of its implementation strategy for the NSDG, the Department of Information Technology (DIT), GoI, has entrusted the responsibility for implementation of NSDG to CDAC, a society formed by the GoI along with consortium of partners. As this is a core infrastructure, which needs replication across the country, government ownership is critical. The National Gateway will be up and running by December end this year. However, the messaging interface behavior along with the APIs is expected to be ready and available to the service providers in the next 2 months.

ANNEXURE IX - CONFORMITY ASSESSMENT FRAMEWORK FOR E-GOVERNANCE

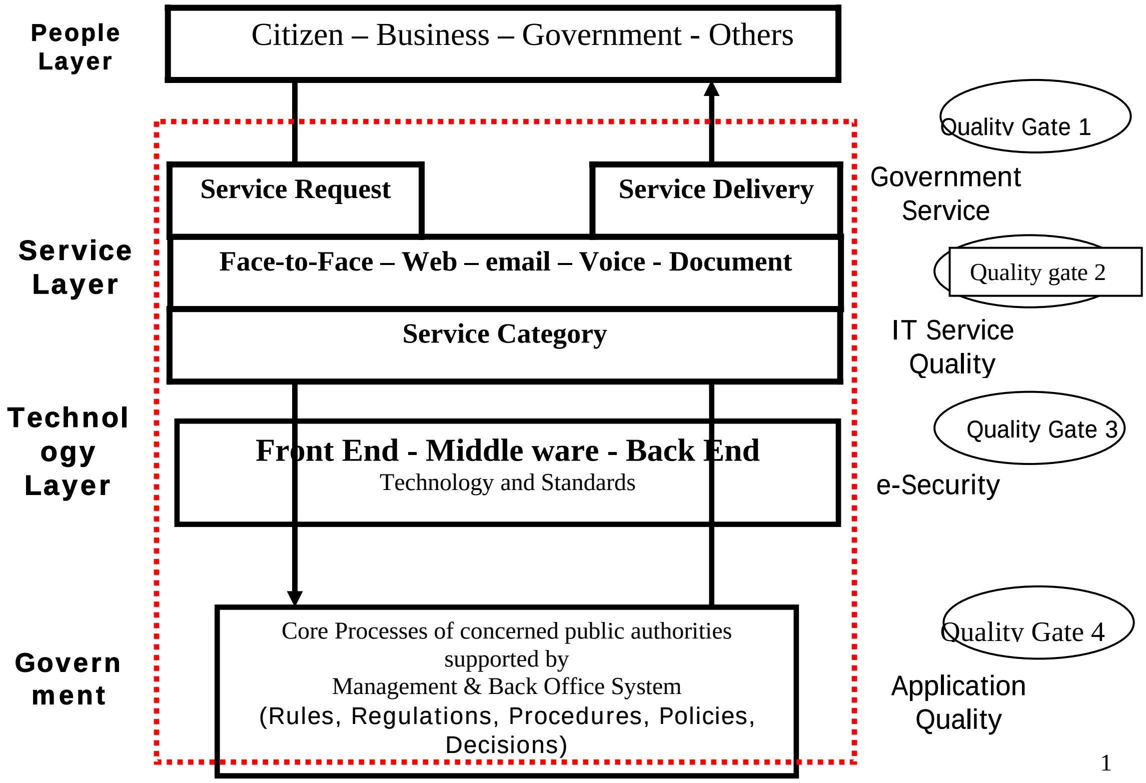
Background:

STQC, which is a Directorate of DIT, has been providing testing, audit, compliance and certification services in IT domain to the private sector. However, with the inception of NeGP, STQC has extended its services to many e-Governance initiatives and the recent one is MCA21. The entire audit and certification of the MCA21 software, security and service delivery was done by STQC as per the ISO standards (9126, ITIL (ISO 20000), ISMS (ISO 27001) etc.)

STQC has set up seven IT centers across the country to provide the necessary 3rd party audit AND TESTING services for Compliance and certification to various mission mode projects. Under this programme STQC has developed a Conformity Assessment framework (CAF) for eGovernance covering all the aspects related to audit and certification of any e-governance application based on standards. This is a very comprehensive framework, which must be considered while drafting the RFP. This framework will ensure that the requirements are clearly specified in the RFP, specifications are complete and the users are satisfied. This framework is flexible and can be tailored to the needs of eGovernance Solutions for different situations. This will not only help in enhancing the confidence of the users, the quality of solution itself will get enhance significantly by removing the anomalies and shortcomings observed during evaluation process.


Confidence in e-Government
Assured Services
Quality of Service to Citizen & Business
Conformance Engineering
Infrastructure
Network
Datacentre
CSC
Conformance to standards & best practices
S/W Quality
Security of Infor. System
Website Legal & Ethical issues
IT Service Levels IT Service Mgmt.

Quality Architecture for E-Governance – Gates for Conformity Assessment


People Layer
Citizen – Business – Government - Others
Service Layer
Service Request
Service Delivery
Face-to-Face – Web – email – Voice - Document
Service Category
Technology Layer
Front End - Middle ware - Back End
Technology and Standards
Government
Core Processes of concerned public authorities supported by
Management & Back Office System
(Rules, Regulations, Procedures, Policies, Decisions)
Qualitv Gate 1
Government Service
Quality gate 2
IT Service Quality
Quality Gate 3
e-Security
Qualitv Gate 4
Application Quality
1

Quality Gates of Conformity Assessment Framework for e-Governance Architecture

1. Quality Gate 1 – Government Services
   - Face-to-Face (CSCs) ISO 9001:2000, IWA4, QMS in Local Govt.
   - Online through Web - ISO 9241 Pt-10 & 11, Web Site Usability

2. Quality Gate 2 – Information Security Management System
   - ITIL, ISMS, ISO 20000

3. Quality Gate 3 – Information Security
   - Component Level (ISO 15408)
   - Application Level
   - System Level (ISO 27001)

4. Quality Gate 4 – Application Management
   - ISO 9126
   - ISO14598
   - ISO 9001-2000 /IS:15700

Quality Gate 1- Government Services

Govt. Services form Citizen Government Interface and this interface could be face-to-face, voice, web, email, documents etc. The requirements of a service quality, needs to be clearly defined in terms of characteristics that are observable and are subject to evaluation. The processes that deliver a service also need to be defined in terms of characteristics that may not always be observable by the customer but directly affect service performance. A citizen charter and service level declaration will enforce this aspect. In case of Services through web/ Internet service delivery characteristics also needs to be separately defined.

Quality characteristics of Service delivery (face-to-face e.g. Citizen Service Centres)

Examples of Quality characteristics that might be specified in requirement documents include:

- Facilities, capacity, number of personnel etc.
- Waiting time, delivery time and process times
- Hygiene, safety, reliability and security
- Responsiveness, accessibility, courtesy, comfort, aesthetics of environment, competence, dependability, accuracy, completeness, state of the art, credibility and effective communication.

In most cases, the control of services and service delivery characteristics can only be achieved by controlling the process that delivers the service. Process performance measurement and control are, therefore, essential to achieve and maintain the required service quality. A criterion based on IS 15700/ISO 9001 IWA4 QMS Standards used to evaluate for demonstrating compliance.

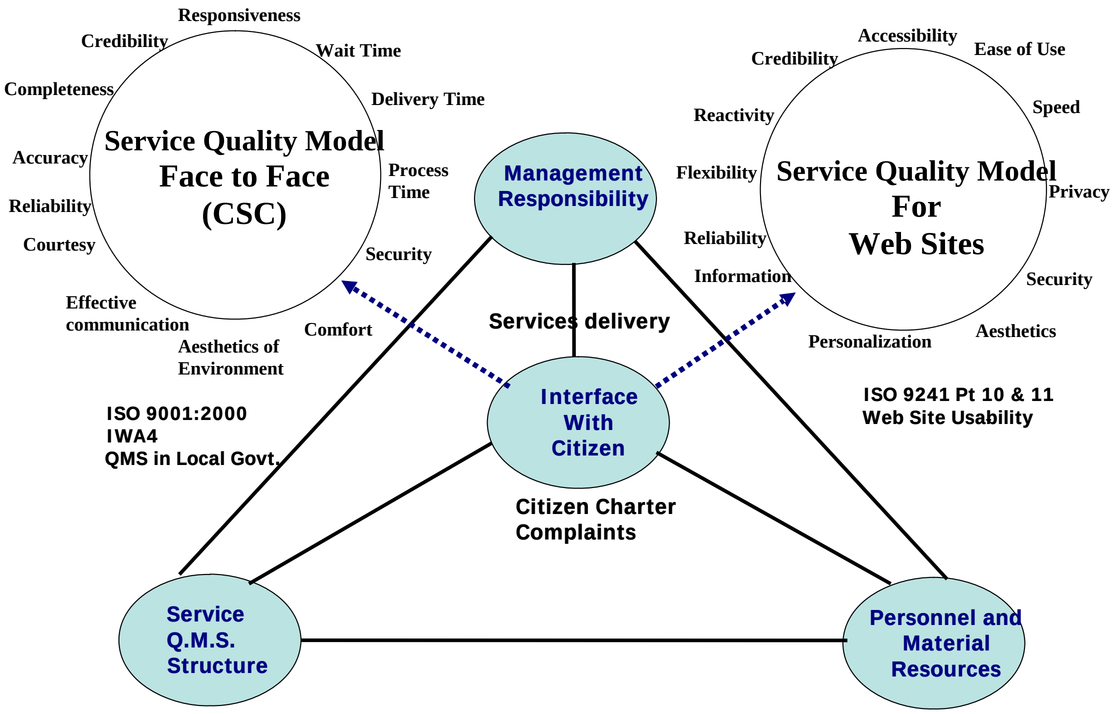
Quality characteristics of Service Delivery (Web)

To successfully evaluate web-based E-Government service delivery, a robust, multidimensional web evaluation strategy is required. Web evaluation methods fall into following major classes.

- Usability testing: By using various techniques for obtaining feedback from a limited number of experts & users, in a controlled laboratory environment by simulating business scenario.
- User feedback: Getting direct, usually qualitative feedback from actual website users.
- Web and Internet performance data: These methods involve measuring the Web site's technical performance, using metrics such as latency, availability, and data transfer rate.

