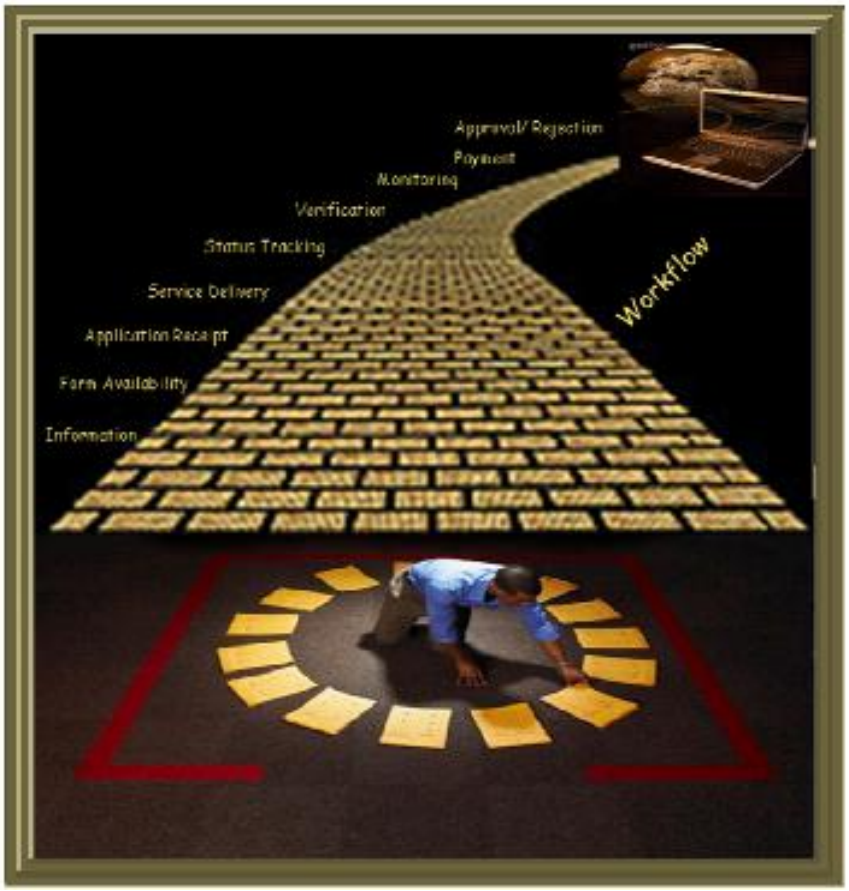
REQUEST FOR PROPOSAL FOR SELECTION OF SYSTEM INTEGRATOR FOR STATE WIDE ROLLOUT OF e-DISTRICT MMP

VOLUME II

RFP No: OCAC-TJ-11/2012/ENQ/14019 Dated: 06.08.2014



General Manager,
Odisha Computer Application Centre (OCAC),
(Technical Directorate under IT Department, Govt. of Odisha), OCAC Building, Plot No. N-1/7D, Acharya Vihar Square, RRL Post Office,
Bhubaneswar – 751 013, Odisha
Website: http://www.ocac.in/

Table of Content

GLOSSARY OF TERMS

The definitions of various terms that have been used in this RFP are as follows:

- "**Request for Proposal (RFP)**" means all three Volumes and its annexures and any other documents provided along with this RFP or issued during the course of the selection of bidder, seeking a set of solution(s), services(s), materials and/or any combination of them.

- "**Contract / Agreement / Contract Agreement / Master Service Agreement**" means the Agreement to be signed between the successful bidder and OCAC, including all attachments, appendices, all documents incorporated by reference thereto together with any subsequent modifications, the RFP, the bid offer, the acceptance and all related correspondences, clarifications, presentations.

- "**Bidder**" means any firm offering the solution(s), service(s) and /or materials as required in the RFP. The word Bidder when used in the pre-award period shall be synonymous with parties bidding against this RFP, and when used after award of the Contract shall mean the successful party with whom the agreement is signed for rendering of services for implementation of this project.

- "**Proposal / Bid**" means the Pre-Qualification, Technical and Commercial bids submitted for this project against this RFP.

- **"Acceptance"** means the Government's written certification that following installation, the system(s) (or specific part thereof) has been tested and verified as complete and/or fully operational, in accordance with the acceptance test defined in the Acceptance Test Documents.

- **"Acceptance Test Documents"** means a mutually agreed document which defines procedures for testing the functioning of the e-District system, against requirements laid down in the agreement. It should define tests to be carried out, test equipments and expected test results.

- **"Authorized Representative"** shall mean any person/agency authorized by either of the parties.

- **"Contract"** is used synonymously with agreement.

- **"Documentary evidence"** means any matter expressed or described upon any substance by means of letters, figures or marks intended to be used for the recording of that matter and produced before a court.

- **"GoI"** shall mean Government of India

- **"Gov./GoO/Government/Govt. of Odisha"** shall mean Government of Odisha.

- **"Law"** shall mean any Act ,notification, bye law ,rules and regulations, directive, ordinance, order or instruction having the force of law enacted or issued by the Government of India or State Government or regulatory authority or political sub-division of government agency.

- **"LOI"** means issuing of Letter of Intent which shall constitute the intention of the Tenderer to place the purchase order with the successful bidder**.**

- **"OCAC"** stands for the Odisha Computer Application Centre, a Society registered under the Societies Registration Act 1962, having its registered office at OCAC Building, Plot No. N-1/7-D, Acharya Vihar Square, RRL Post, Bhubaneswar, PIN. 751 013 (Technical Directorate of I.T. Department, Govt. of Odisha. The term includes its successors and assigns thereof. OCAC acts as the State Designated Agency for the project.

- **"OEM"** means Original Equipment Manufacturer company, that is incorporated in India or abroad, who has management control over the manufacturing/production process, Quality Assurance, Procurement of Raw materials/manufacturing process inputs marketing and warranty services of the resultant products, of at least one manufacturing facility /factory where the manufacturing of equipment, related accessories, as required for the e- District, Odisha etc. is carried out.

- **"Party"** shall mean Govt. or Bidder individually and "Parties" shall mean Govt. and Bidder collectively.

- **"Rates/Prices"** means prices of supply of equipment and services quoted by the Bidder in the Commercial Bid submitted by him and/or mentioned in the Contract

- **"RFP"** means the detailed notification seeking a set of solution(s) ,service(s), materials and/or any combination of them

- **"Services"** means the work to be performed by the Bidder pursuant to this Contract, as detailed in the Scope of Work

- **"Site"** shall mean the location(s) for which the Contract has been issued and where the service shall be provided as per Agreement

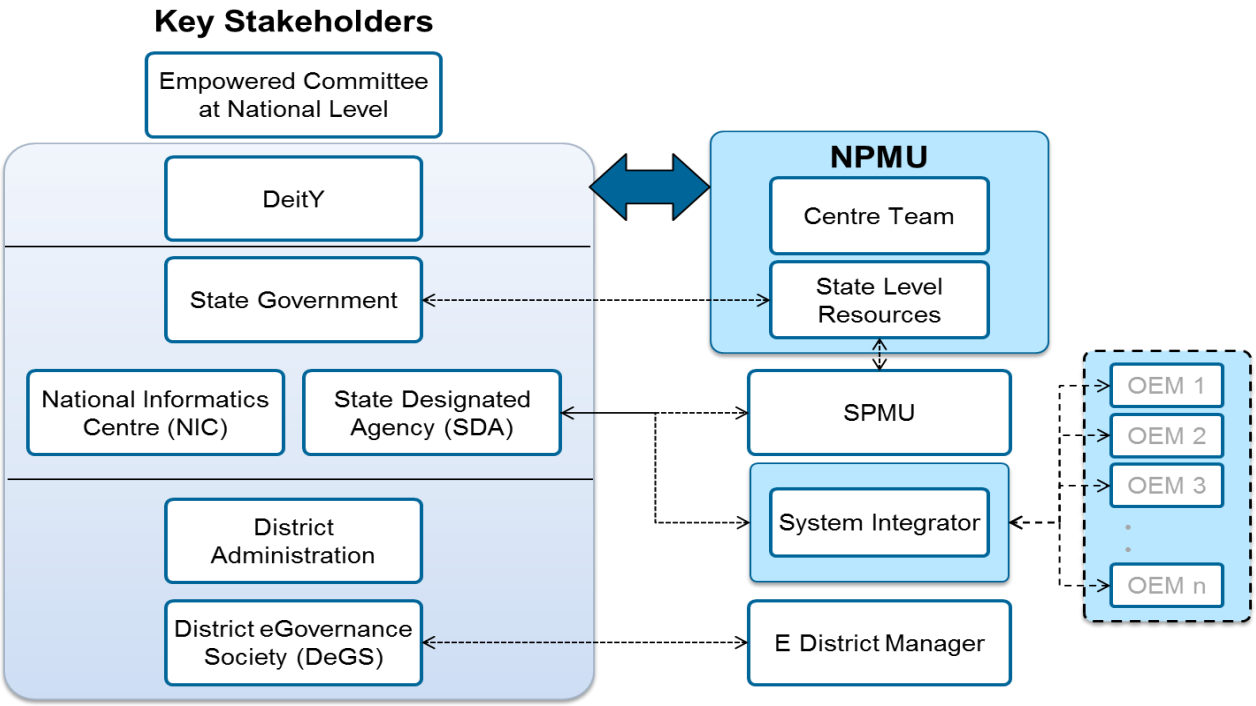
- **"Tenderer"** shall mean the authority issuing this Request For Proposal (RFP) and the authority under whom the e-District, Odisha is to be implemented, operated, managed etc. and this authority shall be the Odisha Computer Application Centre, acting on behalf of Govt. of Odisha as the implementing agency for the 'e-District, Odisha project.

- **"Termination notice"** means the written notice of termination of the Agreement issued by one party to the other in terms hereof.

1 Implementation Framework

I. e-District project shall be implemented in a way where the districts will play a major role. e-District shall be implemented in alignment with the NeGP principle of "centralized planning and decentralized implementation". State IT Department/ Nodal Agency shall play a key role in planning and implementation of the program in collaboration with the district.

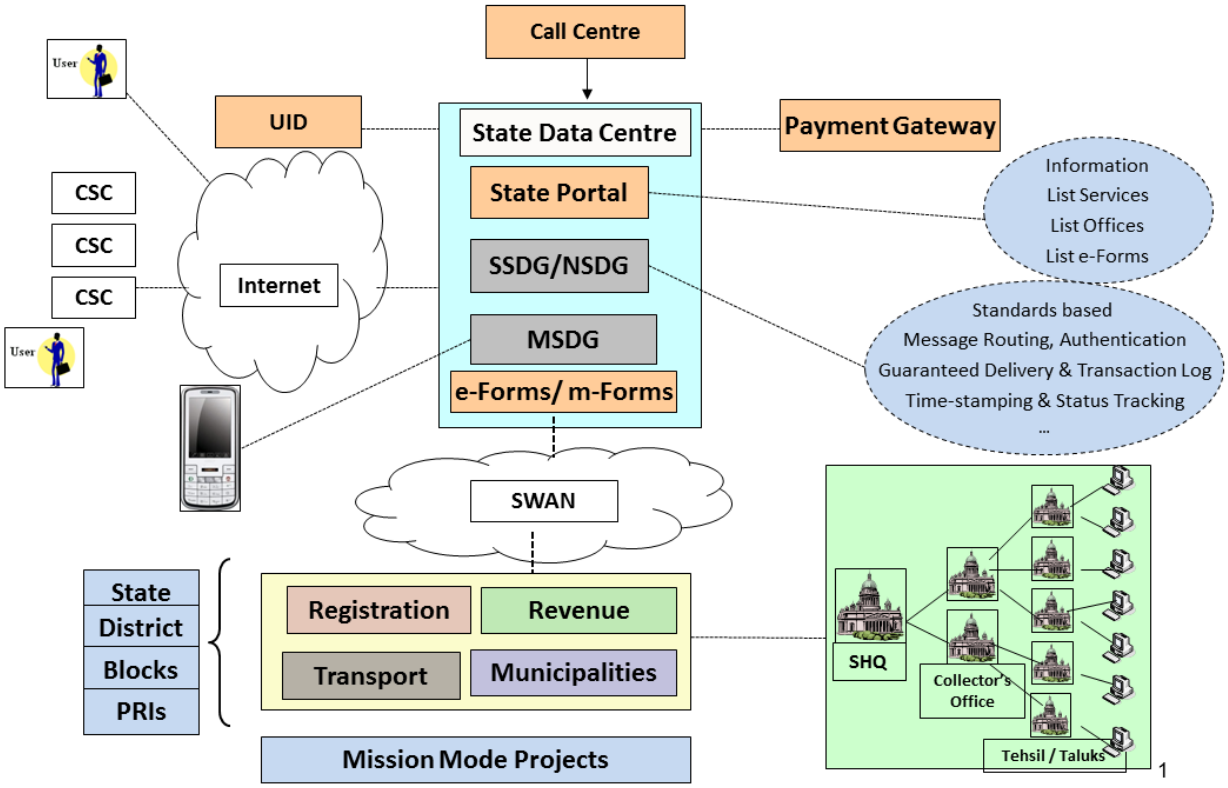
II. The role of the DeitY, GoI focuses primarily in planning of national level roll out, issuing guidelines, funding support to the states, monitor and support the state in implementation of the project. States shall drive the implementation at the state/district level. The diagram illustrating the key stakeholders and their role in implementation and for managing the eDistrict MMP is shown below:



III. An Integrated Service Delivery Framework has been designed by DeitY in July 2012, and communicated to all the States. It can be accessed at (URL: http://deity.gov.in/content/e-district-guidelines). This framework envisages a centralized architecture for each major e-Governance application at the State level. The application software will be hosted in the State Data Centre. Integration across States shall be enabled, through mandatory adherence to technical specifications and e-Governance standards, besides use of the SSDG. Compliance to latest Unicode standard (current version is 6.0) for local language content/data encoding is also mandatory. The Integrated Framework shall be treated as part of this RFP and shall be followed with appropriate modifications.

IV. Two key aspects of the Scheme are Business Process Re-engineering (BPR) and creation of databases based on e-Governance standards for the purposes of ensuring interoperability. BPR is intended to enable process simplification and significant value addition to citizens.

V. The solution architecture of the e-District project envisages a centralised application and database and will leverage the core e-infrastructure of State Wide Area Network, State Data Centre and State Service Delivery Gateway.



VI. Further e-District service will be integrated with a mobile service delivery gateway and Aadhaar numbers of the Unique Identification Authority of India. Localisation of the application will be carried out as per the requirement of the state in terms of local language and other needs. According to this, System Integrator (SI) who shall be responsible to implement the project in the state as per the DeitY, GoI guidelines. Integration of existing applications being used in the state shall not be possible unless the legacy data in the local language is compliant to Unicode version 6.0 or above. In some cases, this legacy data therefore will need to be converted to Unicode 6.0 (or latest version).

VII. The e-District MMP envisages centralised architecture at the state level with common application software for each of the identified services for all the districts of the state. The application software will be hosted in the SDC.

VIII. Integration across states shall be enabled, through mandatory adherence to technical specifications and eGovernance and localization standards. The detailed guidelines in this regard have been issued by Department of Electronics and Information Technology (DeitY) Government of India.

2 Scope of the Project

2.1 Introduction

I. The e-District MMP is to be implemented in 28 districts of the Odisha. The implementation of the project will be completed in ONE year commencing from the date of award to the SI and will be followed by 3 years of Operation and Maintenance (O&M) phase

II. The implementation in the state of Odisha is proposed to be carried out in twenty eight districts simultaneously. The following will be the activities to be carried out by the selected Bidder:

a. Project Planning and Management
b. System Study and Preparation of SRS Document
c. Business Process Reengineering for the selected applications/ services
d. Development of eDistrict Application
e. Network Connectivity
f. Hardware Procurement & Commissioning
g. STQC Certification and C-DAC/TDIL Certification (for localization)
h. UAT & Go live
i. Capacity Building
j. Operation & Maintenance (O&M) support

III. List of districts and CSC roll out status is enclosed at section 4.7-

2.2 Solution & Technology Architecture

2.2.1 *Overview*

I. A centralized architecture (servers and processing at single and central location) has been proposed for the e-District project. All requests from internal and external users will be sent to this system, located in a central place for processing. All users will access the application through local or remote terminals using a browser.

II. The overall technology solution shall be based upon most relevant and suitable architecture standards including standards for Service Oriented Architecture (SOA), XML services & necessary protocols for internet applications, Data Centre standards, Localization (Unicode, Inscript, etc.) standards, W3C (WCAG for accessibility, etc.) standards & GIGW guidelines, etc

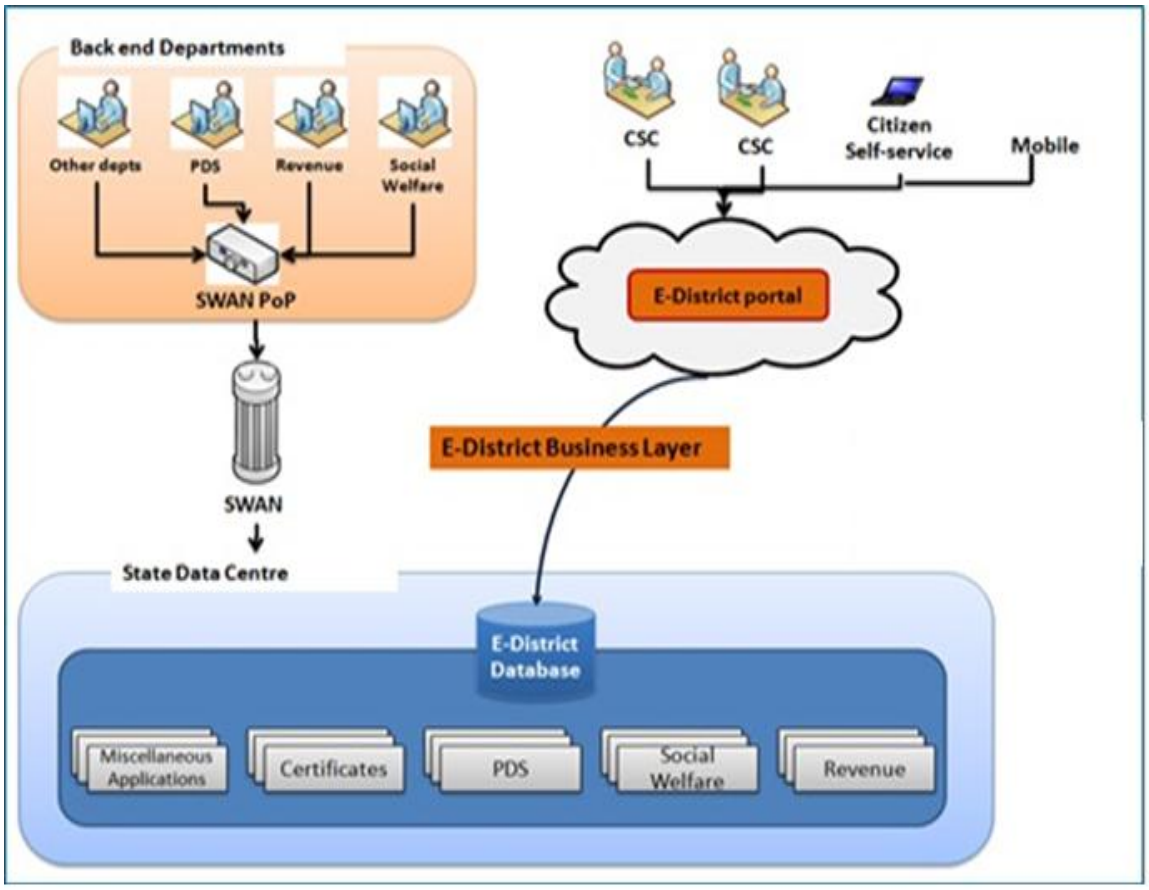
III. The design should include integration with existing IT infrastructure created under SDC, SWAN, CSC, State Portal, SSDG and any other MMP for the implementation of eDistrict Project. eDistrict Application developed should be integrated with existing State Portals and Gateways.