The conformity is assessed against best practices as applicable:

- Content identification and information
- Privacy
- IT Security
- Secure payment
- Process audit (ISO 27001) and Certified ISMS (ISO 27001)
- Quality/ Business Process
- Complaint system
- Process audit and Certified QMS (ISO 9001)
- Software Functionality (ISO/IEC 12119)
- Usability (ISO 9241-10/-11)



Quality Gate 2 – Information Security Management System

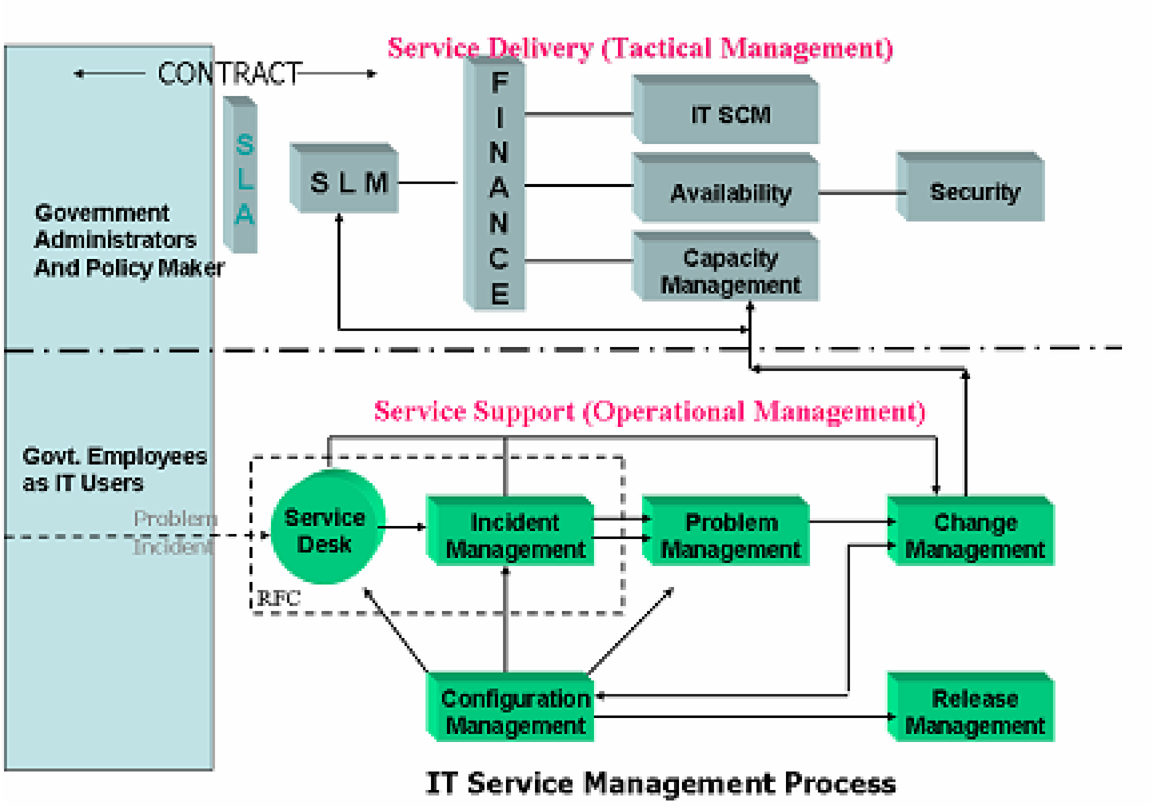
IT driven Government Information System is the backbone for delivery of services, interface with citizen and quality of governance. Due to this, dependence on IT has increased many folds. However, the complex ever-changing environment and rapidly evolving technology offer substantial challenge to effective IT management. It is expected that IT services not only will support the Governance processes, but also to present new options to implement the objectives of good governance.

The effectiveness and efficiency of the Government services to citizen or business greatly depend on the quality of IT services, which in turn needs to be managed properly.

Generally in Government, IT Service and its Management is outsource (except data ownership) for availability of IT Services to a competent body.

To meet the requirements of service level agreement between the Government and IT Service Providers a framework of IT Service Management is required. Best Practices as given in ITIL/ISO 20000 are taken as reference criteria for Conformity Assessment.

High availability implies continuous availability of IT Services, which means little downtime and rapid service recovery. This depends upon Complexity of the IT infrastructure architecture, Reliability of the components, Ability to respond quickly and effectively to faults, Quality of the maintenance and support organizations, Quality of operational management processes. This will be ensured only when IT Service Providers implement processes such as incident Management, Problem Resolution Management, Service Continuity and Availability Management, Service Level Management etc. This will ultimately get reflected in Service Level Agreements, which are part of the contracts between Govt. and IT Service Provider.



Quality Gate 3 – Information Security

e-Governance is heavily dependent on a well functioning of information supply. In this context, information security is not a goal in itself but a means of achieving the good governance objective.

Information Security is intended to safeguard information. Security is the means of achieving an acceptable level of residual risks. The value of the information has to be protected. This value is determined in terms of confidentiality; integrity and availability.

- Confidentiality: protecting sensitive information from unauthorized disclosure or intelligible interception.
- Integrity: Safeguarding the accuracy and completeness of information and software
- Availability: ensuring that information and vital IT services are available when required.

Not all information and not all information services are equally important to the Government and community. The level of information security has to be appropriate to the importance of the information. This tailored security is achieved by finding a balance between the security measures and their associated costs on the one hand and, on the other, the value of the information and the risks in the processing environment.

- Internal importance: In good time, Information security has to be in line with this, ensuring that confidentiality, integrity and availability of information and information services maintained.

An inadequate information supply leads to imperfect services, thereby preventing the objectives from being fully achieved and threatening the continued existence of the

Government objectives. Having adequate information security is an important precondition for an adequate information supply.

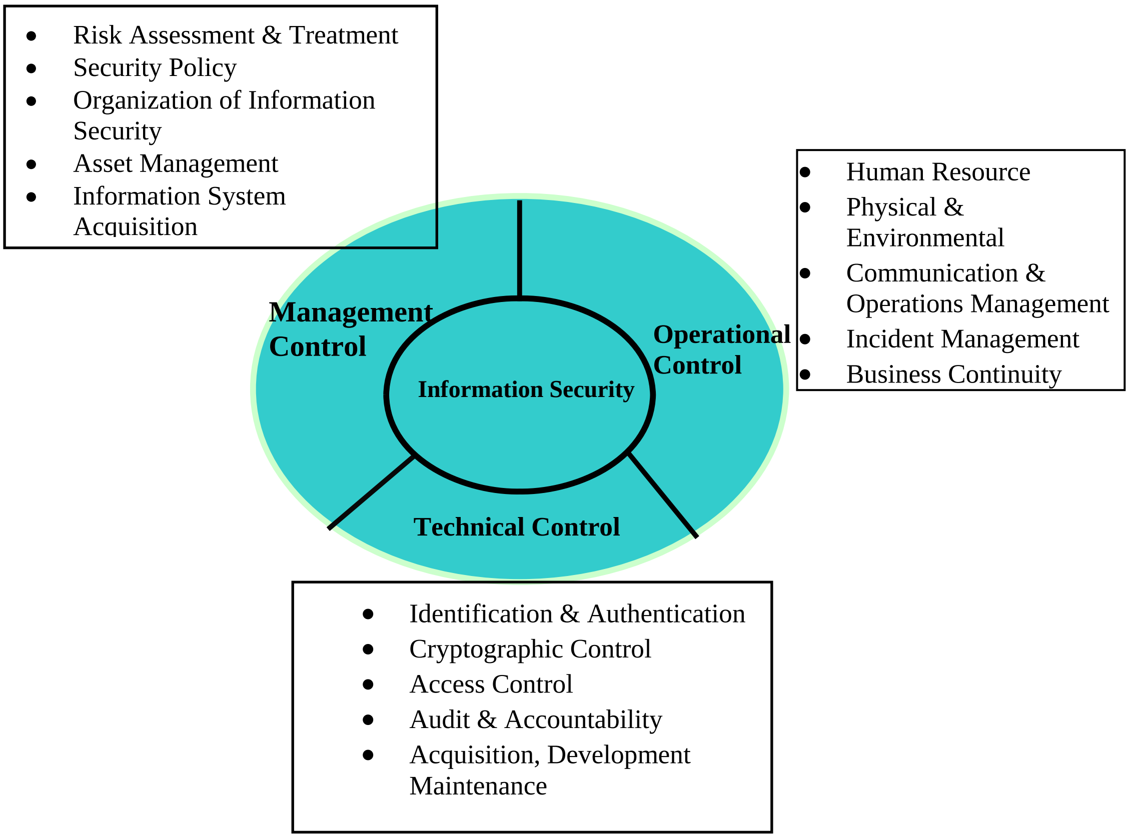
The degree to which the Government processes depend on the information supply has to be specified in quality requirements for the information supply. In that sense, information security must, therefore, form an integral part of an E-Governance overall quality management and quality assurance procedures.

To get the complete security assurance the subject needs to be dealt at various levels:

- ➢ Component level (Operating system, routers, switches etc.) security (ISO 15408)
- ➢ Application level (Basic application for access control, authentication and audit trail etc.) security
- ➢ System level (Physical security, communication and operation management, business continuity management etc.) security (ISO 27001)

The security can be assured by Conformity assessment to the best practices by combination of testing application (Application Security) product with IT Security function (e.g. operating system, network, distributed system). System level security can be assessed by taking Information Security Management standard as a reference.

Information Security Management System



- Risk Assessment & Treatment
- Security Policy
- Organization of Information Security
- Asset Management
- Information System Acquisition

- Human Resource
- Physical & Environmental
- Communication & Operations Management
- Incident Management
- Business Continuity

- Identification & Authentication
- Cryptographic Control
- Access Control
- Audit & Accountability
- Acquisition, Development Maintenance

Quality Gate 4 – Application Management

An application performs those specific functions that directly support the execution of service functions, processes and procedures. Applications, along with data and infrastructure components, such as hardware, the operating system and middleware, make up the technology components of IT system that in turn are part of an IT service. Application Management is viewed Service Management perspective and together. Application and IT Service should deliver Business functionality of (Government services) throughout the lifecycle. The quality requirements include:

- Functional requirements (including regulatory compliances)
- Non-functional requirements

Quality of software application can be ensured by using well-established models and methods for evaluating software characteristics both functional and non-functional. The most important part is the ensuring adequacy of the requirements as specified in software requirements specification and evaluation of the software product from using process data and product test results.

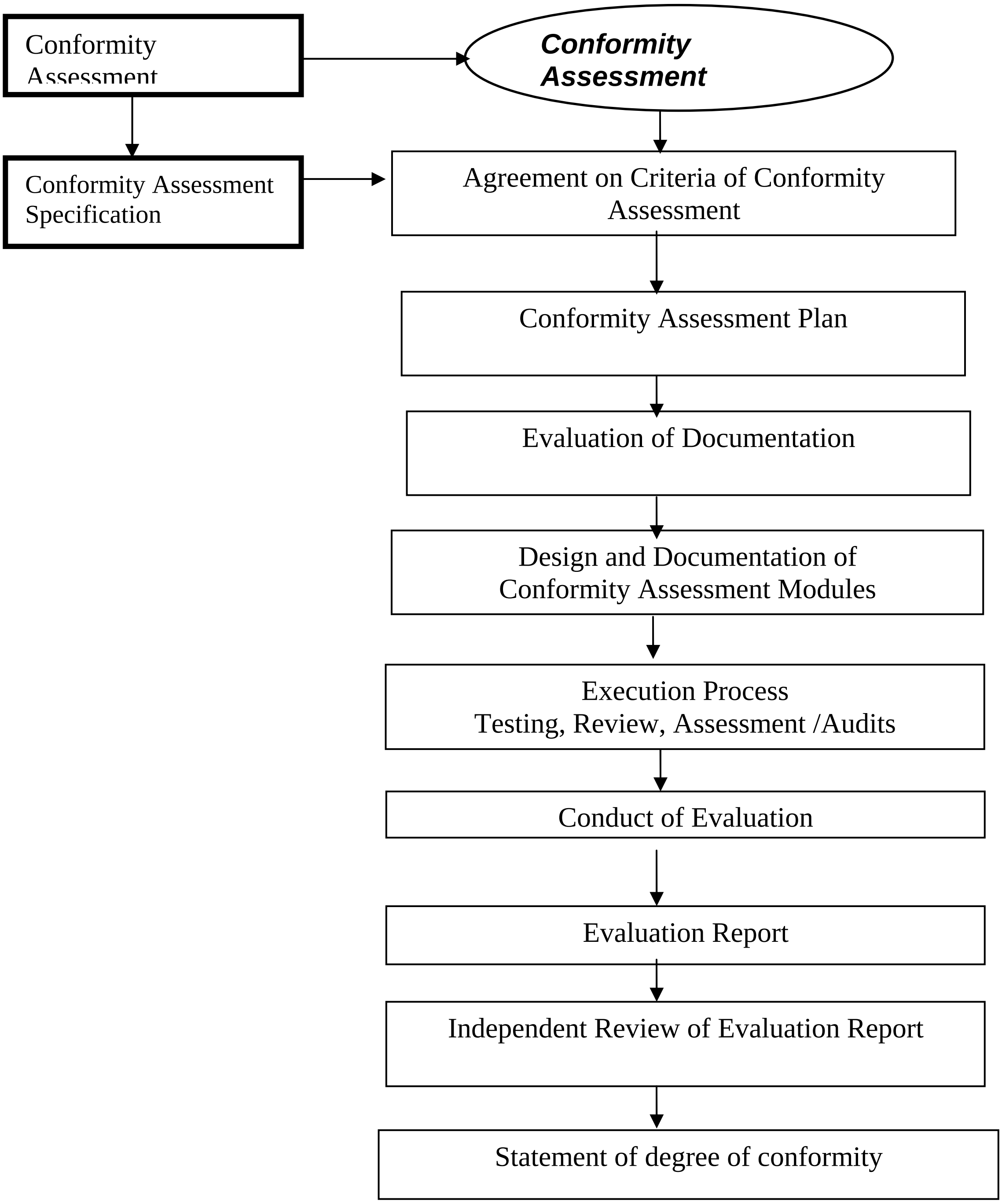
The quality of software products can be described in terms of quality characteristics as described in Quality Model ISO/IEC 9126-1. These are

- Functionality
- Reliability
- Usability
- Efficiency
- Maintainability
- Portability
- Security
- Documentation

However, in general it is not practical to assign measurement values directly to these characteristics. Instead, a set of software quality attributes of the Software product is selected that represents the main aspects of the characteristics. Measurement values of these attributes give a quantitative representative of the quality of the software products. Hence,

- Quality Model to be based on ISO/IEC 9126-1
- Application Quality is basic requirement for successful eGovernance.
- Quality model is applied to evaluate key Quality Characteristics like Functionality, Security, Reliability, Usability, Performance with special emphasis on Document Quality.
- Testing is done in a controlled laboratory environment and latest test tools to ensure that results are repeatable & reproduceable.

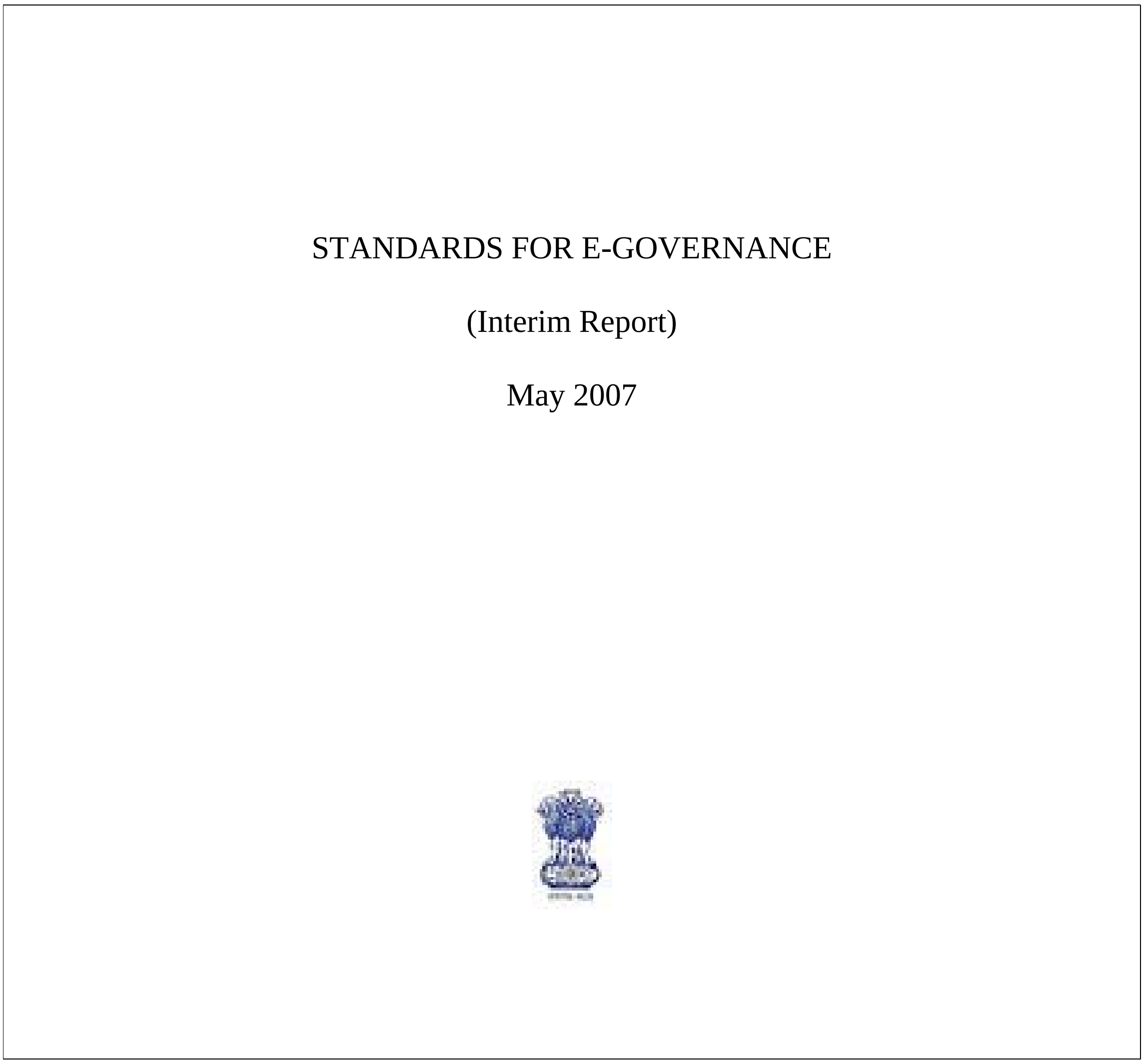
Process Flow (S/W Quality Evaluation)


Conformity Assessment
Conformity Assessment
Conformity Assessment Specification
Agreement on Criteria of Conformity Assessment
Conformity Assessment Plan
Evaluation of Documentation
Design and Documentation of Conformity Assessment Modules
Execution Process
Testing, Review, Assessment /Audits
Conduct of Evaluation
Evaluation Report
Independent Review of Evaluation Report
Statement of degree of conformity

Conformity assessment Framework Validations by STQC–

- MCA 21 Project:
  - Testing & Evaluation of following critical components of the project:
    - Software Application
    - Information Security
    - Service Level Metrics
    - MCA Gateway
    - IT Infrastructure (Hardware, Software & Network)
    - Project Documentation
    - Processes (Development, Operation & Maintenance)
  - Compliance with RFP and contract requirements by rigorous testing, audit & evaluation process and ensuring satisfactory closures of all the reported anomalies.
- Municipality Applications
- Land Record Information System, National Informatics Center
- Treasuries Software of Madhya Pradesh Government
- ENVISION, Ministry of Environment & Forest

ANNEXURE X - STANDARDS FOR E-GOVERNANCE - INTERIM REPORT



STANDARDS FOR E-GOVERNANCE

(Interim Report)

May 2007

Ministry of Communication & Information Technology
Department of Information Technology
National Informatics Center
New Delhi

Table of Contents

The draft recommendations are available on the e-Governance standards website http://egovstandards.gov.in. To access, kindly use the following USERID & PASSWORD

USERID:	**egovstd**
PASSWD:	**interim**

1. Introduction

The Department of Information Technology (DIT), Government of India (GoI) is driving the National e-Governance Plan (NeGP) which seeks to create the right governance and institutional mechanisms, set up the core infrastructure and policies & standards for implementation of a number of Mission Mode Projects (MMPs) at the Center, State and Integrated service levels to create a citizen-centric and business-centric environment for governance.