IV. As in the State of Odisha, State Portal / SSDG is under development, the eDistrict architecture should be compatible with it and should get integrated when the SSDG is operational.

It is estimated that the total number of internal users would be 16500 (approx.) having average length of stay per visit 120 mins per user.

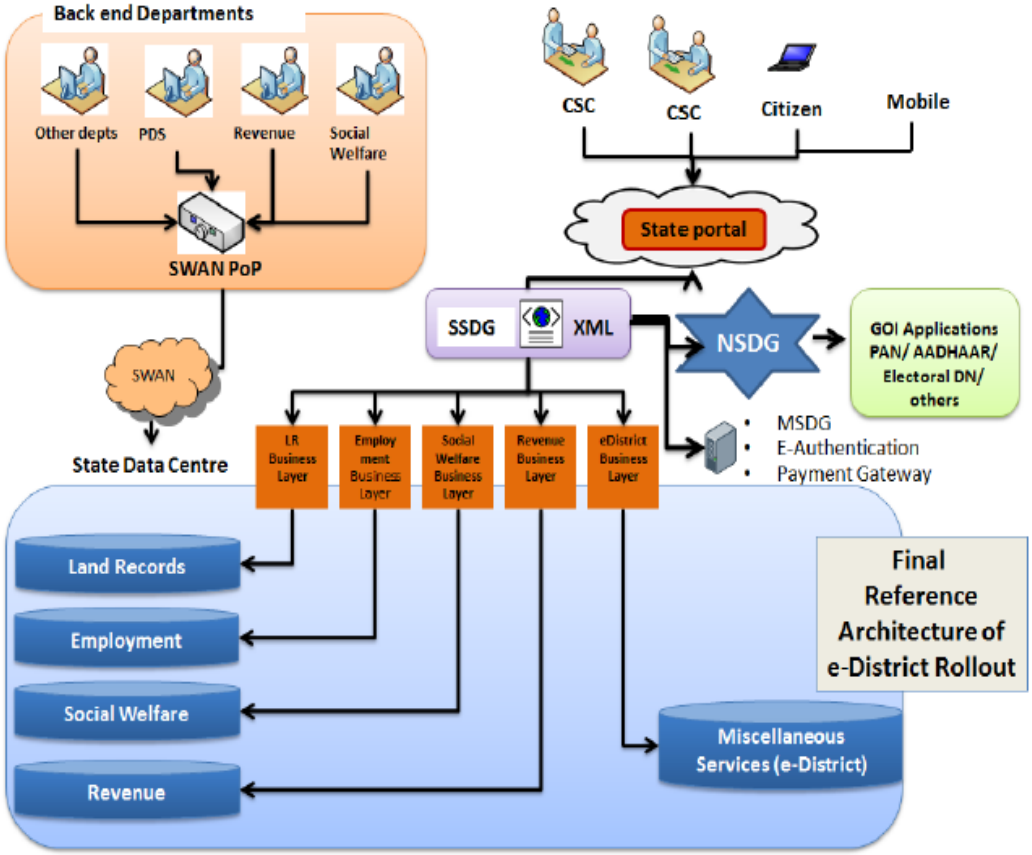
2.2.2 *eDistrict Application Structure*

At present the eDistrict application will host the data of all services in its own database. Once independent applications are rolled out for any service which is part of eDistrict application then the data of that service should be migrated to that new application's database. However data migration is not in the scope of SI.



However, eventually, the eDistrict application should also integrate with SSDG and provide access to citizens for eDistrict services through State Portal. All the existing state applications which have their own independent database and workflow and are identical to e-District should be made available on State Portal through the SSDG. The envisaged architecture is depicted in following diagram.

Note: SI needs to develop the connectors and integrate with SSDG. During integration any modifications to the existing systems (SSDG or State Portal) will be taken up by the existing vendors.



2.3 Scope of Services – Project Implementation Phase

The Government of Odisha had chosen two districts for the pilot implementation of the e-District project. The Pilot implementation has been successfully completed in the following pilot districts.

a. Ganjam
b. Mayurbhanj

The existing eDistrict Application developed for the pilot shall be used for State Wide Rollout for faster replication. All documentation related to the pilot project would be provided to the successful bidder. The pilot application has been tested for all the services included during the pilot project implementation by STQC. The bidder needs to upgrade/enhance the existing application while accommodating the new services. Additional customization efforts are required for the services which are already been tested during the pilot phase. It will be the responsibility of the bidder to get the STQC certification for the entire application prior to Go-Live for the application. Bidders are requested to refer to Annexure-A for comparison of the list

of services. For Technology stack of Pilot Application please refer Vol-I: Section 4.3. Total number of current transaction volume can be referred from Annexure-B.

2.3.1 *Solution Design*

2.3.1.1 System Study and Design

I. The SI shall carry out a detailed systems study to prepare/refine the Functional Requirements Specifications and formulate the System and Software Requirements Specifications documents incorporating the functional specifications and standards provided by the DeitY, GoI and the State nodal Agency requirements.

II. The SI should prepare a detailed document on the implementation of e-District Application with respect to configuration, customization, extension and integration. The SI shall also prepare a change/reference document based on changes or deviations from the base version of the e-District Application with appropriate references to all the artifacts /documents provided by DeitY, GoI / State Nodal Agency.

III. As part of the System Study, the SI shall be responsible for Preparation of a comprehensive System Study document by studying the legislation, business processes and organization design of the state Odisha

IV. The selected Bidder shall perform the detailed assessment of the functional requirements (Including localization framework) and MIS requirements and prepare a new FRS report, as part of the System Study document incorporating list of additional features that shall result in further improvement in the overall application performance for consideration of the OCAC.

V. Further as the existing application will be customized/configured to meet the needs of the state, the SI will provide a comparative report as part of System Study document, on the extent of functionality currently available in the pilot application and the final FRS.

A. **Requirements Traceability Matrix**: The SI shall ensure that developed e-District application is fully compliant with the requirements and specifications provided in the RFP such as functional, non-functional and technical requirements. For ensuring this, the SI shall prepare a Requirements Traceability Matrix on the basis of Functional Requirements Specifications (FRS), Non Functional Requirements Specification, and Technical Requirements provided by State (updated, expanded and fine-tuned by the SI). Refer to section 4.6 for more details on the non-functional requirements.

B. **Project Documentation:** The SI shall create and maintain all project documents that shall be passed on to OCAC as deliverables as per the agreed project timelines. The documents created by the SI will be reviewed and approved by the State Nodal Agency on advice of SPMU. Project documents include but are not limited to the following:

i. Detailed Project Plan
   a. Detailed System Study Report
   b. List of services, Service Definitions, Service Levels
   c. Updated/vetted FRS
   d. SRS document
   e. HLD documents

ii. E-District Application architecture documents.

iii. ER diagrams and other data modelling documents.

iv. Logical and physical database design.

v. Data dictionary and data definitions.

vi. Application component design including component deployment views, control flows, etc.
   a. LLD documents

vii. Application flows and logic.

viii. GUI design (screen design, navigation, etc.).
   a. All Test Plans

ix. Requirements Traceability Matrix

x. Change Management and Capacity Building Plans.

xi. SLA and Performance Monitoring Plan.

xii. Design of real time tools for monitoring e-Transaction volumes and for generating real time MIS

xiii. Training and Knowledge Transfer Plans.

xiv. Issue Logs.

The SI shall share a list of deliverables that they shall submit based on the methodology they propose. The SI shall prepare the formats/templates for each of the deliverables upfront based upon industry standards and the same will be approved by OCAC prior to its use for deliverables.

All project documents are to be kept up-to-date during the course of the project. The SI shall maintain a log of the internal review of all the deliverables submitted. Soft copy of logs shall be submitted to State Nodal Officer on regular basis.

2.3.1.2 Preparation of Software Requirements Specifications (SRS)

As part of the preparation of SRS the selected SI shall be responsible for preparing and submitting detailed requirement specification documents as per IEEE or equivalent standards which meets all the Business, Functional and Technical (including localization) requirements of the departments concerned. Concerned Departments feedback should be taken into account before finalizing the SRS. The SI shall prepare the SRS documents and have it reviewed and approved by the State Designated Agency or its nominated agency. State Designated Agency

will sign off on the SRS documents on the advice of SPMU. The SI is required to update the FRS / SRS as and when any enhancements / modifications are made to the e-District application till the duration of the Contract.

2.3.1.3 Preparation of e-District Project Plan

The SI shall prepare a comprehensive e-District implementation and deployment plan in consultation with OCAC. This document shall also comprise of

I. Trainings to be provided to the departmental officials at different stages of the project, procurement
II. Deployment and commissioning of required hardware and software
III. Provisioning of network connectivity etc

Further, SI will also prepare detailed work plan and estimate the timelines and resources required for configuration, customization, extension, integration, and commissioning of the e-District software as per the DeitY GoI / State requirements. All the plans and frameworks prepared by SI during the duration of the contract shall be required to seek approval from OCAC.

2.3.1.4 Preparation of e-District Application Design Documents

Detailed Design documents shall include:

I. Technical Architecture Document (Application, Network, and Security)
II. The available IT infrastructure available at state shall be a part of the document.
III. Gap infrastructure
IV. High Level and Low Level Design.
V. Database architecture, including defining data structure, data dictionary as per requirements of data storage in English and the local language with compliance to standards defined by DeitY, GoI/ Government of Odisha.

2.3.1.5 Sign off Deliverables

I. Detailed Project Plan
II. Detailed System Study Report
III. List of Services, Service Definitions, Service Levels
IV. Updated/vetted FRS
V. SRS document
VI. HLD documents
VII. E-District Application architecture documents.
VIII. ER diagrams and other data modelling documents.
IX. Logical and physical database design.
X. Data dictionary and data definitions.

XI. Application component design including component deployment views, control flows, etc.

A. LLD documents (including but not limited to)

i. Application flows and logic.

ii. GUI design (screen design, navigation, etc.).

B. All Test Plans

i. Requirements Traceability Matrix

ii. Change Management and Capacity Building Plans.

iii. Design of realtime tools for monitoring e-Transaction volumes and for generating realtime MIS

iv. SLA and Performance Monitoring Plan.

v. Training and Knowledge Transfer Plans.

vi. Issue Logs.

2.3.2 *Software Development/Customization*

2.3.2.1 E-District Application

The existing eDistrict Application developed for the pilot shall be used for State Wide Rollout for faster replication. Bidders are not allowed to develop any new application or use any other existing application software for State Wide Rollout of eDistrict Project. The pilot application has been tested for all the services included during the pilot implementation by STQC. However, additional software development and customization efforts are required to meet the requirements of the project. Source code and all other documents will be provided to SI. UAT has been done for the services which are gone live in the districts. The bidder needs to upgrade/enhance the existing application while accommodating the new services. It will be the responsibility of the bidder to get the STQC certification for the entire application prior to Go-Live for the application. The bidder would be provided with required documents related to the existing application.

2.3.2.2 List of Services (e-District Functional Modules)

e-District MMP aims at electronic delivery of all public services at district / sub district level, progressively. Initially 10 categories (5 mandatory + 5 state specific) of identified high volume citizen centric public services at district and sub-district level will be taken up for implementation. While doing so, the four pillars of e-infrastructure i.e. SWANs, SDCs, SSDGs and CSCs will be leveraged and no new infrastructure would be created. Later on, new services could be added depending on the requirements and the felt needs. Bidder needs to provide service wise quote as per the format given under VOl-I RFP. The "Cost per inclusion of additional Service" will be taken into consideration for implementation of any additional services in eDistrict Project at a later stage. Following table depicts the list of services that are proposed to be implemented during State Wide Rollout of eDistrict. Please refer to Annexure-A for comparison of the list of services.

The SI needs to use the existing e-District Application, FRS and SRS that may be updated as per the State's requirement for state wide roll out of eDistrict.

LIST OF SERVICES FOR STATEWIDE ROLLOUT of eDistrict MMP		
Sl. #	**Service Categories**	**Sub – Services**
1	Certificates	1. Issuance of Birth Certificate (Above 1 Year Case)
		2. Issuance of Death Certificate (Above 1 Year Case)
		3. Issuance of Disability Certificate
2	Social Security	4. Sanction of Assistance under NFBS
		5. Sanction of Indira Gandhi National Old Age Pension Scheme
		6. Sanction of Indira Gandhi National Disability Pension Scheme
		7. Sanction of Indira Gandhi National Widow Pension Scheme
		8. Sanction of Funds under MBPY
3	Revenue Court & Cases	9. Registration of Societies
		10. Certified Copies of RoR
		11. Conversion of Land Under OLR-8 (A)
		12. Certified copies of other Documents
4	Public Distribution System(PDS)	13. Mutation of Ration Cards (Addition/Deletion of Names)
		14. Issue of Fresh/Duplicate ration card
		15. Change of FPS/Dealer
5	RTI/Grievances	16. Online Grievance Registration to Collector
6	Health	17. Application for Registered Medical Practitioner Certificate
7	ST & SC Development	18. Application for Study Loan for ST/SC students
		19. Scholarship for ST/SC students
8	School & Mass Education Department	20. Issue of Conduct certificate
		21. Application for scholarship for students under S&ME Dept.
9	Higher Education Department	22. Application for Scholarship services for students under Higher Education Dept
10	Employment	23. Application for registration to Employment Exchange.

P.S: List of services mentioned here are indicative. There might be addition/deletion of services at a later stage subject to the decision taken by the Government.

The application for e-District is the most critical component for e-District project. Following things need to be taken into consideration while developing the application.

I. The design and development of the eDistrict Application as per the FRS and SRS finalized by all stakeholders (SDA, State DIT, SPMU, etc).

II. eDistrict Application should ensure availability of all services, in accordance with the BPR. BPR reports will be made available to the selected bidder. BPR activity is not in the scope of SI. System Integrator should focus on the following things while developing/customizing the application for State Wide Rollout of eDistrict.

   a) As State portal is not operational, front end should be designed with migration strategy to State portal after operationalization of State portal.
   b) Back end for the printing, status update and centralized MIS application.
   c) Providing automatic acknowledgement with automated date and time stamping.
   d) Enabling tracking of the status of the application from any authorized office through a unique application ID

III. Development of Role based, workflow driven Web based Content Management System (CMS) for contribution of any type of Content to the eDistrict Application including the metadata as specified in SRS.

IV. The user should be given a choice to interact with the system in local language in addition to English. The application should provision for uniform user experience across the multi lingual functionality covering following aspects:
   a) Front end web portal in local language
   b) E-forms (Labels & Data entry in local languages). Data entry should be provided preferably using the Enhanced Inscript standard (based on Unicode version 6.0 or later) keyboard layout with option for floating keyboard.
   c) Storage of entered data in local language using UNICODE (version 6.0 or later) encoding standard.
   d) Retrieval & display in local language across all user interfaces, forms and reports with all browsers compliant with Unicode version 6.0 and above.
   e) Facility for bilingual printing (English and the local language)
   f) Sakal Bharti font (compliant to UNICODE version 6.0) to be used for local language data and content. Latest version of the font is available on www.ildc.in

V. Application should have a generic workflow engine. This generic workflow engine will allow easy creation of workflow for new services with minimum technical programming support and thus enable the State government to create new services as and when required by the various Departments without creating a change request. At the minimum, the workflow engine should have the following features:
   a) Feature to use the master data for the auto-populating the forms and dropdowns specifically with reference to :

i. Name of District, Tehsils, Blocks & Villages

ii. Designation of officials involved in the processing of the application

b) Creation of application form, by "drag & drop" feature (restricted for admin user only) using meta data standards

c) Defining the workflow for the approval of the form, by providing various options like :

i. First in First out

ii. Defining a citizen charter/delivery of service in a time bound manner

d) Creation of the "output" of the service, i.e. Certificate, Order etc.

e) Automatic reports

i. of compliance to citizen charter on delivery of services

ii. delay reports

f) The application should have a module for management of digital signature including issuance, renewal and suspension of digital signatures based on the administrative decisions taken by the State. In case of any change (transfer, promotion, leave, suspension, termination, superannuation etc.) of the officials under e-District Project, a copy of order should be marked to the State Level digital signature management team for assigning and revoking of the access rights.

VI. **Integration of Digital Signatures with e-District Application:** The eDistrict portal should be made accessible to government official users / registered users over internet and to CSC users through secure user id and password. The biometric/digital signatures need to be integrated for enabling authenticity of the approving authority. Procurement of biometric device is the scope of SI. Required number of digital signatures shall be procured by the Department. The Digital Signatures required will be of Class 2. State department will manage the case of individuals having digital signatures getting transferred & retiring.

VII. **Training on use of Digital Signatures:** As the eDistrict project would entail significant amount of field verification and relevant updating of records, digital signatures have to be used by various levels of officials. These officials may also keep on changing due to transfers/ superannuation, etc. Hence, SI would be required to impart training on the use of Digital Signature to the concerned officials.

VIII. **Transaction Report & accounting module:** The e-District services are being provided through the CSCs in the State. The payments to the CSCs are being made to the CSC Operatos on the number of transactions made by the CSCs. The CSCs are aligned to various organizations (SCAs). For e-District project to succeed it is important to ensure that there is a streamlined method to calculate the fee payable to the CSC operator. Therefore, a separate module for calculation of such fee and payments should be developed.

IX. **e-Transaction & SLA Monitoring Tools :**The SLA Performance of Server Hardware, Application, Database and Network devices will be monitored by the existing EMS tool of the Odisha State Data Center. SDC will directly procure additional EMS licenses for application, network, hardware etc from OEM based on the e district infrastructure quoted by the winning SI. SI needs to implement, integrate, commission the EMS SW with Odisha SDC operator to provide support and monitoring activities for the entire e-district system.

Details of EMS tool available in SDC provided in below table:-

Sl. No.	EMS Component	Software Version
1	Infrastructure Monitoring	CA spectrum Infrastructure manager 9.2
2	Application Monitoring	CA Application performance management 9.3
3	Performance Monitoring	CA Ehealth 6.2
4	Network and System Management	CA NSM 11.2
5	Database Monitoring	CA Insight DPM 11.5
6	Helpdesk	CA Service desk manager 12.6

X. It is also further envisaged that the e-District application to be deployed in all States and UTs should have roadmap to integrate with key initiatives of DeitY namely Portal Services, Citizen Contact Centre, Mobile Platform/ Gateway Services / National Service Delivery Gateway (NSDG) / State Service Delivery Gateway (SSDG), National Service Directory, Payment Gateway, Language Switch, Open Data, E-authentication including Aadhaar, Geographical Information System/ Global Positioning System, E-Gov Application Store, Document Repository, Certifying Authority etc. The details for integration with other initiatives are given below. Hence the architecture of eDistrict Application should be open standard and designed in such a way that there will not be any problem during the integration. Contact details for integration with other initiatives are given below.

Name of the initiative	Purpose for integration	Contact Agency	Agency Person details	Deity Nodal Person Details
SSDG	Integration with existing application	CDAC	Mr. Zia Saquib, Executive Director, CDAC, Mumbai. Telephone:+91-22-26201606	Ms. Kavita Bhatia, Additional Director, DeitY. Telephone: +91-11-24364729
Payment Gateway	e-payment	NDML	Mr. Sameer Gupte, Vice-President, NDML. Telephone: +91-9820039921	Ms. Kavita Bhatia, Additional Director, DeitY. Telephone: +91-11-24364729

Name of the initiative	Purpose for integration	Contact Agency	Agency Person details	Deity Nodal Person Details
MSDG	Services over mobile phone	CDAC	Mr. Zia Saquib, Executive Director, CDAC, Mumbai. Telephone:+91-22-26201606	Ms. Kavita Bhatia, Additional Director, DeitY. Telephone: +91-11-24364729
e-Authentication	Validation of beneficiary-using biometric	CDAC	Mr. Zia Saquib, Executive Director, CDAC, Mumbai. Telephone:+91-22-26201606	Ms. Kavita Bhatia, Additional Director, DeitY. Telephone: +91-11-24364729
AADHAR	Applicant authentication	UIDAI	Mr. Tejpal Singh, ADG, UIDAI, New Delhi. Telephone: +91-11-23462611	Mr. Gaurav Dwivedi, Director, DeitY. Telephone:+91-11-24301218
Localisation	Localisation of the application as per the requirement of the State in terms of local language and other needs.	CDAC	Mr. Mahesh Kulkarni, Associate Director, CDAC, Pune. Telephone: +91-20-25883261/25503402	Ms. Swaran Lata, Director, DeitY. Telephone: +91-11-24301272

XI. Complete mobile enablement of the e-District applications and services including all appropriate channels such as SMS / USSD / IVRS and development of corresponding mobile applications to the eDistrict applications and services leveraging the Mobile Service Delivery Gateway (MSDG) and the Mobile App Store developed by DeitY

XII. Operation and Maintenance of eDistrict Application including the suggested changes as indicated by the states for 3 years from the date of Go-Live

XIII. Implement / add any additional forms of State Departments as and when the departments are ready for delivering.

XIV. The Intellectual Property Rights of all the software code, data, algorithms, documentation, manuals, etc. generated as a part of implementation of this project shall solely vest with OCAC.

XV. Detailed User and Operational Manual to be provided to each department, whose services will be hosted on eDistrict Application.

XVI. The application should have a web interface and should publish online transaction volume data for each service for each district & CSC.

XVII. The selected bidder will be responsible for master data entry required to make the services operational. Data migration or digitization of legacy data work would be carried out by separate bidder.

2.3.2.3 Single-Sign On

The application should enable single-sign-on so that any user once authenticated and authorized by system is not required to be re-authorized for completing any of the services in the same session. For employees of the department concerned, the browser based application accessed on the intranet, through single-sign-on mechanism, will provide access to all the services of the departments concerned (based on their roles and responsibilities), Help module,

basic and advanced reporting etc. Similarly, for external users (citizens, etc), based on their profile and registration, the system should enable single-sign on facility to apply for various services, make payments, submit queries /complaints and check status of their applications.

2.3.2.4 Support for PKI based Authentication and Authorization

The solution should support PKI based Authentication and Authorization, in accordance with IT Act 2000, using the Digital Certificates issued by the Certifying Authorities (CA) such as MTNL or NIC. In particular, 3 factor authentication (login id & password, biometric and digital signature) shall be implemented by the selected Bidder for officials/employees involved in processing citizen services.

2.3.2.5 Interoperability Standards

Keeping in view the evolving needs of interoperability, especially the possibility that the solution shall become the focal point of delivery of services, and may also involve cross-functionality with the e-Government projects of other departments / businesses in future, the solution should be built on Open Standards. The SI shall ensure that the application developed should easily integrate with the existing applications of other eGovernance initiatives of the state. Every care shall be taken to ensure that the code does not build a dependency on any proprietary software, particularly, through the use of proprietary 'stored procedures' belonging to a specific database product.

2.3.3.6 Scalability

One of the fundamental requirements of the proposed application is its scalability. The architecture should be proven to be scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering high performance for at-least four years from the date of deployment. In this context, it is required that the application and deployment architecture should provide for Scale-Up and Scale out on the Application and Web Servers, Database Servers and all other solution components.

2.3.2.7 Security

The systems implemented for project should be highly secure, considering that it is intended to handle sensitive data relating to the citizens of the state. The overarching security considerations are described below.

I. The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols.
II. The solution shall support advanced user authentication mechanisms including digital certificates and biometric authentication.
III. Security design should provide for a well-designed identity management system, security of physical and digital assets, data and network security, backup and recovery and disaster recovery system.

IV. The solution should provide for maintaining an audit trail of all the transactions and should also ensure the non-repudiation of audit trail without impacting the overall performance of the system.

V. The overarching requirement is the need to comply with ISO 27001 standards of security.

VI. The application design and development should comply with OWASP top 10 principles

2.3.2.8 Application Architecture

I. It has been proposed that the applications designed and developed for the departments concerned must follow some best practice and industry standards. In order to achieve the high level of stability and robustness of the application, the system development life cycle must be carried out using the industry standard best practices and adopting the security constraints for access and control rights. The various modules / application should have a common Exception Manager to handle any kind of exception arising due to internal/ external factors.

II. Similarly the modules of the application are to be supported by the Session and Transaction Manager for the completeness of the request and response of the client request. The system should have a module exclusively to record the activities/ create the log of activities happening within the system / application to avoid any kind of irregularities within the system by any User / Application.

2.3.2.9 Proposed Application Architecture

A 3-tier architecture (also referred to as multi-tier or N-tier architecture) has been proposed for the Application Solution. The entire processing should take place in n-tier architecture:

I. Front-end software (client tier): - Existing application is running as a separate portal. Services which are available under e-District and SSDG, the e-District application should integrate with the *e-form developed under SSDG* for that service and use the standard connectors provided for this purpose by the SSDG project to connect with the e-District application for end to end integration.

For services under e-District project which are not taken up under SSDG project, *the e-form to be developed under e-District project* and should use the standard connectors provided for this purpose by the SSDG project to connect with the e-District application for end to end integration.

As SSDG is not operational the Bidder will take necessary action at his end to integrate the application with NSDG.

II. **Application and Web Layer** – Application server would be used as middle tier for various web based applications. It would take care of the necessary workflow and Web server would be required for the interfacing with the end user. Both the web and application server would be seamlessly integrated to provide high availability and perfor-

mance. These servers would be installed and operated in clustered configuration to ensure high availability and reliability.

III. **Database Layer** - The application will be hosted on database which will contain all the data of the application. Since this data will be centralized and is very critical, the server would be installed and operated in only clustered configuration to ensure high availability and reliability. The data would be physically stored on an External Fiber Channel (FC) based Storage (SAN).

2.3.2.10 High Level Design (HLD)

SI shall complete the High Level Designing and all HLD documents of all the functionalities, integration with existing application and external application. The SI shall prepare the HLD and have it reviewed and approved by the OCAC. State Nodal Office will sign off on the HLD documents based on the advice of SPMU.

2.3.2.11 Detailed (Low Level) Design (LLD)

The LLD shall interpret the approved HLD to help application development and shall include detailed service descriptions and specifications, application logic (including "pseudo code") and UI design (screen design and navigation). The preparation of test cases will also be completed during this stage. The SI shall have the design documents reviewed and approved by the state Nodal Agency. State Nodal Agency will sign off on the LLD documents based on the advice of SPMU.

2.3.2.12 Test Plan

The SI shall prepare all necessary Test Plans (including test cases), i.e., plans for Acceptance Testing. Test cases for Initial and Final User Acceptance Testing shall be developed in collaboration with domain experts identified at the state nodal agency. Initial and Final User Acceptance Testing shall involve Test Case development, Unit Testing, Integration and System Testing, Functional testing of Application, Performance testing of the Application including measurement of all Service Levels as mentioned in this RFP and finally SI shall also carryout Load/ Stress testing. The SI will submit the test plans and test result reports to the state nodal agency for comprehensive verification and approval.

2.3.2.13 Requirement on Adherence to Standards

eDistrict application must be designed following open standards, and in line with overall system requirements set out in this RFP, in order to provide for good inter-operability with multiple platforms and avoid any technology or technology provider lock-in.

2.3.2.14 Compliance with Industry Standards

In addition to above, the proposed solution has to be based on and compliant with industry standards (their latest versions as on date) wherever applicable. This will apply to all the aspects of solution including but not limited to design, development, security, installation, and testing. There are many standards that are summarized below. However the list below is just for reference and is not to be treated as exhaustive.

I. Portal development W3C specifications
II. Information access/transfer protocols SOAP, HTTP/HTTPS
III. e-District DeitY, GoI guidelines.
IV. Photograph JPEG (minimum resolution of 640 x 480 pixels)
V. Scanned documents TIFF (Resolution of 600 X 600 dpi)
VI. Biometric framework BioAPI 2.0 (ISO/IEC 19784-1:2005)
VII. Latest HTML standards

2.3.2.15 Specification

I. Finger print scanning IAFIS specifications
II. Digital signature RSA standards
III. Document encryption PKCS specifications
IV. Information Security to be ISO 27001 compliant
V. Operational integrity & security management to be ISO 17799 compliant
VI. IT Infrastructure management ITIL / EITM specifications
VII. Service Management ISO 20000 specifications
VIII. Project Documentation IEEE/ISO specifications for documentation
IX. The SI shall adhere to all the standards published by the Department of Electronics and Information Technology, Government of India.

2.3.2.16 Sign-off Deliverables

I. System Requirement Specification (SRS)
II. Functional Requirement Specification (FRS) (if, updated)
III. High Level and Low Level Design
IV. Functional and non-functional testing
V. Fully functional eDistrict Application
VI. User and Operational Manual for e-District Application

2.3.3 *Obtain STQC Certification for eDistrict Application*

The SI will be responsible for engaging STQC to conduct the assessment / review for the system before “Go Live”. The SPMU shall have the right to audit and inspect all the procedures and systems relating to the provisioning of the services. If there is any change /addition in the application’s functionality then the SI will have to obtain the STQC Certification for the changes / additions. SI shall ensure the following points are duly addressed for successful completion of STQC Certification.Successful completion of Application Audit. Application audit will include;

A. Functionality audit that will map the functionality delivered to the FRS agreed upon during development phase.

B. Identify the nature and type of transactions being processed by the application systems.

C. Determine systematic measures implemented to control and secure access to the application programs and data including password controls, user authentications, roles and responsibilities, audit trails and reporting, configuration and interface controls, etc.

D. Review of database structure including:

1. Classification of data in terms of sensitivity & levels of access
2. Security measures over database installation, password policies and user roles and privileges
3. Access control on database objects – tables, views, triggers, synonyms, etc.
4. Database restoration and recoverability
5. Audit trails configuration and monitoring process
6. Network connections to database

E. Review of Network and Website will include:

1. Penetration and vulnerability testing
2. Security exposures to internal and external stakeholders

F. Definition and Implementation of Security Policies and Controls will include:

1. Define and implement backup process, including schedule, storage, archival and decommissioning of media
2. Define physical access controls review (over DC and other critical area)
3. Define IT Change Management process, Incident Management process – covering identification, response, escalation mechanisms
4. Define and implement Anti-virus (malware) controls – patching, virus definition file update

SI is also required to comply with any other Technical/Functional requirements required to receive Final Certification of STQC.

2.3.3.1 Sign-off Deliverables

I. Sign off from SDA
II. STQC Certification

2.3.4 *Alignment with Integrated Framework*

The e-District application should integrate with SSDG and provide access to citizens for e-District services through State Portal. It is envisaged that over a period of time all the existing state applications which have their own independent database and workflow and are identical to e-District should be made available on State Portal through the SSDG. The application may be States' own applications or adopted applications. The key functionalities required are as follows.

- The SAP and SP Connectors will need to connect the e-district Business Layer. This would help in routing requests and responses to back-end departments within a stipulated time period.
- Design and implement an accounting module to keep track of all the transactions service category wise, department wise and break down of transactions VLE, DeGS wise.
- MIS of number of transactions including name of service and category of service on time and geographical scale should be published on e-District portal.
- Use e-authentication (including Aadhaar for citizens), e-payment, Digital signature and Mobile gateway.
- As and when required, migrate the data available in eDistrict database to newly created respective department database. Migration of data from eDistrict to department database will be the responsibility of the vendor who has developed the department application. Only DB design is to be provided by SI.

2.3.5 *SSDG*

I. The Integrated Service Delivery Framework envisages centralized architecture for each MMP at the State level. The application software will be hosted in the State Data Centre. Integration across States shall be enabled, through mandatory adherence to technical specifications and e Governance standards.

II. The solution architecture of the e-District project envisages a centralised application and database and will leverage the core e-infrastructure of State Wide Area Network, State Data Centre and State Service Delivery Gateway.

III. The e-District MMP envisages centralised architecture at the state level with common application software for each of the identified services for all the districts of the state. The application software will be hosted in the SDC.

IV. Integration across states shall be enabled, through mandatory adherence to technical specifications and e Governance standards.

2.3.6 *Payment and SMS Gateway*

I. Provisioning of a payment gateway, SMS gateway and any other components required to meet the functional and Quality-of-Service requirements of the RFP is also within the scope of work of the SI.

II. Payment Gateway should allow net banking and debit card payments through atleast 20 banks in the country (including all leading banks), besides payments through credit cards (VISA, Mastercard).

III. Any one-time charges such as those for tie-ups, development of interfaces, registration, commissioning etc of the gateway and any fixed recurring charges such as monthly rentals, etc will have to be borne by the SI for the Contract period and may be budgeted for in the Total Contract Value of this Project

IV. Any applicable transaction charges for making electronic payments or using SMS based services shall however be payable by the citizen and SDA respectively and need not be accounted for in the Total Contract value of this Project. Any transaction charges should be payable in Indian Rupees only.

V. The contracts that the SI does with the Payment Gateway provider and SMS gateway provider should be structured in a manner to allow the transaction charges to be paid directly by the citizen / SDA. However if the contract with payment gateway / SMS gateway provider require any transactional charges to be paid by the SI, the same will be reimbursed to the SI by the SDA every month on an actual basis. The systems deployed by the SI should be able to provide logs of the transactions done and charges paid. The SDA will however reserve the right to negotiate and examine the rate contracts of the SI with the gateway providers.

VI. Payment gateway should enable receipt of all payments such as Tax, interest, penalty, arrear and fee etc and crediting the same to the SDA/ Department account. The payment gateway should also allow credit of any refund amount to Kiosk/CSC's account. It should be possible to make electronic payments through a 3G / GPRS enabled mobile phone as well.

2.3.7 *UAT and Go-Live Report*

SI will assist in successful completion of User Acceptance Testing (UAT) and audit of the system on the completion of the roll out of eDistrict pilot for each phase and will submit a Go-Live Report for each phase.

2.3.7.1 Sign-off Deliverables

I. Go-Live report for state and district level
II. UAT Report signed off from actual/end users

2.3.8 *Network Connectivity*

For Odisha, the selected Bidder will undertake the following:

I. With implementation of State Wide Area Network (OSWAN, service provider is BSNL) across all the States with 2 Mbps vertical dedicated leased line connectivity up to block level is present. All the DC offices and Block offices are co-located to the respective

SWAN PoP. The selected Bidder shall ensure last mile connectivity from the nearest SWAN PoP to the concerned users of DC Office & Block Office via UTP cable only.

II. For all the Tahsil offices to access the application 2 MBPS Broadband connectivity (internet broadband over DSL) needs to be procured and commissioned by the bidder. SI has to procure the connectivity in the name of concern office and pay the bills. The service provider will install the same. For Tahsil office, the broadband internet connectivity will be independent of SWAN.

III. For all the RI offices to access the application 512 KBPS Broadband connectivity needs to be procured and commissioned by the bidder.

IV. Additionally the selected bidder will need to establish LAN connectivity to all offices as listed in section 4.1 including IP addressing scheme, physical cabling, router/switch configuration, V-LAN configuration, and fail over mechanism. The selected Bidder should coordinate with the local department offices while designing and installing the LAN.

V. All networking equipment required to provide the LAN / WAN connectivity to meet the requirements of the Project is also to be provided by the selected Bidder as part of this RFP

VI. Connectivity of SDC is not scope of SI

VII. Scope of SWAN connectivity at DC, District and Block office is not under scope of SI

VIII. Address, location, contact person and number for each office where connectivity is to be provided will be shared with the selected SI.

2.3.8.1 Sign-off Deliverables

Network Connectivity report signed off by concerned District Nodal officers stating Departmental offices have been connected and SWAN, wherever applicable, has been leveraged to provide connectivity.

2.3.9 *Supply / Procurement of IT Infrastructure at SDC*

State Government of Odisha will provide the Data Center premises for hosting the IT Infrastructure. Load Balancer, SAN Storage, San Switch and Firewall available at the SDC shall be leveraged by the Bidder. Bidders are required to carefully assess the requirements of this RFP and size the infrastructure accordingly. Bidders are free to propose any higher / additional infrastructure that may be required as per their proposed solution to meet the project requirements, its scope of work and SLAs as listed in this RFP.

I. Bids / proposals which do not meet the minimum IT infrastructure specifications given in this RFP will be summarily rejected. The minimum technical specifications for the IT Infrastructure are provided in **Section 4.5: Bill of Material (Infrastructure at SDC) in**

Volume 2 of the RFP. The Bidder will be responsible for sizing the hardware to support the scalability and performance requirements of the e-District application. The Bidder shall ensure that the servers are sized adequately and redundancy is built into the architecture required to meet the service levels mentioned in the RFP.

II. None of the IT Infrastructure proposed is declared "End-of-Sale" by the respective OEM in next 2 years as on date of submission of Bid.

III. The IT Infrastructure proposed should be purchased within last 2 months from the date of deployment and documentary proof for warranty and proof of purchase should be produced at the time of deployment of infrastructure.

IV. The IT Infrastructure proposed should be compatible with infrastructure at SDC, SSDG, SWAN, State Portal, etc.

V. The Bidder should provide requisite licenses for all the system software required for servers including, but not limited to industry standard operating system, enterprise class database software, application server software, web server software, OS hardening, and all other required software with sufficient number of licenses.

VI. The Bidder will be responsible for providing all the details of the Bill of Material (BoM) and specifications of the IT Infrastructure proposed, licenses of the system software, all other equipment proposed as part of its Technical Proposal. The financial quote submitted by the Bidder should include costs for these.

2.3.10 *Hardware Commissioning at Field Offices*

2.3.10.1 Design, Supply, Installation, Commissioning, O & M of IT Infrastructure

This shall consist of

I. Procurement/Supply of IT Infrastructure at Department Offices.

II. Installation and Commissioning of IT Infrastructure

Note: Site Preparation (electrical work and cabling, earthing, furniture) is not in the scope of SI. Also recurring Consumables like paper and tonner are out of scope of bidder.

2.3.10.2 Installation and Commissioning of IT Infrastructure

The selected Bidder is responsible for installation and configuration of the entire infrastructure set-up, including but not limited to the following:

I. All IT Infrastructure including operating systems and any other system software required for making the infrastructure operational and tuned for satisfactory performance.

II. The IT Infrastructure will be installed and configured in accordance with the IT Policies of the state Odisha.

The selected Bidder will ensure that the reports for monitoring of SLAs such as system uptime, performance, etc. are generated automatically from the system.

2.3.11 Licenses

I. The system software licenses mentioned in the Bill of Materials shall be genuine, perpetual, full use and should provide upgrades, patches, fixes, security patches and updates directly from the OEM. All the licenses and support (updates, patches, bug fixes, etc.) should be in the name of OCAC.