Under the NeGP, one of the key objective is **to cooperate, collaborate and integrate information** across different departments in the States and the Centre, which would help in delivering prompt services to the citizens, businesses and other Government departments, in a manner that simplifies Government processes and aggregates different inter-related services amongst various departments. A key driver in this vision has therefore been the need to harness the rich information assets of the Governments in the Centre and States in policy making, towards accelerating the economic growth of the nation as a whole.

Standards for e-Governance are a critical activity to ensure integration and interoperability of data and e-applications. While a lot of work has been done under the Standardization activity of GoI and various drafts are ready, formal approval process is underway. Further, with the Core Infrastructure like Citizen Service Centres (CSCs), State Wide Area Network (SWAN), State Data Centre (SDC) and National E-Governance Service Deliver Gateway (NSDG- Standards based messaging switch) being implemented as shared infrastructure for various MMPs, it is important to provide a top level architecture view of how these components could be used at various levels in the Government.

This interim report on Standards addresses some of the above components as an interim measure pending formal approval of the draft standards. The eGovernance standards given in the document are under draft stage pending formal approval by the Apex Body for standardization. .

2. Need for this interim document

In the past one year, a lot of ground has been covered by way of workshops, white papers and draft recommendations for eGovernance Standardization. While it would take sometime for various standards/specifications to move from present draft stage to approved stage, considering the immediate need and relevance of standards based approach in the implementation of various mission mode projects, it is proposed to prepare a this interim document compiling the draft technical specifications prepared by the Working Groups on Standards This will help various MMPs, which are at the conceptualization stage to take advantage of these standards and proceed on a standards based approach.

Note: This document is only an interim measure pending a formal recommendation by the Standards Apex Body and the associated sections of this document will be overridden by such recommendations.

3.Target Audience

This document is meant for

- Mission leaders of various MMPs at the Central and State Govt who are at the early stage of conceptualization of their projects and are preparing their Detailed Project Proposal /Request for Proposal (RFP)
- Programme Monitoring and the Project Appraisal team of EG PMU, DIT
- State and Central Projects who are wanting to deliver integrated services
- NLSA for CSCs
- National Informatics Centre (NIC)
- Implementation vendors to ensure compliance to standards
- Third party audit and certification agencies.

4. Standards for e-Governance: Initiatives by the Govt. of India

The Department of Information Technology (DIT) under the Ministry of Communications & Information Technology had constituted a Core group on Standards to arrive at an Institutional Mechanism and Processes to be put in place for the key areas for standardization for speedy implementation of E-Governance. The Institutional mechanism and processes have been put in place by DIT and some of the Key priority areas of immediate concern that have been identified for Standardization are:

1. Technical Standards and e-Governance Architecture
2. Network and Information Security Standards
3. Localisation of Applications & Language Technology Standards
4. Meta data and Data Standards for Applications domain
5. Quality & Documentation Standards
6. Legal Enablement of ICT Systems
7. Process Standards

5. Institutional mechanism and processes setup

As regards the Institutional mechanism and processes are concerned, an Apex body has been constituted under the chairmanship of Secretary, DIT with senior representatives from Government, NASSCOM, Bureau of Indian Standards (BIS), etc. with a mandate to approve, notify and enforce the Standards formulated by various Working Groups and to oversee that they are in accordance with international practices in this regard.

National Informatics Centre (NIC) has been entrusted with the task of originating white papers on all the desired standards and Steering the Process for evolving Standards. A separate “e-Governance Standards Division” has been created by NIC to steer the process of evolving the Standards.

Working Groups have been constituted in all the areas mentioned above with members from DIT, NIC, Associations, Industry, Academia, representatives from Central & State Government etc.

Once the Apex Body approves the standards developed by Working Groups, STQC –(Standardization, Testing and Quality Certification, Directorate of DIT with offices across the country), will be responsible for release of these approved Standards on the web and make them available to all the stakeholders for free download. STQC will further ensure conformance & certification (where required) of these standards. A separate "e-Governance Division" has been created by STQC for this purpose. Subsequent to the issuing of these initial standards, STQC is responsible for liaisoning with BIS to make these standards as National standards and ensure compliance.

The e-Governance Division of NIC and STQC function in close coordination with e-Governance PMU of DIT, which is responsible for overseeing their working.

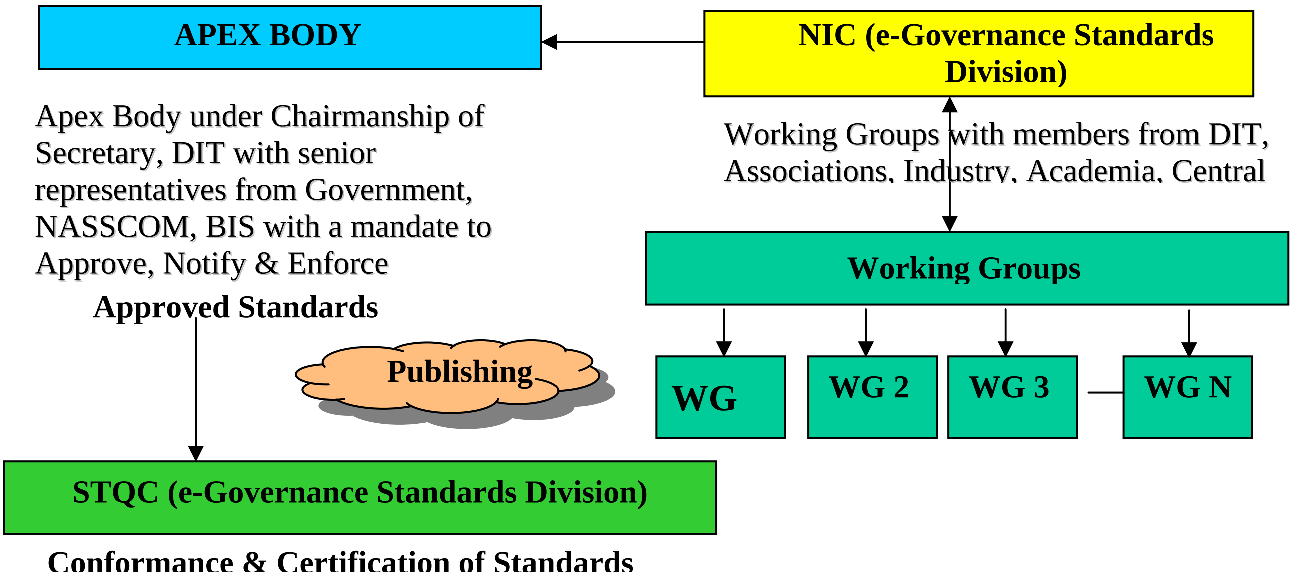

APEX BODY
NIC (e-Governance Standards Division)
Apex Body under Chairmanship of Secretary, DIT with senior representatives from Government, NASSCOM, BIS with a mandate to Approve, Notify & Enforce
Working Groups with members from DIT, Associations, Industry, Academia, Central
Working Groups
Approved Standards
Publishing
WG
WG 2
WG 3
WG N
STQC (e-Governance Standards Division)
Conformance & Certification of Standards

Fig 1: Institutional Mechanism

6. Current status on Standards for e-Governance

Out of the seven areas, following six Working Groups (WGs) have been constituted. The broad areas and outcomes of the Working Groups are as follows:

i. Technical Standards and E-Governance Architecture

- Considering the relevance of Enterprise Architecture based approach in implementing e-Governance projects, the group has prepared a draft document on Enterprise Architecture Framework.
- A draft Interoperability Framework for eGovernance has been prepared. This is key to any technical interoperability.

ii. Network and Information Security

- The group has recommended the ISO 27001/BS 7799 as the base standard to be used in various e-Governance implementations.
- Draft E-Governance Information Security Standard - Based on IS/ISO/IEC 27001 plus has been prepared**.**

iii. Localization and Language Technology Standards

- The group has prepared broad generic recommendations for Localization on OS support, Content creation, Fonts, Coding, Search Engine supporting local language etc.

iv. Metadata and Data Standards for Application Domains

- The group has identified the Generic Data elements including their formats, which are applicable horizontally to various e-Governance applications.
- The UNIQUE ID (UID) data elements are under review of the WG.

v. Quality and Documentation

- The Working Group has prepared a draft version of the Standards Formulation procedure document. This document is internal to the WGs detailing the complete process and procedure while evolving/adopting a standards right from the white paper to the approved standard stage.
- The group has also prepared a Conformity Assessment Framework guideline, which is extremely relevant for any e-Governance project. It details the various standards against which an independent 3rd party audit for compliance and certification of any e-Governance application would be done.

vi. Legal Enablement of ICT Systems

- Working Group constituted.

7. Policy on Open Standards

GOI is in the process of evolving a Policy on Open Standards, which will give a clear direction to all the players involved in the implementation of e-Governance applications on the choice of Technical specifications. A Specialist Committee constituted by the government is working on the same. Once the Policy is in place, the interoperability framework will be revisited to align with the Policy guidelines. The Policy is likely to be made available in the next two months. The objectives of formulating the policy on Open Standards are as follows:

i. Ensure interoperability
ii. Enable and facilitate Data preservation
iii. Avoid vendor lock-in and maximize technology choice
iv. Promote cost effective solutions
v. Ensure Integrated service delivery

8.Draft Recommendations from the Working Groups

8.1 Technical Standards & E-Governance Architecture

A. Enterprise Architecture Framework for NeGP Applications

In the present scenario of eGovernance applications, the developmental efforts are focused on specific departmental needs creating silos of information structures. From standardization of technology platforms to standardization of business processes, the IT systems have reached a stage where business is viewed in a holistic manner. There is an increasing awareness that in order to leverage technology to provide the desired benefits, it is important to have a transition to a broader "Enterprise" objectives rather than focus on singular needs of department/organization.