II. All the licenses and support (updates, patches, bug fixes, etc.) should be in the name of OCAC. SI shall provide a comprehensive warranty that covers all components after the issuance of the final acceptance by OCAC. The warranty should cover all materials, licenses, services, and support for both hardware and software. SI shall administer warranties with serial number and warranty period. SI shall transfer all the warranties to the OCAC at no additional charge at the time of termination of the project. All warranty documentation (no expiry) will be delivered to Department.

2.3.12 Capacity Building / Training

Bidder must impart training to the personnel identified by the State Government on the following aspects.

I. Impart training on functional use of eDistrict Application
II. Usage of Digital Signature
III. Use of Biometric Devices
IV. Medium of Instruction :- Both English & Odia
V. Language of training material :- English

The Training has to be conducted at DHQ & SDHQ as per the requirement and as agreed upon with the district administration. Every attempt will be made by the District Administration to provide the Training Classroom (as per availability) at BHQ, DHQ & SDHQ. Infrastructure required for conducting the training should be arranged by the System Integrator on its own. The SI would be required to prepare a detailed training plan covering at least 2 rounds of training to the target audience, dates for training, duration and training content. The time gap between the first round and second round training would depend on the actual scenario. The timeline for completion of training and change management activities as specified under project schedule is to be accounted for completion of 1st round training. Following format need to be taken into consideration while calculating the cost of training and preparing the training plan. If required the training would be required to be provided again to ensure that personnel are ready to use the application whenever it is rolled out. SI needs to provide refreshments of Worth Rs. 100 for each round of training to the Government Official. Out of 11200 government officials, the ratio of officers and staff would be in the ratio of 30:70 (Approx.).

TRAINING OF GOVERNMENT OFFICIALS				
Name of the Module	**Duration**		**No of times**	**Partici-pant/Batch**
	Officers	**Staff**		
Impart training on Functional use of eDistrict Application	4 days (5 hrs/day)	6 days (5 hrs/day)	2 rounds	20
Usage of Digital Signature	1 day (1 hr)	1 day (2 hrs)	2 rounds	20
Use of Biometric Devices	1 days (1 hr)	1 day (2 hrs)	2 rounds	20

TRAINING OF CSC OPERATORS		
Name of the Module	**Duration**	**Participant/Batch**
Impart training on Functional use of eDistrict Application	1 day (8 hrs) to be given in 2 sessions	(To be decided later)

It is mandatory for the all employees identified for a particular batch/module to attend training. If because of some constraints he/she is not able to attend the same, the implementation agency should accommodate such employee in subsequent batches. SI needs to provide user manuals (must be printed in A4 size paper and spiral binding) to each participants. Bidder also needs to prepare Power Point Presentations and Videos to promote self- learning and assist training participants in undergoing the training. The content of the CD is intended to provide the Audio-Visual representation of the usage of application by the officials (users) for all the services, Digital Signature and Biometric Device etc. The content of the Power Point Presentation should also be prepared in the same line. The Video and Power Point Presentation need to be handed over to each participant in a CD. It is expected that in each District around 400 officials need to be trained by SI. Actual number of users to be trained in each district will be intimated to the SI at a later stage. SI also needs to impart training to 650 CSC operators across the state. The location of CSC operator training would be at the BHQ, DHQ & SDHQ. Number of CSC operators to be trained in each district will be intimated to the SI at a later stage. Trained CSC operators in each district in turn shall impart training to rest of the CSC operators in the district. In case of any change in number of participants the unit rate quoted by the bidder for imparting training will be taken into consideration and the bidder should agree to provide the training at the same cost.

2.3.12.1 Sign off Deliverables

I. Training Plan
II. Completion of training and change management activities

2.3.13 Manpower requirements

The SI would be required to position resources to provide technical support at each of the districts (minimum1 resource per district) during the roll out period. This would be essential to ensure sufficient handholding is provided to personnel in the district level offices to manage the system after the end of SI's Contract Period. SI is required to provide the details of the manpower for 28 districts as per the format given below.

S.No.	Name of Resource	District for which proposed			Qualification (Highest)	No. of Years of Experience	No. of Years with responding firm	Certification
		Choice 1	Choice 2	Choice 3				
1								
2								
3								

I. The Technical support resources would be required to work closely with the eDistrict Manager, DeGS Coordinator and SPMU in ensuring adherence to the project timelines. The technical support staff would be deployed at each district. For better understanding Please refer to Annexure-C for the number of jurisdiction under which the offices will be covered. However, actual number of office will be based on the working location of the user.

II. The SI should ensure that the roster schedule of all deployed manpower for each day at the required locations has been communicated in advance to SDA/ DeGS. No change to the deployed staff shall be done by the SI without written approval from the SDA/DeGS

III. Adherence to all laws pertaining to personnel, labour laws, etc for any manpower deployed by the SI on this Project shall be the responsibility of the SI

IV. The SI would issue Identity cards to each of the staff members deployed at the districts.

V. The SI will maintain adequate leave reserve for the staff, so that the work in the respective districts remains unaffected in all cases.

VI. The State, together with the SPMU would need to devise criteria for selection of technical support resources who will be best positioned to handle the complexities associated with rolling out the application in the specific state, for instance, being conversant with the local language

VII. The resource will reporting to the Collector/Nodal Officer e-District or any other authority as will be defined by the District Authority/ SDA

Brief job description of the technical support staff is given below.

a) Coordination in supply, installation and Inspection of Hardware at the District, Tahsils, Sub-divisions, Blocks, Revenue Inspector Office and any other location pertaining to the project.
b) Preventive Maintenance of District IT Infrastructure supplied under e-District
c) Complaints handling - Hardware & Software Issues
d) Complaints handling through telephone or through travel to respective location & resolve issues.
e) Maintenance of HW & SW records and calling.
f) Monitoring LAN Connectivity
g) Providing handholding support to the users of eDistrict Application

2.3.14 Business Continuity Planning

The selected Bidder is expected to develop a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) for the operations carried out by the selected Bidder. An indicative list of activities to be performed by the selected Bidder is mentioned below:

I. Designing and implementing adequate data backup, business continuity and restoration procedures for the e-District application data (including but not limited to the database, attachments and all other data elements created in and generated by the system and users)
II. Ensuring that there is no single point of failure and adequate level of redundancy is built in to meet the uptime and other requirements of this RFP. While building redundancies, it should be ensured that failure of a single component of communication link does not result in failure of primary as well as secondary connectivity. Hence primary and secondary connectivity should be taken from 2 separate communication link providers and both links should not have any single point of failure. Preferably, all the redundancy will be in auto fail over mode so that if primary component fails, secondary component automatically takes over. Please note that last mile connectivity of SWAN is not in the scope of SI.
III. Ensuring data backup till the last transaction occurring in the system to ensure enhanced service levels and following RPO and RTO objectives:
    A. **Peak hours: Zero RPO and Zero RTO**
    B. **Non-Peak Hours: Zero RPO and RTO <= 60 minutes**
IV. Any storage space / media required to maintain backups and other requirements of the RFP should be provisioned for by the selected Bidder in his Bid.
V. Designing and implementing data synchronization procedures for the DR Site. Periodic testing may be done to ensure that all replication and data synchronization procedures are in place all the time. Replication between Data Centre and DR Site as well as change-over during disaster should be automatic and real-time for minimal impact on user experience.

Notes: - *As of now the DR site for SDC is not operational. The relevant clause will be applicable once the DR site is ready. Connectivity between DC and DR is not the scope of SI.*

Further, according to section 2.3.8, the bidder has to quote for broadband connectivity for Tahsil and RI offices. However, it is not required to provide redundant link from different service providers for each location

2.3.15 *Others*

2.3.15.1 Information Security Management

Security of Application and the data contained therein is paramount for the success of this Project. Hence, the selected Bidder should take adequate security measures to ensure confidentiality, integrity and availability of the information.

Security Requirements	
Overall Solution	
1.	The proposed solution should include design and implementation of a comprehensive IS security policy in line with ISO 27001 standards to comply with the security requirements mentioned in this section. All the necessary procedures / infrastructure / technology required to ensure compliance with IS security policy should be established by the selected Bidder. The IS Policy shall include all aspects such as physical and environmental security, human resources security, backup and recovery, access control, incident management, business continuity management etc.
2.	The designed IS policy should not conflict with the security policy of the State Data Centre where the infrastructure would be hosted. Interested Bidder need to discuss with the SDC Composite Team to ensure the same.
3.	The proposed solution should ensure proper logical access security of all the information Assets
4.	The proposed solution should be able to classify information assets according to criticality of the information asset.
5.	The proposed solution should provide security including identification, authentication, authorization, access control, administration and audit and support for industry standard protocols
6.	The proposed solution should have a security architecture which adheres to the security standards and guidelines such as • ISO 27001 • Information security standards framework and guidelines standards under e-Governance standards (http://egovstandards.gov.in)

Security Requirements	
	• Information security guidelines as published by Data Security Council of India (DSCI) • Guidelines for Web Server Security, Security IIS 6.00 Web-Server, Auditing and Logging as recommended by CERT-In (www.cert-in.org.in) • System shall comply with IT (Amendment) Act 2008.
7.	The proposed solution should support the below Integration security standards: • Authentication • Authorization • Encryption • Secure Conversation • Non-repudiation • XML Firewalls • Security standards support • WS-Security 1.0 • WS-Trust 1.2 • WS-Secure Conversations 1.2 • WS-Basic Security Profile
8.	The proposed solution should a multi-layered detailed security system covering the overall solution needs having the following features: i. Layers of firewall ii. Network IPS iii. Enterprise-wide Antivirus solution iv. Information and incident management solution for complete OCAC landscape v. Two factor authentication for all administrators i.e. system administrators, network administrators, database administrators. vi. Audit Log Analysis Selected Bidder must ensure that the security solution provided must integrate with the overall system architecture proposed
9.	The proposed solution should be monitored by periodic information security audits / assessments performed by or on behalf of the OCAC. The scope of these audits / assessments may include, but are not limited to, a review of: access and authorization procedures, physical security controls, backup and

Security Requirements	
	recovery procedures, and program change controls. To the extent that the OCAC deems it necessary to carry out a program of inspection and audit / assessment to safeguard against threats and hazards to the confidentiality, integrity, and availability of data, the Selected Bidder shall provide the OCAC's representatives access to its facilities, installations, technical resources, operations, documentation, records, databases and personnel. The Selected Bidder must provide OCAC access to various monitoring and performance measurement systems (both manual and automated). OCAC has the right to get the monitoring and performance measurement systems (both manual and automated) audited / assessed without prior approval / notice to the Selected Bidder
10.	The proposed solution should facilitate system audit for all the information assets to establish detective controls. The selected Bidder is required to facilitate this by producing and maintaining system audit logs for entire duration of the project.
11.	The proposed solution should ensure that data, especially those to pertaining to registration process, transaction process as well as the data that is stored at various points is appropriately secured as per minimum standard 128 Bit AES/3DES encryption.
12.	The proposed solution should provide database security mechanism at core level of the database, so that the options and additions to the database confirm the security policy of the OCAC without changing the application code.
13.	The proposed solution should support native optional database level encryption on the table columns, table spaces or backups.
14.	The database of the proposed solution should provide option for secured data storage for historic data changes for compliance and tracking the changes.
15.	The proposed solution should be able to ensure the integrity of the system from accidental or malicious damage to data
16.	The proposed solution should be able to check the authenticity of the data entering the system
17.	The proposed solution should be able to generate a report on all "Authorization Failure" messages per user ID
18.	The proposed solution should be able to monitor the IP address of the system from where a request is received.

Security Requirements	
19.	The proposed solution should be able to differentiate between the systems of the OCAC network and other external systems
20.	Retention periods, archival policies and read-only restrictions must be strictly enforceable on all logs maintained in the system
21.	The proposed solution should provide ability to monitor, proactively identify and shutdown the following types of incidents through different modes of communication (email, SMS, phone call, dashboard etc): a) Pharming b) Trojan c) Domains (old/new)
22.	The proposed solution should be able to monitor security and intrusions into the system and take necessary preventive and corrective actions.
23.	The proposed solution should have the option to be configured to generate audit-trails in and detailed auditing reports
24.	The proposed solution must provide ACL objects and a security model that can be configured for enforcement of user rights
25.	The proposed solution should be designed to provide for a well-designed security of physical and digital assets, data and network security, backup and recovery and disaster recovery system.
26.	The proposed solution should have tamper proof data storage to prevent unauthorised data tampering
27.	The proposed solution should have a Business Continuity Plan and a Disaster Recovery Plan prepared and implemented by the selected Bidder before commencement of the operations. Robust backup procedures to be established for the same.
Password Requirement	
1.	The proposed solution should allow OCAC to define password policies. The minimum password policies to be defined are: a) Minimum/ Maximum password length b) Alpha numeric combination of password c) Compulsory use of special characters d) Minimum password age e) Password expiry period f) Repeat passwords etc.
2.	The proposed solution should be able to automatically check the passwords with the password policy, which can be customized by the OCAC

Security Requirements	
3.	The proposed solution should enforce changing of the default password set by the system (at the time of creation of user ID) when the user first logs on to the system. The proposed solution should enforce all password policies as defined at the time of first change and thereafter.
4.	The proposed solution should store User ID's and passwords in an encrypted format. Passwords must be encrypted using MD5 hash algorithm or equivalent (selected Bidder must provide details)
5.	The proposed solution should be capable of encrypting the password / other sensitive data during data transmission
6.	The proposed solution should ensure that the user web access shall be through SSL (https) only for all level of communication for providing higher level of security.

2.3.16 *Project Management*

2.3.16.1 Project Planning and Management

e-District Mission Mode Project is a geographically spread initiative involving multiple stakeholders. Successful implementation and national roll out of the project ultimately depends on all its stakeholders, the role of SI is very critical. Hence SI is required to design and implement a comprehensive and effective project planning and management methodology together with efficient and reliable tools.

Project planning exercise shall essentially commence with the start of the project, however, project management exercise shall commence at the start of the project and shall continue till the O&M Phase of the project...

To have an effective project management system in place, it is necessary for the SI to use a Project Management Information System (PMIS) at State Headquarters of his respective State to monitor the Project Progress. The SI shall address at the minimum the following using PMIS:

I. Create an organized set of activities for the project.
II. Coordinate and collaborate with various stakeholders including the Departments concerned.
III. Nodal Agency, State IT Department, NIC, SPMU, NPMU, DeitY, GoI.
IV. Establish and measure resource assignments and responsibilities.
V. Construct a project plan schedule including milestones.
VI. Measure project deadlines, budget figures, and performance objectives.
VII. Communicate the project plan to stakeholders with meaningful reports.
VIII. Provide facility for detecting problems and inconsistencies in the plan

During the project implementation the SI shall report to the State Nodal Officer/SPMU, on following items:

I. Results accomplished during the period;
II. Cumulative deviations to date from schedule of progress on milestones as specified in this RFP read with the agreed and finalized Project Plan;
III. Corrective actions to be taken to return to planned schedule of progress;
IV. Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of the SI;
V. Other issues and outstanding problems, and actions proposed to be taken;
VI. Interventions which the SI expects to be made by the State Nodal Officer and / or actions to be taken by the State Nodal Officer before the next reporting period. Progress reports would be prepared by SI on a fortnightly basis. These reports may be required to be shared with either the SDA or the SPMU, as the case may be.
VII. Project quality Assurance
VIII. Change Control mechanism
IX. Project Management activities
X. Issue Management to help identify and track the issues that need attention and resolution from the State.
XI. Scope Management to manage the scope and changes through a formal management and approval process.
XII. Risk Management to identify and manage the risks that can hinder the project progress.

SI will closely work with SPMU and send the reports to the SPMU as well. SPMU will assist Nodal Officer in acceptance of the report/ document and suggest the action plan to the Nodal Officer. The Project plan prepared by the SI at the initial stage of the project shall be reviewed by the SDA/Apex Committee on the advice of the State eGovernance Mission Team and SPMU.

The SI shall update and maintain the Project Plan throughout the duration of the engagement. All changes are to be reviewed and approved by the OCAC.

2.3.16.2 Project Planning and Management

I. PMIS data update & functioning
II. Periodic Reports on on-going basis

2.4 Scope of Services - Operation and Maintenance Phase

The selected Bidder is responsible for the day to day maintenance of the system for the entire period of Contract. For the IT Infrastructure procured as part of this RFP, the selected Bidder will be responsible for smooth Operations and Maintenance Services for the period covering onsite support for 3 year of warranty and followed by 2 years of AMC from the date of Go-Live covering the following:

I. Onsite Warranty support
II. Onsite Periodic and AMC support including repair and replacement
III. Annual Technical Support (ATS) for all the licensed software
IV. Providing Help desk support with Escalation matrix for registration of complaints related to the IT Infrastructure procured through this RFP at the State Data Center.

2.4.1 Overview of Post Implementation Services

An indicative list of activities and nature of support to be provided is mentioned below:

I. System Administration and Trouble Shooting

A. Overall monitoring and management of all IT and Non-IT infrastructure deployed by the selected Bidder for the Project, Departmental locations, networking equipments & connectivity, system software, application, database, and all other services associated with these facilities to ensure service levels, performance and availability requirements as prescribed in the RFP are met.
B. Repair or replace infrastructure deployed for this Project, either directly or through a third party warranty provider depending on the case
C. Replace component due to technical, functional, manufacturing or any other problem with a component of the same make and configuration. In case the component of same make and configuration is not available, the replacement shall conform to open standards and shall be of a higher configuration and shall be approved by the Department
D. Perform system administration tasks such as managing the user access, creating and managing users, taking backups etc.
E. Performance tuning of the system to ensure adherence to SLAs and performance requirements as indicated in the RFP.

II. Network Administration and Trouble Shooting

Coordinate with the network service providers to maintain smooth network operations and ensure uptime and performance requirements of the IT infrastructure as indicated in the RFP are met. The selected Bidder will be totally responsible for all networking equipments installed by him.

III. Database Administration and Trouble Shooting

Undertake end-to-end management of database on an on-going basis to facilitate smooth functioning and optimum utilization including regular database backup and

periodical testing of backup data, conducting configuration review to tune database, maintaining the necessary documentation and managing schemes to database schema, disk space, user roles, and storage.

IV. Overall

A. Undertake preventive maintenance (any maintenance activity that is required before the occurrence of an incident with an attempt to prevent any incidents) and carry out the necessary repairs and replacement of parts wherever needed to keep the performance levels of the hardware and equipment in tune with the requirements of the SLA. Such preventive maintenance shall not be attended during working hours of the State Departments, unless inevitable and approved by the OCAC.

B. Undertake reactive maintenance (any corrective action, maintenance activity that is required post the occurrence of an incident) that is intended to troubleshoot the system with sufficient teams

C. Escalate and co-ordinate with its OEMs for problem resolution wherever required

D. The selected Bidder will be required to comply with various policies relating to monitoring and management of infrastructure such as IS Policy, backup and archival policy, system software update policy etc. of the State Odisha.

2.4.2 Warranty Support

As part of the warranty services SI shall provide:

I. SI shall provide a comprehensive 3 year of warranty and followed by 2 years of AMC from the date of Go-Live.

II. SI shall provide the comprehensive manufacturer's warranty and support in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the RFP.

III. SI must warrant all hardware, equipment, accessories, spare parts, software etc. procured and implemented as per this RFP against any manufacturing defects during the warranty period.

IV. SI shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the RFP.

V. SI is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the RFP. During the warranty period SI shall replace or augment or procure higher-level new equipment or additional licenses at no additional cost to the OCAC in case the procured hardware or software is not adequate to meet the service levels.