Enterprise Architecture

An Enterprise Architecture (EA) helps the departments to incorporate their best practices and experiences into key decision tools. EA acts as a bridge between the business and technology and provides a road map showing the relationships among the People, Processes, Data and Technology. EA ensures that all the players involved (Planners, designers, developers etc) share a common vision and common vocabulary thereby aligning the various process of enterprise (people, applications, data, technology) to business strategies and goals. The shared vocabulary is a first step toward integration and interoperability within and among organizations.

EA provides a central repository to capture, analyze and visually communicate information. It provides the ability to visualize the relationships among systems, applications, data and business processes and an integrated strategic information base for powerful decision-making.

A well-defined EA process helps to answer the basic questions as follows:

a) Is the current architecture supporting and adding value to the organization
b) Helps to document the current and future technology environment and gap between the two.
c) How might the architecture be moved so that it adds more value to the organization
d) Based on what we know about what the organization wants to accomplish in the future, will the current architecture support or hinder that
e) New decisions on IT investments.
f) Increased portability of applications

Enterprise Architecture normally comprises of business architecture, information architecture, technology architecture and application architecture.

Enterprise Architecture Framework

The Framework provide a classification system for EA and a systematic check list of people, systems, processes and internal and external factors that contribute to an organization's strategies and operations. Frameworks help to simplify the development process into discrete, understandable pieces and enable organizations to determine which systems and applications are tied to business needs.

The WG "Technical Standards & E-Governance Architecture" has evolved a Enterprise Architecture Framework that is suitable for NeGP. Several popular frameworks like Zachman, TOGAF, Federal Enterprise Architecture (USA) etc were considered while evolving this Framework

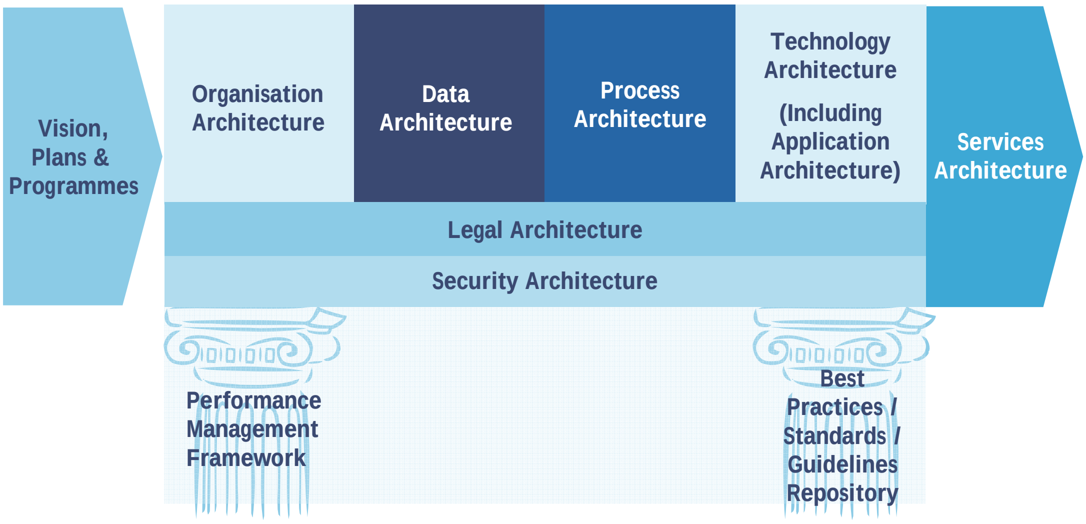

Vision, Plans & Programmes
Organisation Architecture
Data Architecture
Process Architecture
Technology Architecture (Including Application Architecture)
Services Architecture
Legal Architecture
Security Architecture
Performance Management Framework
Best Practices / Standards / Guidelines Repository

Fig2: The NeGP-EA

Enterprise Architecture and the NeGP EA Framework together with the analytical tools and methods deliver information that can be used to improve technology and business decisions. Using the NeGP-EA Framework one can build a comprehensive repository of business strategy, business processes, organizational charts, technical inventories, system and interface diagrams, network topologies and the explicit relationships between them. These inventories and diagrams are tools to support decision making at all levels of the organization. A linkage of the various artifacts can help one to very clearly associate the process to the rules, to the applications drilling down to the related hardware and software. A change anywhere made during the entire chain will reflect the associated changes that would happen at several levels. Hence it can act as an extremely useful tool to arrive at the future state of the architecture after business process engineering. The framework brings out the various business processes, the organization chart, the rules and Principles and the associated applications. IT implementing agencies within a State can use this framework and build the application using the Enterprise Architecture approach and attain the benefits listed above.

Enterprise Architecture for e-District

e-District has at least six services, which are going to be common across the various districts in the State and also across the States. NeGP-EA Framework based Enterprise Architecture can facilitate arriving at common principles, rules, processes associated with the services, applications, standards, infrastructure etc. One can build the current architecture and the target architecture after the re-engineering processes see how it will impact the Business and IT architecture including the information flow. This will also help in making new investments reduce the IT maintenance cost, ensure re usability and use of standards. Thus, EA becomes a foundation for decision-making based on the traceable facts in the repository.

Agencies like Telelogic, NISG, Infosys (that has a separate EA division), TCS, WIPRO, Accenture, MASTEK are among the many, which can assist in building the top level EA framework which would be enough for any IT implementing agency within a State to use that and build the functional requirements and the system requirements leading to application development which aligns to the Business Processes and the Vision.

Recently, for the Commercial Taxes MMP and National Horticulture Mission Project, EA has been used to develop the transformation and change strategy at a Central-level, and also to provide technology architectural guidelines and principles to guide the IT investments at state-levels, aligned to the EA.

Current status of Enterprise Architecture Framework for NeGP

The detailing of the NeGP EA Framework along with the methodology for implementation is presently being prepared. Reference implementation in the National Horticulture Mission Project is also being carried out for validation in E-Governance applications.

B. Interoperability Framework for E-Governance (IFEG)

The Interoperability framework for E-Governance (IFEG) defines the ICT standards and technical specifications, policies and guidelines governing the data exchange, interconnection, access and integration of systems within government and with entities interacting with the Government.

The Interoperability Framework aims to define the set of specifications to facilitate Government systems to communicate and interoperate with other systems, both within Government and those external to it, in an efficient and effective way. By bringing together the relevant specifications under an overall framework, IT management and software developers have a single point of reference when ever a need arises to locate the required interoperability specifications that should be followed for a specific project. By adopting these interoperability specifications, system designers can ensure interoperability between systems while at the same time have the flexibility to select different hardware, and systems and application software to implement solutions.

The four primary domain layers through which two or more applications can interoperate are:

- Access Domain
- Presentation Domain
- Process Domain
- Data Integration Domain

The IFEG is being evolved by consensus between industries, Government, academics, individuals etc through the Working Group on “Technical Standards and eGovernance Architecture” constituted by DIT to evolve eGovernance Standards for India. The IFEG is an integral part of the Enterprise Architecture also being developed by the same Working Group.

The Working Group has adopted existing International Open and de-facto standards and specifications instead of creating new standards.

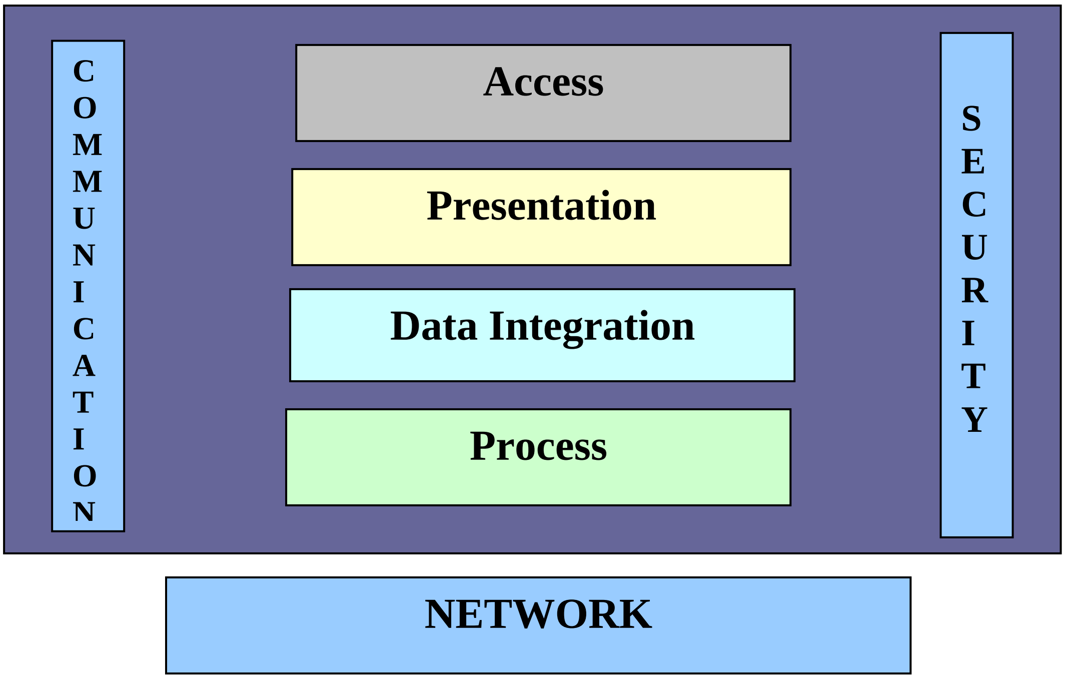


Fig 3: IFEG Layered Architecture Model

The *Fig 3* depicts the layered model for application development to support

the interoperability framework as envisioned. The top layer shows different applications that need to inter operate.

Each application is envisioned to consist of multiple logical layers, where each layer performs a specific task. However, an application may not necessarily have all the logical layers. In addition, two or more layers may be combined to form a single layer. Figure shows four primary logical layers, comprising of access layer, presentation layer, process layer and data layer through which two or more applications can interoperate.

The access layer covers what is required for achieving interoperability between different access media and applications. The presentation layer handles representation of information and data to the end user. The process layer is where the core business logic of an application is captured. The data layer handles the core transactional data of an application.

The remaining elements of the diagram, namely, communication, network and security are common across all the applications and depict the communication medium for an application, the network on which an application operates and the security infrastructure of an application.