VI. Mean Time Between Failures (MTBF): If during contract period, any equipment has a hardware failure on four or more occasions in a period of less than three months, it shall be replaced by equivalent or higher-level new equipment by the SI at no cost to OCAC

VII. However, if the new equipment supplied is priced lower than the price at which the original support services for all system software, DBMS (Database Management System) other products deployed as part of this project will require proper arrangements of SI with OEM.

VIII. During the warranty period SI shall maintain the systems and repair / replace at the installed site, at no charge to OCAC, all defective components that are brought to the SI's notice.

IX. Warranty should not become void, if OCAC buys, any other supplemental hardware from a third party and installs it within these machines under intimation to the SI. However, the warranty will not apply to such supplemental hardware items installed.

X. The SI shall carry out Preventive Maintenance (PM), including cleaning of interior and exterior, of all hardware and testing for virus, if any, and should maintain proper records at each site for such PM. Failure to carry out such PM will be a breach of warranty and the warranty period will be extended by the period of delay in PM.

XI. SI shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.

XII. The SI shall ensure that the warranty complies with the agreed Technical Standards, Security Requirements, Operating Procedures, and Recovery Procedures.

XIII. Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA).

XIV. The SI shall develop and maintain an inventory database to include the registered hardware warranties.

2.4.3 Annual Technical Support

As part of the ATS services SI shall provide the following:

I. SI shall maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements and maintenance.

II. If the Operating System or additional copies of Operating System are required to be installed / reinstalled / de-installed, the same should be done as part of ATS.

III. SI should carry out any requisite adjustments / changes in the configuration for implementing different versions of Application Software.

IV. Updates / Upgrades / New releases / New versions / Patches / Bug fixes: The SI shall provide from time to time the Updates / Upgrades / New releases / New versions / Patches / Bug fixes of the software, operating systems, etc. as required. The SI should provide free Updates / Upgrades / New releases / New versions / Patches / Bug fixes of the software and tools to SDA as and when released by OEM.

V. Software License Management. The SI shall provide software license management and control. SI shall maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements, and maintenance.

VI. SI shall have complete manufacturer's technical support for all the licensed software problems and/or questions, technical guidance, defect and non-defect related issues. SI shall provide a single-point-of-contact for software support and provide licensed software support including but not limited to problem tracking, problem source identification, problem impact (severity) determination, bypass and recovery support, problem resolution, and management reporting.

2.4.4 Help Desk and Trouble ticket management system

I. The selected Bidder as part of provisioning support for Department users at each location and SDC; will setup centralized helpdesk and coordinate with the respective OEMs of the IT Infrastructure deployed at SDC and the Department offices. For the State Odisha the selected Bidder will undertake the following:

A. Provide Help Desk services to track and route requests for service and to assist department users in answering questions and resolving problems related to the IT Infrastructure installed at Data Centre and at all the Department Offices . The helpdesk will be operated from OCAC building, Bhubaneswar. SI needs to arrange the helpdesk hardware/networking infrastructure on its own. OCAC shall provide OSWAN connectivity port.

B. Become the central collection point for contact and control of the problem, change, and service management processes (This includes both incident management and service request management).

C. Shall provide a first level of support for application and technical support at e-District implementation locations across the State where the software, hardware, and other infrastructure will be rolled out. Help Desk Facility will continue from "Go-Live of eDistrict application" till the completion of the project. SI needs to deploy 2 resources for providing the helpdesk services.

D. Provide the following integrated customer support by establishing 9 hrs X 6 days Help Desk facility for reporting issues/ problems with the software, hardware and other infrastructure. The helpdesk will operate on official working days.

II. This shall be an online system deployed centrally and shall be used by the selected Bidder extensively for management of network support activity and handling calls from citizen, departmental staff, any other stakeholders. Service desk is an application that facilitates the end-to-end service support. The proposed system should include required hardware and software.

All relevant infrastructure and supporting system software required for the deployment and operation of the help desk is to be provided by the selected Bidder as per the requirements mentioned in the RFP. The system deployed by the SI shall be complied with ITIL and ISO 20000 service specifications.

2.4.5 General Requirements

I. Licensing Requirements

A. All system software, licenses, etc. have to be procured in the name of OCAC

B. The licenses should be perpetual and enterprise wide for the core application and other software unless otherwise stated. The software licenses shall not be restricted based on location and the OCAC should have the flexibility to use the software licenses for other requirements, if required

II. Asset Management

The selected Bidder will perform the following asset management functions with respect to the infrastructure deployed at various locations:

A. Take periodic stock of, review physical inventory and maintain stock registers of hardware at all locations covered under this Project. The selected Bidder would maintain stock registers as per format agreed with the OCAC.

B. Maintain documentation of the hardware assets, maintain asset Information for all Project locations, on parameters to be mutually agreed between the OCAC and the selected Bidder, which shall include details like -

i. Product type, model number, version number
ii. Manufacturer
iii. Office location
iv. Maintenance status, etc.

C. Update or correct the asset information following any new installations, movement, addition, or change performed by the selected Bidder.

D. Produce periodic reports and machine readable files in agreed upon format pertaining to some or all of the asset information.

E. Restrict movement of server/equipment/items in or out of SDC or any other location under the Project without prior permission from the OCAC.

III. Warranty and Support

A. The selected Bidder shall warrant that the IT Infrastructure supplied to the OCAC for this Project shall have no defects arising from design or workmanship or any act or omission of the selected Bidder. The warranty shall remain valid for the Contract period on all the items supplied as per the Contract.

B. The selected Bidder shall replace any parts/ components of the IT infrastructure supplied for the Project if the components are defective and during the entire warranty period the selected Bidder shall apply latest upgrades for all the hardware components after appropriate testing. The OCAC will not pay any additional costs separately for warranty and the overall IT infrastructure cost quoted by the selected Bidder shall include the same.

C. Since the Project aims to reuse the common infrastructure created under SDC, SWAN, CSC, SSDG Projects, the selected Bidder will also be required to coordinate with SDC, SWAN, SSDG, CSC teams to ensure that uptime and performance requirements of the RFP are met. However, the selected Bidder shall be held solely responsible for

performance and service levels of any infrastructure deployed by the selected Bidder as part of this Contract.

IV. Knowledge Transfer

A. At the end of the Contract period, the selected Bidder will be required to provide necessary handholding and transition support to designated staff or any other agency that is selected for maintaining the system post the Contract with the selected Bidder. The handholding support will include but not be limited to, conducting detailed walkthrough and demonstrations for the IT Infrastructure, handing over all relevant documentation, addressing the queries/clarifications of the new agency with respect to the working / performance levels of the infrastructure, conducting training sessions etc. The knowledge transfer activity would be carried out centrally.

B. Knowledge Transfer is an integral part of the scope of work of the selected Bidder. This will have to be done even in case the Contract with the Bidder ends or is terminated before the planned timelines.

Any other activity, over and above these, as may be deemed necessary by the selected Bidder to meet the service levels and requirements specified in this Contract are also required to be performed by the selected Bidder at no additional cost.

2.4.6 Exit Management

2.4.6.1 Purpose

I. This sets out the provisions, which will apply on expiry or termination of the MSA, the Project Implementation, Operation and Management SLA.

II. In the case of termination of the Project Implementation and/or Operation and Management, the Parties shall agree at that time whether, and if so during what period, the provisions of this Schedule shall apply.

III. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.

2.4.6.2 Transfer of Assets

I. OCAC shall be entitled to serve notice in writing on the SI at any time during the exit management period as detailed hereinabove requiring the SI and/or its sub-contractors to provide the OCAC with a complete and up to date list of the Assets within 30 days of such notice. OCAC shall then be entitled to serve notice in writing on the SI at any time prior to the date that is 30 days prior to the end of the exit management period requiring the SI to sell the Assets, if any, to be transferred to OCAC or its nominated agencies at book value as determined as of the date of such notice in accordance with the provisions of relevant laws.

II. In case of contract being terminated by OCAC, OCAC reserves the right to ask SI to continue running the project operations for a period of 6 months after termination orders are issued.

III. Upon service of a notice under this Article the following provisions shall apply:

A. in the event, if the Assets to be transferred are mortgaged to any financial institutions by the SI, the SI shall ensure that all such liens and liabilities have been cleared beyond doubt, prior to such transfer. All documents regarding the discharge of such lien and liabilities shall be furnished to the OCAC.
B. All risk in and title to the Assets to be transferred / to be purchased by the OCAC pursuant to this Article shall be transferred to OCAC, on the last day of the exit management period.
C. OCAC shall pay to the SI on the last day of the exit management period such sum representing the Net Block (procurement price less depreciation as per provisions of Companies Act) of the Assets to be transferred as stated in the Terms of Payment Schedule.
D. Payment to the outgoing SI shall be made to the tune of last set of completed services / deliverables, subject to SLA requirements.
E. The outgoing SI will pass on to OCAC and/or to the Replacement SI, the subsisting rights in any leased properties/ licensed products on terms not less favorable to OCAC/ Replacement SI, than that enjoyed by the outgoing SI.

2.4.6.3 Cooperation and Provision of Information

During the exit management period:

I. The SI will allow the OCAC or its nominated agency access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable the OCAC to assess the existing services being delivered;
II. promptly on reasonable request by the OCAC, the SI shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with this agreement relating to any material aspect of the services (whether provided by the SI or sub-contractors appointed by the SI). The OCAC shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. The SI shall permit the OCAC or its nominated agencies to have reasonable access to its employees and facilities as reasonably required to understand the methods of delivery of the services employed by the SI and to assist appropriate knowledge transfer.

2.4.6.4Confidential Information, Security and Data

I. The SI will promptly on the commencement of the exit management period supply to the OCAC or its nominated agency the following:
A. information relating to the current services rendered and customer and performance data relating to the performance of sub-contractors in relation to the services;
B. documentation relating to Computerization Project's Intellectual Property Rights;
C. documentation relating to sub-contractors;
D. all current and updated data as is reasonably required for purposes of OCAC or its nominated agencies transitioning the services to its Replacement SI in a readily available format nominated by the OCAC, its nominated agency;

E. all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable OCAC or its nominated agencies, or its Replacement SI to carry out due diligence in order to transition the provision of the Services to OCAC or its nominated agencies, or its Replacement SI(as the case may be).

II. Before the expiry of the exit management period, the SI shall deliver to the OCAC or its nominated agency all new or up-dated materials from the categories set out in Schedule above and shall not retain any copies thereof, except that the SI shall be permitted to retain one copy of such materials for archival purposes only.

III. Before the expiry of the exit management period, unless otherwise provided under the MSA, the OCAC or its nominated agency shall deliver to the SI all forms of SI confidential information, which is in the possession or control of Chairperson, PIU or its users.

2.4.6.5Employees

I. Promptly on reasonable request at any time during the exit management period, the SI shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide to the OCAC or its nominated agency a list of all employees (with job titles) of the SI dedicated to providing the services at the commencement of the exit management period.

II. Where any national, regional law or regulation relating to the mandatory or automatic transfer of the contracts of employment from the SI to the OCAC or its nominated agency, or a Replacement SI ("Transfer Regulation") applies to any or all of the employees of the SI, then the Parties shall comply with their respective obligations under such Transfer Regulations.

III. To the extent that any Transfer Regulation does not apply to any employee of the SI, department, or its Replacement SI may make an offer of employment or contract for services to such employee of the SI and the SI shall not enforce or impose any contractual provision that would prevent any such employee from being hired by the OCAC or any Replacement SI.

2.4.6.6Transfer of Certain Agreements

On request by OCAC or its nominated agency the SI shall effect such assignments, transfers, licences and sub-licences as the OCAC may require in favor of the Chairperson, PIU, or its Replacement SI in relation to any equipment lease, maintenance or service provision agreement between SI and third party lessors, vendors, and which are related to the services and reasonably necessary for the carrying out of replacement services by the OCAC or its nominated agency or its Replacement SI.

2.4.6.7Rights of Access to Premises

I. At any time during the exit management period, where Assets are located at the SI's premises, the SI will be obliged to give reasonable rights of access to (or, in the case of Assets located on a third party's premises, procure reasonable rights of access to) the

OCAC or its nominated agency and/or any Replacement SI in order to make an inventory of the Assets.

II. The SI shall also give the OCAC or its nominated agency or its nominated agencies, or any Replacement SI right of reasonable access to the Implementation Partner's premises and shall procure the OCAC or its nominated agency or its nominated agencies and any Replacement SI rights of access to relevant third party premises during the exit management period and for such period of time following termination or expiry of the MSA as is reasonably necessary to migrate the services to the OCAC or its nominated agency, or a Replacement SI.

2.4.6.8General Obligations of the SI

I. The *SI* shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to the OCAC or its nominated agency or its Replacement SI and which the SI has in its possession or control at any time during the exit management period.

II. For the purposes of this Schedule, anything in the possession or control of any SI, associated entity, or sub-contractor is deemed to be in the possession or control of the SI.

III. The SI shall commit adequate resources to comply with its obligations under this Exit Management Schedule.

2.4.6.9Exit Management Plan

I. The *SI* shall provide the OCAC or its nominated agency with a recommended exit management plan ("Exit Management Plan") which shall deal with at least the following aspects of exit management in relation to the MSA as a whole and in relation to the Project Implementation, and the Operation and Management SLA.

A. A detailed program of the transfer process that could be used in conjunction with a Replacement SI including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;

B. plans for the communication with such of the SI's sub-contractors, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on the OCAC's operations as a result of undertaking the transfer;

C. (if applicable) proposed arrangements for the segregation of the SI's networks from the networks employed by OCAC and identification of specific security tasks necessary at termination;

D. Plans for provision of contingent support to OCAC, and Replacement SI for a reasonable period after transfer.

II. The SI shall re-draft the Exit Management Plan annually thereafter to ensure that it is kept relevant and up to date.

III. Each Exit Management Plan shall be presented by the SI to and approved by the OCAC or its nominated agencies.

IV. The terms of payment as stated in the Terms of Payment Schedule include the costs of the SI complying with its obligations under this Schedule.

V. In the event of termination or expiry of MSA, and Project Implementation, each Party shall comply with the Exit Management Plan.

VI. During the exit management period, the SI shall use its best efforts to deliver the services.

VII. Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.

VIII. This Exit Management plan shall be furnished in writing to the OCAC or its nominated agencies within 90 days from the Effective Date of Agreement.

3 Detailed Implementation and Roll-out Plan

I. SI shall prepare a detailed roll-out plan for each of the districts in the phase and get the same approved by the OCAC. SI is also responsible for conducting workshops for the key officers (State Mission Team, District Mission Team, and District Core Team, NIC, SPMU, NPMU, OCAC, State DIT) of the Districts / State for presenting the District-Wise roll-out plan and get the approval of the same.

II. Before getting the final approval of the State Nodal Officer, the SI shall also provide the necessary assistance for the key stakeholder of the Districts / State during the design and implementation of e-District project in the State Odisha. A detailed rollout checklist should be maintained for migrating application to production as well as for location readiness.

III. One of the important factors that would determine the success of the e-District implementation in the Odisha is the continuous availability of domain experts like Project Manager, Database Administrator, Technical Experts etc to the implementation team which would be selected with the approval of Odisha. SI shall put together the specified team of domain experts with required experience who will work on this project during the entire duration of the project.

4 Annexures:

4.1 Office Wise Requirements

DISTRICT	NO. OF SUBDIVISION	NO. OF TAHSILS	NO. OF BLOCKS	NO. OF RI OFFICES	e-District Service being delivered from this District	Network Availability? (Yes/ No)	Additional H/W Required? (Yes/ No)
Sundargarh	3	18	17	112	Yes	Yes	Yes
Jharsuguda	1	5	5	32	Yes	Yes	Yes
Deogarh	1	3	3	20	Yes	Yes	Yes
Sambalpur	3	9	9	55	Yes	Yes	Yes
Keonjhar	3	13	13	80	Yes	Yes	Yes
Angul	4	8	8	55	Yes	Yes	Yes
Bhadrak	1	7	7	75	Yes	Yes	Yes
Jajpur	1	10	10	80	Yes	Yes	Yes
Dhenkanal	3	8	8	50	Yes	Yes	Yes
Balasore	2	12	12	85	Yes	Yes	Yes
Nuapada	1	5	5	32	Yes	Yes	Yes
Bolangir	3	14	14	86	Yes	Yes	Yes
Sonepur	2	6	6	38	Yes	Yes	Yes
Boudh	1	3	3	22	Yes	Yes	Yes

Kandhamal	2	12	12	74	Yes	Yes	Yes
Cuttack	3	15	14	128	Yes	Yes	Yes
Khurda	2	10	10	71	Yes	Yes	Yes
Puri	1	11	11	107	Yes	Yes	Yes
Kendrapara	1	9	9	92	Yes	Yes	Yes
Jagatsinghpur	1	8	8	76	Yes	Yes	Yes
Bargarh	2	12	12	84	Yes	Yes	Yes
Kalahandi	2	13	13	80	Yes	Yes	Yes
Nabarangpur	1	10	10	66	Yes	Yes	Yes
Rayagada	2	11	11	81	Yes	Yes	Yes
Gajapati	1	7	7	44	Yes	Yes	Yes
Koraput	2	14	14	233	Yes	Yes	Yes
Malkangiri	1	7	7	44	Yes	Yes	Yes
Nayagarh	1	8	8	50	Yes	Yes	Yes

4.2 Template for Capturing Network Connectivity Requirement

DISTRICT	NO. OF SUBDIVISION	NO. OF TAHSILS	NO. OF BLOCKS	NO. OF RI OFFICES	Swan Available(Yes/NO)	SWAN Available		
						Type of connectivity	Existing service provider	Service level / baseline
Sundargarh	3	18	17	112	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Jharsuguda	1	5	5	32	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Deogarh	1	3	3	20	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Sambalpur	3	9	9	55	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Avialable
Keonjhar	3	13	13	80	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Avialable
Angul	4	8	8	55	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Avialable
Bhadrak	1	7	7	75	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Avialable
Jajpur	1	10	10	80	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Avialable
Dhenkanal	3	8	8	50	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Avialable
Balasore	2	12	12	85	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Nuapada	1	5	5	32	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Bolangir	3	14	14	86	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Subarnapur	2	6	6	38	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Boudh	1	3	3	22	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available

Kandhamal	2	12	12	74	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Cuttack	3	15	14	128	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Khurda	2	10	10	71	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Puri	1	11	11	107	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Avialable
Kendrapara	1	9	9	92	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Jagatsinghpur	1	8	8	76	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Bargarh	2	12	12	84	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Kalahandi	2	13	13	80	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Nabarangpur	1	10	10	66	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Rayagada	2	11	11	81	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Gajapati	1	7	7	44	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Koraput	2	14	14	233	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Malkangiri	1	7	7	44	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available
Nayagarh	1	8	8	50	Yes All Block Offices & Sub-divison offices	Broadband	Ms Spancho	Available

4.3 FRS for the Proposed Application

The computerization under the e-District project envisages meeting of the requirements through the e-District Application consisting of Certificates, Pensions, Revenue Court Cases, PDS services, Grievance Redressal services etc. The following depicts the brief scope and the indicative functional requirement specifications of the applications envisaged for development of solution under e-District. This however does not mean that the functionalities have been captured entirely. The final scope will be documented in detail with the selected bidder. SPMU will prepare the AS-IS, TO-BE & FRS documents and the same will be handed over to the selected Bidder after approval to carry out necessary task at his end.

Functional Specification for Common Functionalities:

The common functionality shall address the automation of typical processes that shall be common for all the services irrespective of the service categories. Broadly, these can be seen as the general service components which remain same for services. These general service components along with the detailed Functional Requirement Specifications are given below.

4.3.1 Information Dissemination Component

This component deals with the Content creation, content updation and approval for the proper dissemination of information for availing the various services

S. No.	Functional Requirement Specifications - Information Dissemination
1.	The system should allow the authorized user(s) to update information obtained from the departments
2.	The system should provide detailed information on the following to the user: ▪ Scheme Name: ▪ Eligibility Criteria: ▪ Nodes of obtaining service: ▪ Application Fees: ▪ Grievance filing procedure: ▪ Authorities to contact: ▪ Forms and documents required: ▪ Other locations for obtaining detailed information
3.	The system should be able to add new or delete existing information components besides the above without any delay and without jeopardizing any other existing feature
4.	The system should be accessible to citizens, department officials, other government officials, e district centre operators, SCA
5.	The authorized user(s) should be able to update the document over the e district application but this information would not be viewable to the end user until the department head puts his digital signature, verifying its authenticity and correctness

S. No.	Functional Requirement Specifications - Information Dissemination
6.	The system should not allow any unauthorized user to upload information besides authorized user(s)
7.	The system should have different presentation layer for each set of users i.e. Information seekers, updaters, approvers etc.
8.	The system should notify the HoD once the information is updated over the e application
9.	The system should allow the HoD to either approve or reject the information update
10.	The system should update information over the e-district application only after digital signatures of the HoD has been put up on the information update
11.	The system should ask for digital signature of the HoD in case of rejection also
12.	The system should ask for changes from the HoD desired in case of rejection by the HoD
13.	The system should notify the authorized user(s) both in case of acceptance or rejection of the information update
14.	The system should allow only the authorized user(s) to make changes in the updated information hosted over the e district application
15.	The system should request authorized user(s) to put his digital signature after each updation
16.	The system should have a counter at the bottom of the page to record the number of people hitting the website, this would prove beneficial in capturing the usefulness of information
17.	The system should auto generate grievances in case of HoD or authorized user(s) are not performing against their set SLAs
18.	The system should capture time stamp and IP address of the user accessing the system
19.	The system should have bar-coding technology for printing and authorizing necessary documents.

4.3.2 Forms Availability Component

This component deals with the availability of latest electronic forms that will be made available in the e-District portal.

S.No	Functional Requirement Specifications – Form Availability
1.	The system should store all the service request form at predefined location for the selected services
2.	The system should be able to retrieve service request form from the predefined location
3.	The system should allow for service request form to be easily downloadable both through HTML and word format
4.	The size of the forms created for delivering the services through application shall be kept to the minimum so as to suit bandwidth typical to dial-up Internet connections. The form filling should be easy, user friendly and shall avoid common form filling errors (such as, ensuring all mandatory fields are entered, selecting options by checking boxes where applicable, number entry etc.)
5.	The Application shall provide Easy-to-use step-by-step guidance to fill the Forms in the form of form-wizards
6.	The system should provide for printable version of the service request form. The forms must be supported for use by the stakeholders on all widely used web` browsers like Chrome, IE, Mozilla etc. preserving the functionality, look and feel of the form. When printed, the eForms must preserve the appearance as on the screen"
7.	The system should give an error message in case it is not able to retrieve the application from the given location
8.	The system should have a provision for uploading new version of the forms as and when it is required to change the version
9.	The system should maintain the version control for the service request form
10.	The system should have a security feature embedded for changing the version of the form and should allow only predefined process owners to change the form version
11.	The system should maintain log for all version change with the details of the process owner making version change
12.	The system should not allow to change the content of the form and should be in read only version

S.No	Functional Requirement Specifications – Form Availability
13.	The system should be able to make available service request form should be through • Online / website • CSC • eDistrct Center/Facilitation Center
14.	The system should allow for easy searching of the service request form
15.	The system should allow for easy and user friendly layout for locating the service request form
16.	The system should be able to export forms in multiple formats so as to ensure compatibility of forms
17.	The system should have a life counter feature to keep track of number of forms being downloaded from the application
18.	The system should support multi-lingual interface (minimum Hindi and English) as per localization and language technology standards for National e-Governance plan defined in the e-District guidelines

4.3.3 Application Receipt Component

This component deals with the receipt of the application by the CSC/e-District centre operator and forwarding of the same to the concerned office, depending upon the nature of the service.

S.No	Functional Requirement Specifications – Application Request
1.	The System should enforce secure login as per the Login process, where the CSC or e-District center operator will have to authenticate his Username, Password to access the Application home page.
2.	The System, on successful login, should display the Main page or the Home page of the Applications Services Request with links to various services as per the Service Request Form mentioned above.
3.	The System should be able to retrieve and load the online Application Form for the service as selected by the Applicant / Operator.
4.	The System should assign a Unique Application Number to every form.
5.	The System should allow the Operator / Applicant to take a printout of the form before submitting it.
6.	The System should allow editing of the details in the online Application form even after a printout has been taken.
7.	The System should allow the Operator / Applicant to attach any scanned documents, photograph, or any other supplementary attachments as required with the Application Form
8.	The System should imprint the Unique Application Number and the ID details of the operator on the Application Form.
9.	The System should allow the operator to submit the Application Form online
10.	The System must display a message for Successful or Unsuccessful submissions and it should log all such events.
11.	The System must refresh the page and Load a new Application form in case the previous submission attempt was unsuccessful.
12.	The System should save the Application Form and all attached documents into a Database.
13.	The System should be able to immediately electronically forward the Application Form and the attachments and notify to the

S.No	Functional Requirement Specifications – Application Request
	Process Owner, as identified in respective processes.
14.	The System should be able to generate a Receipt for the Applicant, and allow it to be printed.
15.	The system should support multilingual interface (minimum Hindi and English) as per Localization and Language Technology Standards for National e-Governance Plan defined in e-district guidelines.

4.3.4 Payment Component

This component deals with the receipt of payment by the CSC/e-District kiosk operator for a particular service. The service charges and the revenue sharing model (between the participating departments, Implementation Agency of the CSCs & the CSC operators) for each of the services will be decided at a later stage. Each of the stakeholders should get their share as per the revenue sharing model with respect to each service.

S.No	Functional Requirement Specifications – Payment
1.	The system should provide for and allow financial transaction functions
2.	The system should check for all details of the service request form before initiating the payment
3.	The system should enable the payment option only when all the fields of service request forms are filled
4.	The system should return back and highlight the field which have inconsistencies / error for user to rectify the error
5.	The system should retain all the information of the service request form besides those having inconsistencies
6.	The system should return back after successful checking of the fields with the prompt of confirmation to open the payment page
7.	The system should open a new page for recording payment details against the service request
8.	The system should allow payment to be registered on the service application request against the following –

S.No	Functional Requirement Specifications – Payment
	▪ Payment against the service ▪ Payment against the dues / payments as defined under service charter of the specific service
9.	The system should record and maintain all details of payment against a unique service application number
10.	The system should be able to maintain all the payment records in a database and retrieve the same as and when required.
11.	The system should be able to open a page with declaration on successful payment output
12.	The system should able to record specific payment details on the service request form after successful payment has been made
13.	The system should be such that it should allow for part payment function
14.	The system should be able to retrieve information of first part payment during the final delivery of service output for final payment as per the overall payment specified for service request • Unique application number for requested service • CSC details and unique number for CSC
15.	The system should be able follow the payment cycle as mentioned above for the final payment also
16.	The system should be able to maintain all records of part payments as well as consolidated payment amount against the service request
17.	The system should support multi-lingual interface (minimum Hindi, Oriya and English) as per localization and language technology standards for National e-Governance plan defined in the e-District guidelines

4.3.5 Application Processing Component

This component deals with the processing of the application by the concerned authorities.- This component deals with the preparation of the Case file, noting and forwarding of the same to the Approver.

S.No.	Functional Requirements Specifications – Application Processing
1.	The System should notify the forwarder once the request has been forwarded from the CSC/e-District centre
2.	The system should provide inbox, forward, noting, view attachment facilities etc. to the forwarders
3.	The system should allow defined users(identified as forwarders) to login to the system for approving the service request through a valid user ID & password and bio-metric authentication
4.	The system should show a login failure screen in case the user name and password are not matched by the application
5.	The system should show a login failure screen in case the biometric authentication is not correct
6.	The system should highlight the pending service requests for the users on entering the application after the log-in
7.	The system should allow the forwarder to view the scanned supporting documents one by one, as uploaded by the Kiosk operator
8.	The system should allow 'zoom- in' and Zoom-out' facilities of the scanned documents for better viewing of the same
9.	The system should allow the forwarder to reject the application incase the application does not contain the required supporting documents
10.	The system should request forwarder to give comments in case of non-acceptance or forwarding
11.	The system should be able to generate an auto-file number before the forwarder forwards the application to the approving authority
12.	The System should be able to generate an auto generated note sheet before the forwarder forwards the application to the approving authority. Auto generated note sheet should not be editable and must record the full log of the said application users from start to end with time stamp and IP records.

S.No.	Functional Requirements Specifications – Application Processing
13.	The system should allow the forwarder to add to the note sheet before the submission of the application form to the approving authority
14.	The system should ask for re-confirmation of the forwarder before actually submitting the request
15.	The system should allow the forwarder to forward the applications individually and all at one go
16.	The system should open a page informing the forwarder of successful completion of approval/rejection

4.3.6 Verification Component

This component deals with the allocation of the field verification officers by the approving authority, if the required details are not found in the database or if the approving authority has doubts on the genuineness of the service requests.

S.No.	Functional Requirements Specifications – Verification
1.	The System should be able to allow the Process Owner/proper authority to enter query parameters to search any Database connected with the System.
2.	The System should be able to query the specified Database with the specified parameters and return the result of the same to the Process Owner.
3.	The System should be able to retrieve various information from the individual databases and aggregate it before displaying it.
4.	The System should allow the Process Owner to electronically, using his digital signature, forward / delegate the Application to a Field Officer or any other Officer registered with the System.
5.	The System should be able decode the digital signed data and display the details of the signatory.
6.	The System should allow the Field Officer to modify the Database as per the Access rights
7.	The System should allow the Field Officer to electronically forward the Application back to the Process Owner after the details in the Database have been updated.

S.No.	Functional Requirements Specifications – Verification
8.	The System should notify the Process Owner after the Field Officer has marked the Application back to him.
9.	The System should allow the Process Owner to either Approve or Reject the application as per the Approval or Rejection component, using his digital signature.
10.	The System should ensure that a Reason for Rejection is entered by the Process Owner if he selects to reject an application before accepting the Rejection.
11.	The System should log all the electronic movements of the application with date and time details along with the sender's and receiver's information.
12.	The system should support multilingual interface (minimum Hindi, Oriya and English) as per Localization and Language Technology Standards for National e-Governance Plan defined in e-district guidelines.

4.3.7 Approval/Rejection Component (Intermediary Approver and Final Approver)

This component deals with the approval/rejection by the concerned authority.

S.No.	Functional Requirements Specifications – Approval
1.	The system should allow defined users to login to the system for approving the service request through a valid user ID and password and bio-metric authentication
2.	The system should show a login failure screen in case the user name and password are not verified by the application
3.	The system should intimate the users through predefined channels for pending approval on a daily basis
4.	The pending approvals should highlighted for the users on entering the application
5.	The pending approvals should be intimated to the users through SMS on pre-defined intervals until the same is addressed and closed by the respective process owner
6.	The system should have a provision to mark the approval of service request

S.No.	Functional Requirements Specifications – Approval
7.	The system should allow the user to digitally sign the documents one by one
8.	The system should also allow the user the digitally sign all the selected approved service request at one go
9.	The system should open a page for all approved service request with a prompt of digital signature in form a button to initiate the process of digital signing
10.	The system should reconfirm from the user for initiating the digital signing before actually initiating the process
11.	Upon digitally signing the document, digitally signed document should be saved in the given repository for future references and a hard copy of the same document will be provided to the applicant
12.	System should print the unique encrypted key/code on the hard copy of the digitally signed document such that the same printed unique encrypted key/code can be used to check the authenticity of the document. The unique encrypted key/code will be information of the authority who digitally signed the document in the encoded form
13.	System should provide a link to the page where the user can enter the unique encrypted key/code printed on the hard copy of the document to check for the authenticity of the document
14.	On clicking the link, system should display the fields as described in the section Document retrieval form such that the user can retrieve the required information
15.	System should retrieve and display the digitally signed document on the user screen once the user enters the unique encrypted key/code printed on the document
16.	System should not allow the user to make any alteration in the digitally signed document or access the database on entering the unique encrypted key/code
17.	System should display an appropriate message in case of retrieval failure or any other communication failure or in case the document could not be found due to any reason

S.No.	Functional Requirements Specifications – Approval
18.	The system should allow the user to terminate the approval process at any point of time during approval
19.	The system should keep and maintain the data in a data repository (database) for all the approval made
20.	The system should be able to keep the records of all transaction performed and link it to the unique code of digital signature
21.	The system should open a page informing the user of successful completion of approval
22.	The system should open a page at any point of process in case the process termination with the request to restart the process
23.	The system should not allow the user to initiate the process of digital signature in case of no selection of pending service request for approval
24.	The system should not allow the user to modify the approval once it has been digitally signed
25.	The system should not allow the user to delete any service request pending for approval at his end
26.	The system should support multi-lingual interface (minimum Hindi, Oriya and English) as per localization and language technology standards for National e-Governance plan defined in the e-District guidelines

4.3.8 Delivery Component

This component deals with the issuance of the final output from the CSC/e-District centre to the applicant, on producing the application receipt issued to the citizen at the time of submission of application.

S.No.	Functional Requirements Specifications – Delivery
1.	The system should be able to provide delivery against all service request made
2.	The system should be able to link delivery against specific service request through unique service application request number
3.	The system should allow delivery only when the service request has been either approved / rejected
4.	The system should allow only validated predefined users to log into the e-district application for retrieving the delivery against the service request

S.No.	Functional Requirements Specifications – Delivery
5.	The system should ask for unique service request number / unique application number to retrieve specific service delivery
6.	The system should provide for the printable version of the service output
7.	The system should be able to print the unique kiosk number, unique application number on the every service output generated through it
8.	The system should be able to print the url of the site from where the content of the service delivery could be verified
9.	The system should have adequate security features built in the architecture of the system to ensure that it cannot be manipulated
10.	The system should open new page specifying error in case of incorrect digital verification
11.	The system should be able to maintain the database of the all the service delivery output in a logical manner to ease the retrieval of the same as and when required
12.	The system should have a life counter to keep log of all delivery made with specific association of unique service application number and unique CSC number
13.	The system should support multi-lingual interface (minimum Hindi, Oriya and English) as per localization and language technology standards for National e-Governance plan defined in the e-District guidelines

4.3.9 Status Component

This component deals with the status tracking component with which the status can be tracked by the user and the citizens for the requested service.

S.No	Functional Requirement Specifications – Status Component
1.	The system should have integrated auto status tracking features embedded in the overall architecture of the system
2.	The system should keep track of all the service requests from the citizens along with the respective unique application reference id generated at the time of the application receipt
3.	The system should be available in public and administrative view
4.	The system should be able to keep track of the status of all the service requests with the help of the respective unique application reference id (application id) and map the current status with the pre-defined service level against each process
5.	The system should be able to detect any change in the status of a given unique application reference id
6.	In case there is a change in the status of a unique application reference id , the system should update the status information in the database
7.	The system should have provisions for intimating the applicant about the current status of his/her application through SMS and/or Email especially if there is a change in the status with respect to the final delivery of the service
8.	The system should not provide details about the internal SLAs to the applicant and only provide update about the status with respect to the final delivery. This feature should also allow the system to update the applicant if there is any change in the service level of the final delivery
9.	System should display the link for e-district portal from where the applicant can retrieve the status information by entering the unique application reference id

S.No	Functional Requirement Specifications – Status Component
10.	The system should also allow the applicant to retrieve update about his/her service request through the web portal by entering the reference id in the link provided on the portal
11.	System should display the number from where the applicant can retrieve the status information by sending SMS along-with the unique application reference id
12.	The system should also allow the applicant to retrieve update about his/her service request by sending a SMS containing the unique application reference id to the e-District application
13.	The system should display an appropriate message if the system is unable to retrieve the details due to any reason like connectivity issues, maintenance issues, etc and also provide contact details of the system administrator and alternate link (if available)
14.	The System should have Side Menu on each page so as to reflect the contents of the containing directory, making it easier to navigate the site and locate the link for retrieving update against a given reference id
15.	The system should be adequate security features built in the architecture of the system to ensure that it cannot be hacked or manipulated
16.	The system should not allow the users to edit the details of the application upon retrieving the status update against a given reference id
17.	The System should allow the end user to print the status update information if the applicant is retrieving the status through the portal or email
18.	The System should have provision for Calendar System, which displays the dates and time of schedule events on a page formatted as a standard monthly calendar
19.	The system should have additional capability to integrate and extend portals to support a vast array of mobile devices in addition to PCs (WAP enabled)

S.No	Functional Requirement Specifications – Status Component
20.	The system should have provisions such that the System Administrator can add/remove/modify the hierarchy of the Government officials with adequate authentication mechanism
21.	If there is any modification in the hierarchy of the relevant authority against a given service (in the system), system should automatically map the escalation levels with the new hierarchy of Government officials
22.	The system should support multi-lingual interface (minimum Hindi, Oriya and English) as per localization and language technology standards for National e-Governance plan defined in the e-District guidelines

4.3.10 Monitoring Component (MIS)

This component deals with the generation of various reports at various levels who are involved in the delivery of services under the e-District project.

S. No.	Functional Requirement Specifications – Monitoring Component
1.	The Process Owner should be able to use the e-District Application to query the Departmental Databases using the name or other details of the applicant.
2.	Should allow the e-District Application to retrieve various information from the individual databases and aggregate it
3.	The application should support the monitoring in both the occurrence, when an event or time driven activity is triggered.
4.	Should be able to retrieve all information about the status of the application form of the citizen.
5.	Should be able to automatically generate the following reports to the concerned authorities at regular time interval:-
6.	Should be able to generate Service Report on a regular time interval, this report should include the no of application received, no of application processed, no of application rejected and the no of application under process.
7.	Should able to generate SLA Report on regular time interval, this report should give information related to centre wise details of no of SLA met and centre wise details of no of SLA breached.

S. No.	Functional Requirement Specifications – Monitoring Component
8.	Should be able to generate Performance Report on regular time interval, this report should give information related to centre wise details of no of application processed against the no of application received.
9.	Should be able to generate Payment Report on regular time interval, this report should give information related to centre wise transaction, money collected and money deposited along with date and time.
10.	Should be able to generate Inventory Report on regular time interval, this report should give information related to pre-printed stationary used and issued to each centre.
11.	Should be able to generate Attendance Report on regular time interval, this report should give information related to centre wise attendance.
12.	Should provide a search option to the authorized stakeholder so that he can search the information which should be sorted according to Date, Department/Section, Service, District, Block, Sub Division, Tehasil, RI Circle etc
13.	Should allow the stakeholder to review the progress report and give his comments online.
14.	Should provide the facility to print and e-mail the report.
15.	Should provide a printer – friendly version automatically for all pages.
16.	The system should support multi-lingual interface (minimum Hindi, Oriya and English) as per localization and language technology standards for National e-Governance plan defined in the e-District guidelines

4.3.11 Log in Component

S. No.	Functional Requirement Specifications – Log In Component
1.	Should allow only the authentic users (Kiosk Operators, Department Officials) to login to the system through the use of: ▪ User id and Password combination (for kiosk operators and verification officers) ▪ Both (for Forwarders and issuing Authorities)
2.	Should display the login page as the first page when the user enters the e district application.
	User id & Password Combination
1.	The user login and password both should be a combination of following: Alphabets (at least 1) , Special Character, Numeric
2.	The user name and password should have a minimum of 8 characters each
3.	Should not create duplicate user ids or passwords
4.	Should not allow the user to have the same password for more than 30 days
5.	Should generate alerts for password expiry from two days of actual expiry
6.	Should not allow same user id and password
7.	Should not allow blank spaces while setting user id or password
8.	Should notify the user in case the Caps Lock is on
9.	Should notify the use if Num Lock is on
10.	Should generate user id based on the criteria of - Zone, district, Circle an SCA name, kiosk number
11.	Should not allow a user who forgets the password to access the password retrieval mechanism
12.	Should allow only the machines whose mach id is registered with the application enter the e district application
13.	Should prompt the user to change the password in case of first login at the client side i.e. after imaging
14.	Should give a welcome message once the user is able to successfully login to the e district application.