Table 1 given below gives the Interoperability areas in the IFEG and also the standards and specifications recommended for each area.

i. Information Access Domain

Interoperability Area	Specification	Owner
Information Access for Client applications		
WAN	IP v4	Iana /internic
	IP v6	Iana /internic
Wireless	IEEE802.11b	IEEE
Transport Layer (OSI Layer 4) Layer	TCP	ISO/OSI
	UDP	ISO/OSI
Network Layer (OSI Layer 3)	IP	ISO/OSI
Mobile Access		
	GPRS	ETSI
	WAP	OMA
	SMS	ETSI
	MMS	ETSI
	3G	ITU

ii. Presentation Domain

Interoperability Area	Specification	Owner
Document type for Web publishing content	HTML 4.01	W3C
	XHTML 1.0	W3C
Distributed Authoring and Versioning	WebDAV	IETF
Content for Mobile Devices	WML 1.3	OMA
	XHTMLBasic v1.0	W3C
	XHTML Mobile Profile V1.1	OMA
Style Sheets	CSS2	W3C
Extensible Style Sheets	XSL v1.0	W3C
Document Type for Text	.odt v1.0	ISO/IEC 26300:2006
	.txt	W3C
	Open XML	ECMA
	PDF	Adobe
Document Type for Presentation	.odp v1.0	ISO/IEC 26300:2006
	Open XML	ECMA
Document Type for Spreadsheet	.ods v1.0	ISO/IEC 26300:2006
	OpenXML	ECMA
Graphics	JPEG2000	ISO/JPEG Committee
	PNG	PNG
	SVG v1.1	W3C
	ECW	ER Mapper
Moving Image	MPEG-1/2	ISO/IEC JTC1/SC29/WG11
Animation	X3D	W3C
Audio	OGG Vorbis	Xiph Foundation
Video	OGG	Xiph Foundation
Character Set and Encoding for Web Content	UTF-8 /16/ 32	Unicode Consortium /ISO/IEC 10646
Character Set and Encoding for other types of Information Exchange	UTF-8 /16/ 32	Unicode Consortium /ISO/IEC 10646
Geographical Information System	GML3.0	Open GIS Consortium

iii. Process Domain

Interoperability Area	Specification	Owner
Business Process Execution Language for Web Services	BPELWS 1.1	OASIS
XML Process Definition Language	XPDL 1.0	WFMC
Business Process Definition Metamodel	BPDM RFP	OMG
Business Rules Management	BRM RFI	OMG
Business Semantics of Business rules	BSBR RFP	OMG
Production Rule Representation	PRR RFP	OMG
Business Process Modeling Notation	BPMN 1.0	BPMI

iv. Information Domain: Data Integration

Interoperability Area	Specification	Owner
Data Schema Definition	XML Schema Part 1: Structures, XML Schema Part 2:Datatypes	W3C
Data Transformation for Presentation	XSL 1.0 6 XSL 1.1	W3C W3C
Data Transformation for conversion from XML schema format to another format	XSLT 1.0 7 XSLT 1.1 XSLT 2.0	W3C
Data Modeling Language	ISO/IEC 19501:2005 (UML 1.4.2), UML 1.5, UML 2.0	OMG
Data Description Language (for exchange of data)	XML 1.1 9	W3C
E-Forms	XFORMS & XFDL along with XML related technologies like XSLT, XPATH, HTML, and XHTML.	

v. Information Domain: Meta data

Interoperability Area	Specification	Owner
Metadata Description Language	RDF 1.0	W3C
XML Metadata Interchange	ISO/IEC 19503:2005 , XMI 1.0, XMI 2.0	OMG

vi. Information Domain: Data Interchange

Interoperability Area	Specification	Owner
Web services description language	WSDL 1.1	W3C
Web service request delivery	SOAP 1.2	W3C
Web service request registry	UDDI 3.0 UDDI 3.0.1 UDDI3.0.1	OASIS OASIS OASIS
Web Services WS-I	WS1 – Basic Profile 1.1	WS-I
	WS1 – Basic Profile 1.2	WS-I
Web Services Security	WS1 – Basic Security Profile 1.1	WS-I
	WS1 – Reliable secure Profile 1.0	WS-I
	SOAP Message Security 1.0	OASIS
	Username Token Profile	OASIS
	X.509 Certificate Token Profile	OASIS

vii. Network

Interoperability Area	Specification	Owner
Internet Protocol	IP V4 / IP V6	IANA Internic
Wireless LAN	IEEE802.11b	IEEE
Routing Information	OSPF and BGP 4	IEEE
Video conferencing over IP	ITU H.261 and H.263	

viii. Security

Interoperability Area	Specification	Owner
Remote Login	ssh v.2	IETF
Secure Electronic Mail	S/MIME v3	Network Working Group/RSA LAB
Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL	HTTPS	Netscape
Security Architecture for Internet Protocol	IPSec	IETF
Secure Socket Layer	SSL V3.0	IETF
Symmetric Encryption Algorithms	DES 3DES AES	NIST
Digital Signature Algorithms	DSA RSA	NIST RSA Security Inc.
Secure Hash Algorithm	SHA-1	NIST/NSA
Message-Digest Algorithm	MD5	R. Rivest
Password-Based Cryptography Standard	PKCS#5	RSA Data Security, Inc

Cryptographic Message Syntax Standard	PKCS#7	RSA
Exchange of authentication and authorization information-Web Services Security	SAML v1.1	OASIS

ix. Communication

Interoperability Area	Specification	Owner
Hypertext Transfer	HTTP v1.1	IETF
File Transfer	FTP	IETF
E-mail Transport	SMTP	IETF
	MIME (Multipurpose Internet Mail Extensions)	IETF
Mailbox Access	POP3 / IMAP4	IETF
Directory Access	LDAP v3	IETF
Domain Name Services	DNS	IETF

x. Gateway

Interoperability Area	Specification	Owner
eGov Messaging Service Specifications (eGGMS)	Interoperability Interface Protocol (IIP)	Government
	Interoperability Interface Specifications (IIS)	Government
	Inter Gateway Interconnect Specifications (IGIS)	Government
	Gateway Common Services Specifications (GCSS)	Government

xi. Data Preservation - In view of the fact that Government data has to be preserved for a large duration, standards for documents storage/archival must be based on the Policy framed by the Govt. of India.

The complete draft on IFEG is available at http://egovstandards.gov.in under “Technical Standards and E-Governance Architecture”. You can access the document using the following USERID and PASSWORD.

USERID: **egovstd**
PASSWD: **interim**

The draft on IFEG would be revisited once the government policy on Open Standards is in place and formal approval sought.

8.2 Network and Information Security Standards

The Network and Information Security WG has proposed the use of BS 7799 / ISO 27001 standards by e-Governance applications. This is in line with the Security policy issued by DIT to all critical sector organizations. The security policy additionally addresses the periodic measure to be taken to ensure security. As per the Policy, all the Govt Ministries/Dept. are expected to follow this policy in the spirit of proposed amendments to Indian IT Act 2000. A copy of this policy can be downloaded from http://egovstandards.gov.in website.

Information security policy issued by DIT

In order to reduce the risk of cyber attacks and improve upon the security posture of critical information infrastructure, Government and critical sector organizations are required to do the following on priority:

- Identify a member of senior management, as Chief Information Security Officer (CISO), knowledgeable in the nature of information security & related issues and designate him/her as a ‘Point of contact’, responsible for coordinating security policy compliance efforts and to regularly interact with the Indian Computer Emergency Response Team (CERT-In), Department of Information Technology (DIT), which is the nodal agency for coordinating all actions pertaining to cyber security
- Prepare information security plan and implement the security control measures as per IS/ISO/IEC 27001: 2005 and other guidelines/standards, as appropriate

- Carry out periodic IT security risk assessments and determine acceptable level of risks, consistent with criticality of business/functional requirements, likely impact on business/functions and achievement of organizational goals/objectives.
- Periodically test and evaluate the adequacy and effectiveness of technical security control measures implemented for IT systems and networks. Especially, Test and evaluation may become necessary after each significant change to the IT applications/systems/networks and can include, as appropriate the following:
  - Penetration Testing (both announced as well as unannounced)
  - Vulnerability Assessment
  - Application Security Testing
  - Web Security Testing

- Carry out Audit of Information infrastructure on an annual basis and when there is major Upgradation/change in the Information Technology Infrastructure, by an independent IT Security Auditing organization

Note: *Government and critical infrastructure organizations can make use of CERT-In evaluated and empanelled third party agencies for their organization/site specific IT security assessment services (including ISMS assessment, risk assessment, network security profiling, penetration testing, vulnerability assessment, application security testing etc) under specific contract and pre-determined rules of engagement. Contact* *details of the agencies empanelled by CERT-In are available at 'http://www.cert-in.org.in'*

- Report to CERT-In cyber security incidents, as and when they occur and the status of Cyber security, periodically

The Working Group has also prepared a Draft Information Security Plus document that includes additional controls required for E-Governance Applications. This is currently under review.

The complete Security Policy is available on the eGov Standards portal http://egovstandards.gov.in/. You can access the document using the following USERID and PASSWORD.

USERID: **egovstd**
PASSWD: **interim**

8.3 Localization & Language Technology Standards –

This section highlights some of the recommendations made by the WG on Localisation and Language Technology with regard to localization and language technology applications in India, especially in the context of e-Governance.

Localization & Language Technology Standards for National e-Governance Plan

Issue	Present Status/Standard	Need of Standardization for NeGP	Recommendations & Roadmap
Encoding	**ISCII, Unicode and Proprietary codes are in use.**	**Unicode**	**Unicode characters are almost complete to suffice the respective language requirements.**
Keyboard Layouts	**INSCRIPT keyboard layout.**	**INSCRIPT keyboard layout.** **Note: Existing INSCRIPT standard should be upgraded to include new Unicode code points for all Indian Scripts.**	**Typewriter keyboards shall also be supported for some time, purely for backward compatibility, to cater the need of those who are master in the typewriter keyboard.** **Roman-Phonetic keyboard should also be supported to facilitate Indian Language users who do not type the language matter in INSCRIPT & Typewriter keyboard layouts.** **Keyboard layouts already standardized by State Governments should also be supported (KGP keyboard layout for Kannada, TAM99 for Tamil).** **Note: Output of any user specific keyboard layout must conform to Unicode current version. Specification for non-INSCRIPT keyboard layouts should be made available by either TDIL/CDAC.**
Font	**No Fonts are standardized so far.**	**Cross platform Open Type Fonts must be used in National e-Governance Plan applications.**	**1. Customers should only adopt fonts that have been tested on different platforms for the relevant scripts.** **2. Proprietary fonts should not be adopted unless the vendor assures interoperability.**

			3. Vendors should ensure that the fonts provide the complete glyph-set and associated tables for the end-result to be met.
Content Creation - Browser Support	**So far no standardized Content Creators available.**	**W3C Standard**	**Adoption of W3C specifications. All citizen interfaces should carry the W3C certified logo.**
Search/ Cross Lingual Search/ Transliteration	**There is no existing standard so far.**	**There is no existing standard for Search/ Transliteration.** **If database/ contents are in Unicode/W3C format, then there is no problem in Search.**	Transliteration tools in the NeGP are extremely important since it is presumed that a large part of the information on the identity of users will be in their local languages. Therefore, at the very least this information will have to be transliterated into the scripts of users of this information in different states. For example, a Smart-Card based driving-license issued by an Regional Transport Office may serve a restricted purpose if any information in one script cannot be read in different parts of the country. Though there are other examples, the criticality of a 'perfect' transliteration tool will depend on the criticality of local language data in a given NeGP application.

For details pl. read the White Paper on Localization & Language Technology Standards prepared by the WG, which is available on the eGov Standards portal http://egovstandards.gov.in/. You can access the document using the following USERID and PASSWORD.

USERID:	**egovstd**
PASSWD:	**interim**

8.4 Metadata & Data Standards for Application Domains

There is an immediate need for having Data and Metadata Standards for Generic elements like Name, address, etc which are common across e-Governance applications and for various government domains. In the absence of these, there is no consistency on the various data formats used leading to difficulties in Data sharing, Search and Query across databases etc.

The Working group has identified the following

1. Generic Data elements including their formats, which are applicable horizontally to various e-Governance applications.
2. Unique ID (UID) elements
3. Metadata Elements

A. Summary Format of the Data elements for Common Data elements (Generic)

Data Element	**Parts if any**	**Business Format**
Amount		Number (15,2)
Caste Category (Default Value "OC")		VARCHAR (2)
Organization Name		VARCHAR (255)
Organization Type		VARCHAR (2)
Economic Status		VARCHAR (1)
Education		VARCHAR (3)
Email ID		VARCHAR (255)
Financial Year		VARCHAR (7) Format YYYY-(YY+1)
House Hold category		VARCHAR (1)
Language Name		VARCHAR (2)
Measurement	Distance	Number (12,3)
	Area	Number (12,3)
	Volume	Number (12,3)
Occupation		VARCHAR (2)
Payment Details		VARCHAR (2)
Period Duration		CHAR (10) format YYYY-MM-DD
Religion Code		VARCHAR (2)
Telephone Number		VARCHAR (15)
Calendar Year		VARCHAR (4), YYYY

B. Unique ID Element details as per the recommendations of the Sub-Group

Elements	Parts if any	Business Formats
Person Name	Title (English) Person Full Name (English) Title (Local Language) Person Full Name (Local Language)	VARCHAR (25) VARCHAR (75) VARCHAR (50) VARCHAR (150)
Address	Address 1 Address 2 Address 3 Pin Code	VARCHAR (75) VARCHAR (75) VARCHAR (75) VARCHAR (6)
Relationship	-	Number (2)
Unique Village Code	-	VARCHAR (8)
Unique Town Code	-	VARCHAR (8)
Hamlet Code	-	Number (6)
Unique Ward Code	-	Number (6)
State Code	-	VARCHAR (3)
Country Code	-	VARCHAR (3)
Date	-	CHAR (10) format YYYY-MM-DD
Date of Birth (DOB)	-	CHAR (10) format YYYY-MM-DD
Place	Country or State/District/village	VARCHAR (15)
Place of Birth (POB)	Country if not born in India or State/District/village	VARCHAR (15)
Gender	-	CHAR (1)
Marital Status	-	VARCHAR (1)
Signature	-	BLOB
Facial Identification	-	BLOB
Finger Print	FINGER ID1 FINGER PRINT IMAGE1 FPCLA1 FPPK1	Number & BLOB

The above draft is yet to be approved by the WG chair and the Apex Body for Standardization (Chaired by Secretary, DIT). The complete draft is available on the eGov Standards portal http://egovstandards.gov.in/. You can access the document using the following USERID and PASSWORD.

USERID:	**egovstd**
PASSWD:	**interim**

9. Policy for Identity and Access Management

The need for security and privacy, demand for online services, and issuance and management of digital identities, to make e-Government Programs and their services a reality is being increasingly felt. This requires, among the others, **an integrated framework** of laws, policies, operational best practices and guidelines, technology, and institutionalization. The policy document prepared by the Task force on "Identity and Access Management " is targeted for government agencies and private businesses in formulating best practices and standards and enforcing these across different platforms. One of the key objectives is to mitigate the cost of maintaining multiple identity repositories that may exist by achieving unambiguous mapping of identities representing the same entity or multiple entities collaborating together. The integration of identity and access management services provides personalized security and access rights based on an individual's identity. Identity management automates the provisioning and de-provisioning of user accounts and authentication, authorization and auditing capabilities.

The entire policy is available at http://egovstandards.gov.in. You can access the complete document using the following USERID and PASSWORD.

USERID:	**egovstd**
PASSWD:	**interim**

The draft policy has the following key recommendations:

- The rules, regulations, instructions, manuals and records of Government of India should include detailed guidelines for government agencies to implement Identity and Access Management System while providing online services. It should also help government agencies and other stakeholders to understand potential risks involved and requirements to address them while adopting the Identity and Access Management solutions.
- Laws specific to address Identity and Access Management issues like identity theft, online fraud, authentication, authorization, integrity, non-repudiation, protection of privacy, confidentiality, etc should be formulated or necessary amendments should be made in existing laws with the help of members from law and IT fraternity
- The governance structure should be set up to oversight and manage the current and future Identity needs of various Government organizations
- The IAM architecture should be based on standard protocols, guidelines and best practices to ensure the interoperability and consistency.
- The Identity Information is stored by multiple agencies in multiple documents like Ration card, Driving License, Passport, Voter's card, Birth Certificate etc. The purpose of the Project Unique ID (UID) initiated by the Planning Commission is to create a central database of resident information and assign a Unique Identification number to each such resident (Citizens and Persons of Indian Origin) in the country. The outcome of this project may act as input to the Identity and Access Management System.

- The appropriate Identity Aggregations and Synchronization should be used to integrate systems to share their identity information.
- Single sign-on should be provided to the citizens accessing e-Government services.
- Risk Assessment should be carried out to identify the impact that may result from accepting fraudulently asserted identity. Risk assessment involves identification of resources, identification of threats and identification of vulnerabilities that might be exploited by the threats.
- Organizations should have Risk Management Plan in place if identity is compromised.
- Based on authentication assurance level requirements identity authentication credential types should be selected. Basic authentication should be used for services like request for specific information on government services, online discussion groups etc. Strong authentication should be used for the services which needs signing of documents and where it is very important to know the identity of the user for e.g. submission of duly signed reports. The detail classification is shown in Annexure – III.
- User should be provided with a consistent, comprehensive and integrated, easy-to learn user interface for presenting his identity.
- Automated provisioning and Self-service capabilities such as self-registration and changing password should be provided wherever possible to avoid administrative overhead.
- The mechanism for receiving a credential should be closely scrutinized for e.g. receiving password through an encrypted, direct channel, smart card after showing identification.
- Identity and Access Management should enforce the consistent application of policies for requesting and approving entitlements. The provisioning system should also provide audit trail that records when decisions and approvals were made and by whom.
- Orphaned accounts can be used for unauthorized access of resources. Hence these accounts should be disabled quickly in case complete deletion of these accounts is not possible. The IAM system should not just identify the orphan accounts, but must also take corrective actions automatically.
- IAM should automatically alter the privileges to access resources depending on change in job functions and authority. In order to avoid misuse, the privileges to access Government resources should be immediately revoked in case of the death of the citizen, or on expiry of the period for which privileges are granted.
- Security can be enhanced by policy enforcement such as
    - Requiring user to choose complex password which is difficult to guess but easy enough to remember eliminating the need to write it down, password of minimum length, change it frequently
    - Removing/disabling orphan accounts to avoid misuse of such accounts.
    - Session Time out – Termination of inactive session after a defined period of inactivity
    - Restriction on connection times for high-risk applications
    - Implementing strong authentication for sensitive and critical applications
    - Reducing attack surface
    - Dedicated, isolated computing environment for sensitive systems

  - Integrating and Consolidating the identity stores
  - Single Sign On to make it easier for user and avoiding the need for him to write down complex password since it becomes difficult to remember multiple passwords. Only in case of performing critical operation or accessing sensitive information user may be asked to provide credentials again.
- Privacy and integrity of the identity information should be maintained.
- To automate the processes, which span various government departments, agencies, divisions, the application of Identity Federation technology should be implemented.
- The policy should be reviewed at planned intervals or if significant changes occur to ensure its suitability, adequacy and effectiveness.

10. Policy on E-Forms

The draft Policy on E-Forms below is at the initial stage. Once it is approved after undergoing due process laid, the various recommendations will be acted upon. Hence, at this stage there is no National Repository or internal committees within the various Ministries /Departments.

Definition: *e-Form is an electronic form, which enhance and simplify data capturing with inbuilt data validation, data calculations, electronic signatures, and database integration.*

An e-Form is an electronic document that presents information and gathers responses to that information. e-Form can be downloaded unlike the traditional forms and can be filled and submitted. It supports offline filling and submitting e-Forms helping users where connectivity and bandwidth is an issue.

Benefits: It has been realized that use of e-Form technology can accelerate the e-governance initiative of the government of India, if it is used effectively. It can cut down the application development time and help the citizen in electronic preparation and filing of information for various govt. services. The entire set of policies; guidelines have been framed to help in achieving this objective.

Policy & Guidelines

- **Data Standards to ensure Interoperability:** While implementing e-Form, all the forms should be collected, data elements standardized and then new e-Form should be designed. This should be done by the designated e-Form task force.