S. No.	Functional Requirement Specifications – Log In Component
15.	Should give an error message once the user provides wrong login information and ask the user to re log in.
16.	Should block the user to enter into the e-district application if he puts in wrong login info continuously thrice.
17.	Should support multilingual interface (minimum Hindi, Oriya and English) as per Localization and Language Technology Standards for National e-Governance Plan defined in e-district guidelines

4.3.12 Service Specific Functionalities

The e-District portal is envisaged to be a single point information access for all the users under the e-District project through which the citizens can avail the specific services and get the required information of those services that are proposed to be delivered under e-District project. This portal will provide comprehensive information about the services of District Administration, its functions and also host links to certain specific categories of services which can be availed through the Common Service Centres (CSCs)/e-District Centres. Service Specific functionalities comprise of functions that are specific to service categories/services and deals with the day-to-day functioning of the same. Indicative Functional Requirement Specifications for one of the Certificate is mentioned below. SPMU shall prepare the As-Is, To-Be Process, FRS document for the services and the same shall be handed over to the selected bidder after approval to carry out necessary task at his end.

S. No.	General Functional Requirement Specifications
1	The system should be able to display Service related page through multiple routes, Service links, Information links, District links
2	The system should be able to identify the user logging into the system using the login component.
3	The system should be able to provide information to the citizens about the relevant services both in public as well as private domain as per the 'Information component' Web access to information content in public domain

S. No.	General Functional Requirement Specifications
	e-District application access to information content
4	The system should make available the latest copy of the Application Form online (24x7) as per the Form Availability component.
5	The system should be able to retrieve the service request form for a particular service
6	The system should allow the operator to fill in the online application on behalf of citizen availing the service as per the 'application receipt' component
7	The system should be able to generate a unique registration number during registering an applicant with the application.
8	The system should be able to identify the applicant uniquely based on this registration number for all future references.
9	The system should be able to record the payment made by the applicant against the service as per the Payment Component
10	The system should display a message regarding successful or unsuccessful completion of any transaction.
11	The system should refresh the page in case of failure in submission of service request
12	The system should be able to issue an acknowledgement receipt once the applicant is registered with the system
13	The system should be able to notify the concerned officer about the new application and this date and time must be logged through e-District application
14	The system should allow concerned officials to view the service request only on authenticated login as per login process
15	The system should show service request to concerned Approving authority as pending for approval till it is marked for further action by default the system should be able to auto escalate within the service level as per the escalation matrix defined
16	The system should be able to auto generate MIS reports for the following officials as per the requirement– District Collector, Sub Collectors/Tehasilders/BDOs, Other concerned authorities
17	The system should be able to support the status tracking as per the status tracking component

S. No.	General Functional Requirement Specifications
18	The system should be able to support the monitoring and reporting as per the monitoring and reporting component
19	The system should be able to detect changes in status and send status updates to the citizen as per the Status Tracking component.
20	The system should be able escalate the application as per the Auto Escalation matrix, defined, by notifying the next level of authority and sending him a copy of the application.
21	The system should be able to maintain all records for the login sessions with date and time
22	The system should be able to provide date and time stamping for all transactions done with digital signature
23	The system should have a facility for forwarding of the application, with remarks and digital sign of the sender, to any person in District administration registered with the System.
24	The system should support multilingual interface (minimum Oriya, Hindi, English) from the first day of its operation, as per Localization and Language Technology Standards for National e-Governance Plan defined in e-district guidelines.

4.4 Bill of Material Summary

4.4.1 Requirement at Field Level Offices

Item Name	Dist. Magistrate Office	Sub Collector Office	Tahsildar Office	BDO Office	Total Nos.
Laptop	56	51	536	266	858
Desktop	224	102	536	532	1394
UPS	224	102	536	532	1394
Printer	140	102	536	266	1044
Laser Jet Printer, Scanner, Copier all in one Device	28	0	0	0	28
Scanner	56	102	536	266	960
Biometric Device	280	153	1072	798	2303
Antivirus	280	153	1072	798	2303
24 Port LAN Switch	56	51	268	0	375
9 U Networking Rack	56	51	268	0	375
UTP cable CAT-6 (Box of 305 Mtrs)	56	51	268	266	641
Jack Panel 24 Port CAT 6	56	51	268	0	375
Information Outlet CAT6	420	255	1340	1330	3345
Surface Mount Box Single	420	255	1340	1330	3345
Mounting Cord 7 Ft. CAT 6	420	255	1340	1330	3345
Mounting Cord 3 Ft. CAT 6	420	255	1340	1330	3345
6 Core Generic Multimode Fiber with necessary terminator & LIU adapter as per actual	14000Mtr	0	0	0	0

P.S.: Number of equipment's/peripherals displayed in the above table may vary during the actual implementation in the field. In case of variance the actual requirements needs to be presented in front of the SDA. After approval, the unit price quoted by the selected vendor will be taken into consideration for payment. Also, as per requirements, the distribution of materials across the offices may also vary during the actual course of implementation.

4.4.2 Requirement at SDC

Sl No.	Item	Total Qty (Q)
1.	Web Server	1
2.	Database Server	2
3.	Application Server	2
4.	Staging/Production Server	2
5	Rack Mounted 8-Port IP based KVM Switch	1
6	Server For Helpdesk and SLA	2
7	Server for Antivirus	1
8	Antivirus Software solution	1
9	24 Port Managed LAN Switch	1
10	42 U Server Rack with PDU	1
11	My SQL Enterprise Edition Latest version	2 no.s license

4.5 Technical Specifications

For information of the bidders, this is to share that following numbers of servers were procured during pilot implementation of eDistrict Project.

Sl.No	Description of Item	Quantity	Make/Model
1	Web Servers	1	IBM 8204 Model E8A
2	Application Servers	1	IBM 8204 Model E8A
3	Database Servers	2	IBM 8204 Model E8A

The specifications of the existing server are as follows.

Specification of each Server	
Specified Components of Server	**Qty.**
RIO-2 (Remote I/O-2) Cable, 3.5M	1
146GB 15K RPM SAS Disk Drive	2
4096MB (2x2048MB) RDIMMs, 667 MHz, 1Gb DRAM	4
2-core 4.2 GHz POWER6 Processor Card	2
4MM 80/160GB TAPE, SAS, (CADENZA-4 SAS)	1
Dual-Port 1Gb Integrated Virtual Ethernet Daughter Card	1
IBM 2-Port 10/100/1000 Base-TX Ethernet PCI-X Adapter	1
4 Gb Dual-Port Fibre Channel PCI-X 2.0 DDR Adapter	1
SATA Slimline DVD-RAM Drive	1
2-Port 10/100/1000 Base-TX Ethernet PCI Express Adapter	2
4 Gigabit PCI Express Dual Port Fibre Channel Adapter	1
Power Cable -- Drawer to IBM PDU, 14-foot, 250V/10A	1
Power Cord (9-foot), Drawer to IBM PDU, 250V/10A	1
IBM/OEM Rack-Mount Drawer Rail Kit	1
IBM Rack-mount Drawer Bezel and Hardware	1
Power Supply, 1700 Watt AC, Hot-swap, Base and Redundant	2
PowerVM Express	4
DASD/Media Backplane for 3.5 DASD/SATA DVD/Tape	1
Three Years Onsite Comprehensive Warranty	1

The selected SI needs to work on a new set of servers, specifications of which are to be referred from the following tables.

4.5.1 Specification of Web, Database, Application Server

SlNo	Features	Specifications	Specification Offered	Compliance (Yes/No)	Deviation if any
1	Form Factor	Rack Mountable			
2	CPU	2 Nos X86 based Processor. Processor Core Per CPU should be minimum Eight. The Frequency should be minimum 2.4 GHz. The Server should scalable up to 4 processors.			
3	L3 Cache	20MB or more Cache per processor			
4	Memory	Server should be configured with 256 GB of ECC DDR3 Memory and scalable to 1 TB or more.			
5	Clustering	Server should support Clustering.			
6	DIMM Slots	Server should support 16 DIMM Slots and should be expandable up to 32 DIMM Slots using 4 sockets.			
7	HDD Bays	Minimum 4 Hot Plug SFF SAS / SSD disk bays.			
8	Optical drive	DVD-RW (Internal / External)			
9	Hard disk drive	Server should be configured with 2 * 600GB 10K SAS 6Gbps SFF HDD scalable up to 4 drives. To be configured with RAID 1.			
10	RAID Controller	PCIe 3.0 based SAS Raid Controller with RAID 0/1/1+0 with 512MB flash backed write cache.			
11	Networking features	Server should be configured with the minimum 4 or more nos of 10 Gb Ethernet ports (populated with requisite number of trans receiver, if required). Connectivity of the ports should be compatible for both 10G and 1G Link			

12	IPv6 Ready	Server should be IPv6 Ready			
13	HBA Controller	Dual Port 8Gbps FC HBA Card			
14	Bus / PCIe Slot	Server should support 5 or more nos. of PCIe 3.0 slots			
15	Fan	Hot Plug Redundant Fans			
16	Power Supply	Hot Plug Redundant Power Supply			
17	Industry Standard Compliance	ACPI 2.0 Compliant, PCIe 3.0 Compliant, PXE support, WOL Support, USB 2.0 Support.			
18	OS Support	Server should support latest version of Microsoft Windows Server, RHEL, SLES, Vmware.			
19	OS to be bundled with	The server should be configured with latest version of SUSE Linux Enterprise Server along with High Availability Extension for X86, AMD64 & Intel64 (Up to 4 CPU Sockets, 3 Years Subscription)			
20	Remote Management	1. System remote management should support browser based Graphical Remote Console. 2. Should provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD. 3. The Server Management Software should be of the same OEM as of the server supplier. Complete Licensing (If any) for Server Management Soft-			

		ware should be provided.			
21	Warranty	3 years Comprehensive Onsite warranty with support of 24x7 (for hardware & OS) from OEM.			

4.5.2 Specification of Staging/Production server

SlNo	Features	Specifications	Specification Offered	Compliance (Yes/No)	Deviation if any
1	Form Factor	Rack Mountable			
2	CPU	2 Nos X86 based Processor. Processor Core Per CPU should be minimum Eight. The Frequency should be minimum 2.4 GHz. The Server should scalable up to 4 processors.			
3	L3 Cache	20MB or more Cache per processor			
4	Memory	Server should be configured with 512 GB of ECC DDR3 Memory and scalable to 1 TB or more.			
5	Clustering	Server should support Clustering.			
6	DIMM Slots	Server should support 16 DIMM Slots and should be expandable up to 32 DIMM Slots using 4 sockets.			
7	HDD Bays	Minimum 4 Hot Plug SFF SAS / SSD disk bays.			
8	Optical drive	DVD-RW (Internal / External)			
9	Hard disk drive	Server should be configured with 2 * 600GB 10K SAS 6Gbps SFF HDD scalable up to 4 drives. To be configured with RAID 1.			
10	RAID Controller	PCIe 3.0 based SAS Raid Controller with RAID 0/1/1+0 with 512MB flash backed write cache.			
11	Networking features	Server should be configured with the minimum 4 or more nos of 10 Gb Ethernet ports (populated with requisite number of trans receiver, if required). Connectivity of the ports should be compatible for both 10G and 1G Link			
12	IPv6 Ready	Server should be IPv6 Ready			
13	HBA Controller	Dual Port 8Gbps FC HBA Card			
14	Bus / PCIe Slot	Server should support 5 or more nos. of PCIe 3.0 slots			
15	Fan	Hot Plug Redundant Fans			

16	Power Supply	Hot Plug Redundant Power Supply			
17	Industry Standard Compliance	ACPI 2.0 Compliant, PCIe 3.0 Compliant, PXE support, WOL Support, USB 2.0 Support.			
18	OS Support	Server should support latest version of Microsoft Windows Server, RHEL, SLES, Vmware.			
19	OS to be bundled with	The server should be configured with latest version of SUSE Linux Enterprise Server along with High Availability Extension for X86, AMD64 & Intel64 (Up to 4 CPU Sockets, 3 Years Subscription)			
20	Remote Management	1. System remote management should support browser based Graphical Remote Console. 2. Should provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD. 3. The Server Management Software should be of the same OEM as of the server supplier. Complete Licensing (If any) for Server Management Software should be provided.			
21	Warranty	3 years Comprehensive Onsite warranty with support of 24x7 (for hardware & OS) from OEM.			

4.5.3 Specification of Rack Mounted 8-Port IP based KVM Switch

Sl No	Description	Specification Offered	Compliance (Yes/No)	Deviation if any
1	KVM Switch should be IP Based.			
2	The switch supports dual interface (PS/2 or USB) keyboard and mouse computer connections with automatic interface detection.			
3	The switch should allow both local & remote operators to monitor and control the Servers.			
4	Should have monitor and control minimum 8 Servers.			
5	Multiplatform support like Windows, Linux, Mac, and Sun, RISC Architecture, X-86 Architecture			
6	Servers can be added or removed without having to power down the KVM switch			
7	Should support USB or PS/2 keyboard and mouse emulation (Servers boot even when the console focus is elsewhere)			
8	Should support up to 2048 x 1536; DDC2B video quality			
9	Servers can be selected via front panel pushbuttons, hotkeys and multilingual on-screen display (OSD) menu of the KVM switch			
10	Should have two level password security for authorized users administrator to view and control servers with a separate profile for each			
11	Rack mountable			
12	Should have 8 Nos 6 ft. USB KVM Cable			
13	Should support Multilanguage web UI support featuring a tree-structured local and remote OSD			
14	Should support IPv6			
15	Should support IP/MAC Filter			
16	Should support authentication for Local and remote access			
17	Should support external authentication support: RADIUS, LDAP, LDAPS, MS Active Directory			

4.5.4 Specification for 24 Port Managed LAN Switch for SDC

Features	Specifications	Specifications Offered	Compliance (Yes/No)	Deviations if any
Make	Must be specified			
Model	All the relevant product brochures and manuals must be submitted.			
General	The OEM of the Switch shall be from one of the leaders as per the latest Gartner's Magic Quadrant Report on Wired LAN category"			
Architecture	The switch should have 24 x 10/100/1000BaseT ports plus 2 x 1000BaseX ports			
	Should support 1000 Base-SX, LX Mini-GBICs			
	Should have a minimum of 50 Gbps switching capacity			
	Should have a minimum of 100 Gbps Forwarding capacity			
	Should have switching throughput of 65 million pps			
	MAC Address table size of 8,000 entries			
	Should support minimum of 9216 bytes jumbo frame – Ethernet frame			
	Should support minimum of 9198 bytes MTU .			
	All the switch ports Should offer non-blocking, wire speed performance			
Resiliency and high availability	Should support IEEE 802.3ad Link Aggregation Control Protocol (LACP)			
	Should support IEEE 802.1s, IEEE 802.1d STP & IEEE 802.1w RSTP			
Layer 2 switching	Should support IEEE 802.1Q VLANs, up to 256 port-based VLANs			
	Should support GVRP or IEEE 802.1Q or Equivalent			
Security	Should support MAC and IP-based ACLs and Time-based ACLs			
	Should support IEEE			

Features	Specifications	Specifications Offered	Compliance (Yes/No)	Deviations if any
	802.1X user authentication			
	Should support Web-based authentication & MAC-based authentication			
	Should support management access securely encrypted through SSL and SNMPv3			
	The Switch should be IPv6 Ready from Day 1.			
Convergence and QoS	Should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)			
	Should support LLDP-MED			
	Should support IEEE 802.1p Traffic prioritization			
	Should support IP multicast (data-driven IGMP) to automatically prevent flooding of IP multicast traffic			
	Should support rate limiting			
Manageability	Should support SNMPv1/v2c/v3			
	Should support Web Interface for switch configuration			
	Should support Port mirroring			

4.5.5 Specification for servers for Helpdesk, SLA and Antivirus

4.5.5.1 Specification of Blade chasis

Feature	Specifications
Make	Must be specified
Model	Must be specified. Tower Model Required. Must be specified. All the relevant product brochures and manuals must be submitted.
Form Factor	Up-to 10 U Form factor per chassis with all redundancy features (Hard Drives, Power, and Cable Management). The requisite number of Enclosures to be configured to populate the Servers and Storage/Expansion Units
Blade Bays	Blade Chassis to accommodate minimum of 8 hot pluggable blade servers with SAS HDDs.
Chassis Feature	▪ Dual network connectivity for each blade server for redundancy should be provided. ▪ Backplane should be completely passive device. If it is active, dual backplane should be provided for redundancy ▪ Should have the capability for installing industry standard flavors of Windows, Linux, Unix, Solaris for x86 Operating Environments ▪ Single console for all blades in the enclosure or KVM Module ▪ DVD ROM can be internal or external, which can be shared by all the blades allowing remote installation of S/W and OS ▪ Minimum 2 external USB connections functionality
Ethernet Switch Modules	Two hot-plug, redundant 1Gbps Ethernet module which enable connectivity to Ethernet via switch. Switch should be Internal/external. The number of Ethernet ports should be sufficient to connect fully populated chassis being offered to network.
SAN Connectivity	Two hot-plugs, redundant 4 Gbps Fiber Channel for connectivity to the external Fiber channel Switch and ultimately to the storage device.
Redundancy	Mechanical Devices such as Hard Disks, Fans and Power Units should be completely Hot Swappable and Redundant to ensure High Availability
Blade Management	▪ Systems Management and deployment tools to aid in Blade Server configuration and OS deployment, ▪ Remote management capabilities through internet browser ▪ Blade enclosure should have provision to connect to display console / central console for local management like trouble shooting, configuration, system status / health display
Power	▪ Hot Swap redundant power supplies to be provided ▪ Power supplies should have N+N. All Power Supplies modules should be populated in the chassis
KVM	To be enabled Virtually over IP for Remote Access