- **National E-Form Repository / Registry of Dataset Schema:** The data standardized and e-Form designed by each Ministry / Dept should be registered with the National e-Form repository agency.

- **Uniformity of e-Form layout:** The e-Form task force setup in each Ministry / Dept should ensure uniformity of presentation styles across various e-Forms so that anyone familiar with one form can easily learn to use other forms.

- **Business Process Reengineering:** As introducing e-Form will involve, data standardization, designing of new version of forms, developing e-Form application and workflow automation, it is a good opportunity to re-look at the entire business process to simply and make it more efficient.

- **Standards for e-Forms Technology**: E-Form solutions should use open standards, preferably Xforms & XFDL along with XML related technologies like XSLT, XPATH, HTML, and XHTML. If the solution uses other standards, to ensure interoperability, e-Form should exchange data in XML and e-Form should be convertible to Xforms and vice versa

- **Online & Offline e-Form:** E-Form solution support should be both online as well offline e-Forms. The user should be able to down load the e-Form, fill it, keep it, print it and upload it as and when required. The uploaded form is signed before submission.

- **Protection of interest - users and organizations**: Use of electronic filing of information has the potential for easy manipulation of information. The integrity of electronic information has to be protected at all levels using digital signatures. The guidelines proposed have addressed this issue.

- **Submission & Acknowledgement - Digital Signing:** The e-Form along with attachments will be signed by the user using his / her digital certificate and uploaded. This will ensure that the information filed cannot be changed by anyone. The service provider will send an acknowledgement using their digital certificate. This will complete the submission cycle.

- **E-notary facilitation**: As all the user may not have digital certificate, e-notary services can be provided by a central agency at a national level. The user can submit the e-Form through the e-notary agency, which will sign the e-Form and send it to both the user and the service provider. E-notary agency will keep a copy for reference if needed

- **Support Attachments - unstructured data:** E-Forms should support attachments, which may be needed to fulfill all the requirements of an e-Form application. These may be various types of electronic documents including scanned images. Attachments and e-Form together form one object, which is digitally signed by the user (or signed by e-notary).

- **Workflow to support internal processes:** As the entire e-Form application and attachments are available in electronic form, it become a good case for workflow application. Appropriate workflow application should be designed and implemented, where each person can add more information, digitally signed and send to the next person in the process. Open source workflow technology should be preferred for implementing workflow application

- **Status tracking / notification (G2C):** As the e-Form will get into the workflow system and pass through the various steps of the process, status information should be accessible to the end user.

- **Integrity of E-Form, attachment and workflow information:** Integrity of e-Form along with attachment should be maintained using digital signature. When additional information is added in the workflow system, the original object and the added information will become another object, which is also to be digitally signed. This will ensure that no part of the information is tempered at any time.

- **Security & Privacy Issue (Roll based access):** The information filed by the user should be accessible based on the role to protect the privacy rights of the user. While transmitting the e-Form, to protect against snooping on the communication channel for very sensitive information, appropriate encryption technology should be supported by the service provider.

- **Multiple Devices Support:** The e-Form application should support multiple devices like PDA, Mobile phones etc to increase accessibility of the services.

- **Localization:** The e-Form based solution should support multiple languages so that users can use local language. This may require support of Unicode compliant solutions.

- **Archival and Content Management**: e-Form information also needs to be preserved like database information. Content management technology may be used for managing e-Form information on-line. After some time interval, it can be archived. It should be possible to retrieve the archived e-Forms as and when needed for reference. As archival may be for a very long duration, accessing information may become harder with time, as technology is changing rapidly. To ensure long-term access, archived information may have to be converted to open document standard format before archiving.

- **E-Form Management – catalog, version etc**: E-Form catalog needs to be maintained for reference. As forms may undergo revision, all versions will have to be maintained in the catalog. Older versions may be needed, as information in the system will exist in all the versions. In order to optimize, applications may separate the form and the content. In that case the form and version no information will be used by the application.

- **Scalability and Availability:** The solution built using e-Form technology should be scalable to meet the volume of transactions. The solutions should utilize or integrate with the digital access points available through Post Offices, Common Service Centers (CSCs) and information kiosks.

- **Integration with legacy Applications and Paper Submission:** It should be possible to extend or integrate e-Form based interface with the existing application. As all the users may not have access to digital medium, paper based form submission may also have to be supported. These can be digitized and entered into the e-Form application by the service provider.

- **Legal Status of E-Form:** Legal provision needs to be made so that e-Form is taken as a legal document the court of law in case of any dispute between the service provider and the end user.

- **Digital Certificate for G2G, G2B, G2E:** As digital signing of e-Forms and attachments if any and also the information added by various actors during the workflow is necessary, to maintain the integrity of information and linkages with person concerned (non-repudiation), digital certificate will have to be made available. It may not be practical to make digital certificate mandatory at end user (citizen) level because of the scale and cost. However, it can be made mandatory for all govt. functionaries and business organizations.

- **Organizational structures to facilitate accelerated implementation:** We need organizational structures at two levels. (1) National Level e-Form Steering Group and (2) Ministry/Dept Level e-Form Task force, with mandate to collect all the paper based forms, create Meta data for forms, data Analysis and standardization (Horizontal & Vertical), designing new versions of forms, register meta data of forms, data standards & e-Forms with National E-Form repository, development of e-Forms and workflow application etc.

- **Call Centre / Online help:** The help to end users of e-Forms should be available in form of e-learning materials on the web site of the service provider. On line help desk / call center should also be supported to provide the necessary help the end users.

- **Training: Capacity/Capability building:** To promote use of e-Form technology would require large-scale training programmes. Training programme can be more effective if well-documented case studies are developed for demonstration during the training programme.

- **e-learning materials for users of e-Form :** Self learning e-learning materials can be created to facilitate developing e-Forms and its applications. It could also have recorded lectures created using virtual classroom systems. Similar materials can also be created for end users of e-Forms.

- **Measures to foster Citizen adoption of e-Forms:** Experience abroad indicates that mere availability of e-Form does not promote its use. Each e-Form application will have to make its own strategy to promote its use by the end users. It may require media campaign, self-learning materials on web sites, trained personnel in CSC and other service outlets etc.

The entire draft policy is available at http://egovstandards.gov.in. You can access the complete document using the following USERID and PASSWORD.

USERID:	**egovstd**
PASSWD:	**interim**

11. Web Accessibility Standards

Web sites being developed make use of proprietary features of the tool sets and consequently become tightly coupled to the browser and Operating System, resulting in variances in performances under different browser and Operating System environments.

Web Accessibility Standards is to ensure access to web pages for everyone and address access issues for people using different technologies. The requirement of Web Sites is compliance of all Web Sites to the basic W3C standards and Web Accessibility standards. A site built to web standards should adhere to standards (HTML, XHTML, XML, CSS, XSLT, DOM, MathML, SVG etc) and pursue best practices (valid code, accessible code, semantically correct code, user-friendly URLs etc).The key objective is to have the site built to web standards be lean, clean, CSS-based, accessible, usable and search engine friendly.

Guidelines for Development of Web Sites:

a) Government Agencies must ensure that their web pages accessible by different types of assistive technologies. Text readers do not always support scripts and other programmed objects, which means that pages that use scripts are inaccessible.
b) Web developers must use technologies to resolve problems that are not addressed very well by existing technologies;
c) Web Developers should make the pages work with older browsers and must be accessible even if the user has turned off the scripting option.
d) Web page must use clear and consistent navigation mechanisms.
e) Ensure that users are able to interact with web page elements in a device independent manner.
f) Web page must provide a text equivalent for every non-text element and must ensure that the use and selection of color do not affect the information conveyed on a page.
g) All information published on a Government web page must be published in HTML, whenever possible, to eliminate the need for additional software.
h) The files (video and audio) used in the Web Sites must be optimized files to improve download time.

The sample checklist for developers is as below:

WEB STANDARDS CHECKLIST for Developers

1. Quality of code

1.1. Does the site use a correct Doctype?
1.2. Does the site use a Character set?
1.3. Does the site use Valid (X)HTML?
1.4. Does the site use Valid CSS?
1.5. Does the site use any CSS hacks?
1.6. Does the site use unnecessary classes or ids?
1.7. Is the code well structured?
1.8. Does the site have any broken links?
1.9. How does the site perform in terms of speed/page size?
1.10. Does the site have JavaScript errors?

2. Degree of separation between content and presentation

2.1. Does the site use CSS for all presentation aspects (fonts, color, padding, borders etc)?
2.2. Are all decorative images in the CSS, or do they appear in the (X)HTML?

3. Accessibility for users

3.1. Are "alt" attributes used for all descriptive images?
3.2. Does the site use relative units rather than absolute units for text size?

3.3. Do any aspects of the layout break if font size is increased?
3.4. Does the site use visible skip menus?
3.5. Does the site use accessible forms?
3.6. Does the site use accessible tables?
3.7. Is there sufficient color brightness/contrasts?
3.8. Is color alone used for critical information?
3.9. Is there delayed responsiveness for dropdown menus (for users with reduced motor skills)?
3.10. Are all links descriptive (for blind users)?

4. Accessibility for devices
4.1. Does the site work acceptably across modern and older browsers?
4.2. Is the content accessible with CSS switched off or not supported?
4.3. Is the content accessible with images switched off or not supported?
4.4. Does the site work in text browsers such as Lynx?
4.5. Does the site work well when printed?
4.6. Does the site work well in Hand Held devices?
4.7. Does the site includes detailed metadata?
4.8. Does the site work well in a range of browser window sizes?

5. Basic Usability
5.1. Is there a clear visual hierarchy?
5.2. Are heading levels easy to distinguish?
5.3. Does the site have easy to understand navigation?
5.4. Does the site use consistent navigation?
5.5. Are links underlined?
5.6. Does the site use consistent and appropriate language?
5.7. Do you have a sitemap page and contact page? Are they easy to find?
5.8. For large sites, is there a search tool?
5.9. Is there a link to the home page on every page in the site?
5.10. Are visited links clearly defined with a unique color?

6. Site management
6.1. Does the site have a meaningful and helpful 404-error page that works from any depth in the site?
6.2. Does the site use friendly URLs?
6.3. Do your URLs work without "w