4.5.5.2 Specification of Servers

Features	Specifications Required
Make	Must be specified
Model	Must be specified. All the relevant product brochures and manuals must be submitted
Part No	Must be specified for all the required components
CPU	Two numbers X86 based Processor. Processor Core Per CPU should be Minimum Six. The Frequency should be minimum 2.0 GHz. Processor should be latest series/generation for the server model being quoted
Chipset	Suitable Processor OEM motherboard/chipset
Form factor	Half/Full Height Blade with I/O connectivity to backplane
Memory	32 GB ECC DDR3-SDRAM DIMMs
Memory Expandability	Minimum 128 GB
Controllers	Integrated SAS Raid Controller with RAID 0, 1
Bays	Dual 2.5" SAS Hard Disk bays
Hard Disk Drives	Two 146 GB 2.5" SAS Hard Disk Drive hot swappable system disk with mirroring using integrated RAID 0,1 on internal disks
Ethernet Adapter	Dual Port 1000BASE-T Gigabit Ethernet Adapter
SAN Connectivity	The Blade should have redundant 4/8 Gbps Fiber Channel HBA (For Application and Mail Messaging)
I/O Expansions	I/O expansion slot for up gradation of Ethernet Adapter
Power Supply	From the Blade Chassis
System Management and Diagnostics	LED lights indicating failing component and on-board diagnostics (via on-board system management processor)
Software	Server Management software with the device drivers
OS Compatibility	Microsoft Windows Server latest version Standard Edition (32 bit and 64 bit) Microsoft Windows Server latest version Enterprise Edition (32 bit and 64 bit) Red Hat Enterprise Linux latest version (32 bit and 64 bit) Red Hat Enterprise Linux latest version (32 bit and 64 bit) SUSE LINUX Enterprise Server latest version (32 bit and 64 bit) SUSE LINUX Enterprise Server latest version (32 bit and 64 bit)
Warranty	3 year comprehensive warranty

4.5.6 Specification of Desktop

Features	Specifications	Specifications Offered	Compliance	Deviations if any
Make	Must be specified			
Model	Tower Model Required. Must be specified. All the relevant product brochures and manuals must be submitted.			
Part No.	Must be specified for all the required components			
Processor	Intel Core i-3 Processor or equivalent AMD Processor Minimum 2.2 GHz, 3 MB cache			
Motherboard	Intel Q57 or AMD equivalent chipset or OEM motherboard			
Bus Architecture	Integrated Graphics, Integrated (on board) High Definition Audio controller with internal/external speaker, also 2 PCI/PCIe slots			
Bays	2x Internal 3.5” bays, 2xExternal 5.25” bays			
Memory	4 GB DDR3 SDRAM			
Hard Drive	320 GB SATA HDD			
Removable drive	52 X Sata CD ROM drive			
Network	Integrated 10/100 Mbps Ethernet Adapter (RJ-45), PXE support			
Key board	Normal Keyboard(Minimum 86 Keys)			
Mouse	2 button optical wheel mouse			
Monitor	17” TFT Color Monitor			
Interface	1 serial, 5 USB (Minimum 2 in front), 1 PS/2 Keyboard, 1 PS/2 Mouse, VGA, audio ports for Microphone & headphones in front.			
OS Certification	Microsoft Windows			
Office Productivity Suite	Microsoft Office Standard 2013 Indic OLP Gov			
OS	Windows 7 Professional Edition or higher edition preloaded			
Certification	For OEM:ISO 9001 and 14001. For quoted Model: FCC, UL, Energy Star 5.0, DMI			

4.5.7 Specification of Laptops

Features	Specifications	Specifications Offered	Compliance	Deviations if any
Make	Must be specified			
Model	Must be specified. All the relevant product brochures and manuals must be submitted.			
Part No.	Must be specified for all the required components			
Processor	Intel Core i-3 Processor or equivalent AMD Processor Minimum 1.8 GHz, 2 MB cache			
Motherboard	Compatible motherboard to support the processor and memory. Motherboard from the original OEM.			
Memory	4 GB DDR3 SDRAM			
Hard Drive	320 GB SATA			
Removable drive	Integrated DVD R/W			
LAN Network	Integrated 10/100 Mbps Ethernet Adapter (RJ-45), PXE support			
Wireless Support	Integrated 802.11 b+g 54 MBPS Wireless LAN adapter			
Key board	Spill-resistant keyboard (minimum 86 keys) with bi-lingual keys (English and local language of the State) compliant to Enhanced Inscript Keyboard based on Unicode version 6.0 or later.			
Graphics	Integrated Graphics with up-to 384 MB of shared memory			
Display	14.1" WXGA Active TFT (1280X800) & with Integrated WEB CAMERA (1.3 MP)			
Interface	3 USB 2.0, 1XLine in , 1X MIC , 1XRJ45 LAN, 1X External VGA , 1X DC In			
Power	Universal DC Adapter			
Battery	6 Cell Li Ion Battery			
OS Certification	Microsoft Windows			
Office Productivity Suite	Microsoft Office Standard 2013 Indic OLP Gov			
OS	Windows 7 Professional Edition or higher edition preloaded			

4.5.8 Specification of Scanner

Features	Specifications	Specifications Offered	Compliance	Deviations if any
Make	Must be specified			
Model	Must be specified. All the relevant product brochures and manuals must be submitted.			
scanner type	Flatbed/Sheetfeed			
input modes	front panel scan, copy buttons,			
speed	**preview speed:** 10 seconds **Scan speed:** Photo to files: 29 secs; Text to document: 26 secs			
Résolution	4800 dpi optical resolution, 4800 x 9600 dpi hardware resolution,			
Imaging Technology	CCD			
bit depth	48-bit			
scaling	10 to 2000%			
max document size	220 x 300 mm			
Interface and Operating System Compatibility	USB -compatible with USB 2.0,Windows 7 Home and Professional Edition			
power	Universal AC adaptor: 100 to 240 VAC (+/- 10%), 50/60 Hz (+/- 3Hz) input (according to configuration), 12 VDC, 1.25 Amp output, Energy Star™ compliant			

4.5.9 Specification of Laser Jet Printer, Scanner, Copier all in one Device

Features	Specifications	Specifications Offered	Compliance	Deviations if any
Make	Must be specified			
Model	Must be specified. All the relevant product brochures and manuals must be submitted.			
Print speed	Minimum 25 PPM Letter			
Resolution	▪ Printing: upto 1200 x 1200 dpi ▪ Copying: up to 600 x 600 dpi ▪ Scanning: up to 1200 x 1200 dpi			
Printing Features	▪ Manual duplex and booklet printing ▪ N-up printing, ▪ Collation, ▪ Watermarks, ▪ Economic mode for toner savings			
Copying Features	▪ 1 to 99 multiple copies ▪ reduce/enlarge from 25 to 400% ▪ 2-up or 4-up allowing 2 or 4 pages to be copied onto 1 page ▪ Contrast (lighter/darker), ▪ resolution copy quality (draft, text, mixed)			
Scanning Features	▪ Flatbed scanner up to letter, A4 size; ▪ supported file types: JPEG, TIFF, PDF, GIF, and BMP ▪ Should be able to scan Legal Documents			
Control panel	▪ 2-line LCD text display, ▪ Asian character support, ▪ 16-character display, ▪ menu and navigation buttons, ▪ copy control buttons, ▪ cancel button			
Memory	32 MB RAM			
Paper Handling Tray	▪ 10-sheet priority input tray, ▪ 250-sheet multipurpose input tray, ▪ 125-sheet output bin, ▪ manual two-sided printing			

Features	Specifications	Specifications Offered	Compliance	Deviations if any
Paper Size	▪ 76 x 127 mm (3 x 5 inches) to 216 x 356 mm (8.5 x 14 inches); ▪ letter, ▪ legal, ▪ index cards, ▪ postcards; ▪ A4, ▪ A5			
Interfaces	▪ Hi-Speed USB 2.0 port, ▪ Ethernet port			
operating systems support Required	Windows 7 Home and Professional Edition ; Windows Vista, Linux			
Power	220 to 240 volts (±10%), 50/60 Hz (±2 Hz) Input Power port with required English power chord			

4.5.10 Specification of Laser Printers

Features	Specifications	Specifications Offered	Compliance	Deviations if any
Make	Must be specified			
Model	Must be specified. All the relevant product brochures and manuals must be submitted.			
Print speed	Up to 14 ppm A4 &letter			
Resolution	Up to 600 x 600 dpi			
Printing Features	▪ Manual duplex printing ▪ N-up printing, ▪ Economic mode for toner savings			
Memory	2 MB RAM			
Paper Handling Tray	▪ 150-sheet adjustable main input tray, ▪ 100-sheet output bin, ▪ manual two-sided printing			
Paper Size	▪ A4, ▪ A5, ▪ A6, ▪ B5, ▪ letter, ▪ legal, ▪ postcards, ▪ envelopes			
Interfaces	Hi-Speed USB 2.0 port,			
operating systems support Required	Windows 7 Home and Professional Edition ; Windows Vista, Linux			
Power	220 to 240 volts (±10%), 50/60 Hz (±2 Hz) Input Power port with required English power chord			

4.5.11 Specification for 1 KVA offline UPS

Parameter	Specifications	Specifications Offered	Compliance	Deviations if any
Make	Must be specified			
Model	Must be specified. All the relevant product brochures and manuals must be submitted.			
Type	Line-interactive			
Capacity	1 KVA			
Input Voltage Range	90 – 280 V AC			
Input Frequency	50 Hz +/-10%			
Output Voltage	220 V +/- 10% (under line mode)			
	220 V +/- 5% (under battery mode)			
Output Frequency	50 Hz +/- 1% (under battery mode)			
Noise	< 40 db at 1 m			
Protection	Overload, Short Circuit, Low Battery			
AVR	Built in Automatic Voltage Regulator (AVR)			
Indicators	LED indicators for AC Mains, DC, Load on Mains/Battery			
Battery Type & back-up time	Batteries shall be of Sealed Maintenance Free (SMF) type The system must be capable of providing requisite battery back-up time of 60 minutes using SMF Batteries as per VAH rating below : **(Minimum VAH for 60 minutes back-up = 1008 VAH)** Total number of batteries offered should be clearly mentioned. Voltage of each battery offered should be clearly mentioned. Ampere-Hour rating of each battery offered should be clearly mentioned. Total Volt-Ampere-Hour rating of the Battery Bank Offered			

Parameter	Specifications	Specifications Offered	Compliance	Deviations if any
	should be clearly mentioned.			
Recharge Time to 90% capacity	3 to 4 hours			
Ambient Conditions	Temperature: 0 to 45 deg Celsius Humidity: upto 95%			
Certifications	ISO 9001			

4.5.12 Specification for 9 U Rack

Feature	Specification	Specifications Offered	Compliance	Deviations if any
Make	Must be specified			
Model	All the relevant product brochures and manuals must be submitted.			
Dimensions	600(w)x 530(d)x 9U(h)			
Weight Capacity	132 lbs (60 kg)			
Side doors	Complete knockdown format for easy installation & later maintenance; with lock & key			
Ventilation	Standard with one side exhaust fan			

4.5.13 Specification of Biometric Device

Feature	Specification	Specifications Offered	Compliance	Deviations if any
Make	Must be specified			
Model	All the relevant product brochures and manuals must be submitted.			
Identification Time (s)	<=2 Sec			
Enrollment and Matching	Upto ten finger prints for enrollment and one Finger print for matching			
Fingerprint placement(Optional)	Any Angle (360°)			
Resolution	Minimum 500 PPI/DPI			
FAR	<0.0001%			
FRP	<1%			
Connectivity	Ethernet :- 10/100 Base T(UDP) USB:- Standard USB connectivity for PC based application			
Serial Communication (bps)	9600/38400/115200(Rs 232/Rs 485)			
Operating Temperature (0°C)	0-45			
Operating Humidity (%)	20 -80			
Display Language	English			
Operating Voltage	5 VDC			
Power	Should be USB Powered			

4.5.14 Specification of 24 Port Managed LAN Switch

Features	Specifications	Specifications Offered	Compliance	Deviations if any
Make	Must be specified			
Model	All the relevant product brochures and manuals must be submitted.			
Architecture	The switch should have 24 x 10/100/1000BaseT ports plus 2 x 1000BaseX ports			
	Should support 1000 Base-SX, LX Mini-GBICs			
	Should have a minimum of 50 Gbps Switching capacity			
	Should have switching throughput of 36 million pps			
	MAC Address table size of 8,000 entries			
	All the switch ports Should offer non-blocking, wire speed performance			
Resiliency and high availability	Should support IEEE 802.3ad Link Aggregation Control Protocol (LACP)			
	Should support IEEE 802.1s, IEEE 802.1d STP & IEEE 802.1w RSTP			
Layer 2 switching	Should support IEEE 802.1Q VLANs, up to 256 port-based VLANs			
	Should support GVRP or IEEE 802.1Q or Equivalent			
Security	Should support MAC and IP-based ACLs and Time-based ACLs			
	Should support IEEE 802.1X user authentication			
	Should support Web-based authentication &			

Features	Specifications	Specifications Offered	Compliance	Deviations if any
	MAC-based authentication			
	Should support management access securely encrypted through SSL and SNMPv3			
Convergence and QoS	Should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)			
	Should support LLDP-MED			
	Should support IEEE 802.1p Traffic prioritization			
	Should support IP multicast (data-driven IGMP) to automatically prevent flooding of IP multicast traffic			
	Should be IPv6 Ready from Day 1			
	Should support rate limiting			
Manageability	Should support SNMPv1/v2c/v3			
	Should support Web Interface for switch configuration			
	Should support Port mirroring			
Certification	The OEM of the Switch should be from one of the leaders as per the latest Gartner's Magic Quadrant Report on Wired LAN category			

For each hardware, Bidder should provide the following information in a table

i. Reference of the server/storage information in the Submitted Proposal (Please provide page number/section number/ volume)
ii. Services proposed to be hosted on the Server
iii. Quantity
iv. Year of Introduction

v. Operating System along with version (if applicable)
vi. Processor and Number of Cores Offered (if applicable)
vii. Architecture (RISC/EPIC/CISC) (if applicable)
viii. RAM/HDD/LAN Ports/ HBA (as relevant)
ix. Additional Information as required to indicate the compliance to the requirements in the RFP (ex, Capacity, Disk Space) (if applicable)

Important Note for bidders:

i. It is mandatory to furnish complete technical specifications of the hardware & peripherals being offered, strictly as per the format, provided here. Correct technical information of the product being offered must be filled in.
ii. Filling the technical specifications/ information in the format using terms such as 'OK', Accepted', 'Noted', 'As given in Brochure/ Manual', 'Complied' is not acceptable. The offers not adhering to these guidelines are liable to be rejected.
iii. All relevant product information such as user manuals, technical specifications sheet etc. should be submitted along with the offer. Failure to submit this information along with the offer could result in disqualification of the bid.
iv. In case any technical variance is offered, the same must be specified under the "Deviation, if any" column.
v. For each item, the bidders should propose only one product.
vi. These specifications should be considered as the minimum to be fulfilled.

4.5.16 Specification of Antivirus software

Anti-Virus software to protect LAN Servers

The software should be with following functionality:

- Shall provide domain based central management – organize and manage computers in logical domains
- Shall support pattern file rollback – shall be able to return to past pattern file if problem with new file
- Able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)
- The solution should support true file type or true file type group scanning and blocking
- Shall be able to remotely uninstall the antivirus software
- The solution shall be able to block specified ports and Network shares on all the servers to stop the proliferation of Network viruses which use ports to spread after entering the Network
- System does not require restarting of the Virus Scanning service after a Pattern update
- Shall be able to scan Object Linking and Embedding (OLE) File

Anti-Virus software to protect Desktops on the network

The software should be with following functionality:

- Must have a Personal Firewall to protect the clients from common network based hacker attacks and Intrusion detection features
- Must have enhanced Spyware/Adware detection capabilities in real-time
- Must have exclusion list to exclude Spyware/Adware from scanning
- Virus Outbreak Monitor and Firewall Outbreak Monitor to notify the Antivirus server/Administrator when the client detects excessive network traffic or log counts from IDS/personal firewall exceed certain thresholds respectively
- Should have flexible port blocking capabilities in the Personal Firewall component which can permit or deny traffic from a specified port or range of ports
- The Client firewall should use stateful inspection to scan network traffic for profile and security level; filters connections by IP address, port number and protocol
- Should support Network Virus Scanning to detect and drop infected packets from the network layer
- Outbreak Prevention option to block specific shared folders, ports, and to deny write access to specified files and folders on selected clients from the central console during a virus outbreak
- Should be able to specify CPU usage during file scans
- Should have a feature to consolidate virus logs resulting from recurring infections made by the same network virus and send them to the Antivirus server
- Should come in-built with a Policy server which will have the ability to configure settings to perform actions on at-risk clients to bring them into compliance with the organization's antivirus policies
- Should be able to deploy the Client software using the following mechanisms:
    - Support MSI in Client Packager tool
    - Notify Clients to install via E-Mail
    - Client Packager tool for client local install
    - Web Install via Active X control
    - NT Remote Install
    - Via Login Script
- Through disk imaging:- is one of the means to transfer the client version of antivirus
- Support MS Systems Management Server (SMS)
- There should be only a one-time deployment of the client Antivirus components (Antivirus, Firewall, Spyware and Damage Cleanup) rather than deploying it separately
- The update component should download all components required including the pattern file, scan engine, program files, damage cleanup template/engine, Spyware pattern, firewall engine

and network worm engine instead of downloading every component separately

- The Server component should have the flexibility to update itself from multiple update sources
- Clients should get virus updates, Spyware/Adware pattern updates, network worm updates and personal firewall updates from a single server Antivirus server
- Clients should automatically look at another update source to get updates if the primary antivirus server is not available
- Solution must allow specified clients to act as Update Agents (sources for updated components) so other clients can receive updates from these clients to ensure effective use of corporate bandwidth
- Should provide with Web-based centralized management through which all the clients can be centrally managed / configured for antivirus and firewall policies
- Secure remote access via Web browser (SSL-enabled)
- Customizable client alert message for virus detection and Personal Firewall
- Should generate Virus activity log, update log, Personal firewall/intrusion detection log, network virus logs, Client connection status log and Server system event log and should be able to send notification to the infection source
- A quarantine manager to set the capacity of the quarantine folder and the maximum size of the quarantined files
- Should have a feature to scan and detect for vulnerable systems in the network and remotely deploy the client software to them automatically
- Able to automatically uninstall existing antivirus software at the desktop
- Solution should be capable of protecting itself from virus attacks

HTTP Gateway level Antivirus and URL Filtering solution

- The solution should be a single product solution to provide HTTP & FTP Gateway level Antivirus. The product should be software based solution
- The solution should support Microsoft Windows & Linux platforms
- The solution should be a fully integrated solution designed to block Web-based threats, including Viruses, Trojans, Worms, Phishing attacks and Spywares / Adwares
- The solution should be capable of preventing installed Spyware from sending confidential data via HTTP
- The solution should be capable of working in the following configurations; (1) As a standalone proxy, (2) Integrated with upstream proxy servers, (3) Integrated with ICAP-compliant caching servers, Network Appliance, or BlueCoat, (4) It should be capable of working as a transparent proxy utilising WCCP or a Load balancer, (5) Reverse proxy
- The solution should support True File type Scanning

- The solution should be capable of automatically blocking Infected URLs
- The solution should be capable to taking action on password-protected or encrypted files
- The solution should be able to selectively bypass certain MIME content types
- The solution should be capable of automatically sending a customized email message on detecting malicious code in a file, which a user requested
- The solution should have Inbuilt logging and reporting capabilities (Reports by User/Group, Consolidated user reports, Blocking events report, traffic report etc.)
- The solution should log performance statistics, including CPU usage, Memory usage, and number of transactions processed
- The solution should support for Remote Installation
- The solution should support SNMP based System and Event Notifications
- The solution should be able to Rollback the pattern file update if required
- It should allow setting of URL policies by category, group, or user and control access by time of day, day of week, and bandwidth quotas to improve network performance, reduce legal liability, and increase productivity
- It should support Microsoft Active Directory, Linux OpenLDAP Directory and Sun Java System Directory Server via LDAP, enabling IT administrator to easily set policies and assign rules for single PCs or groups
- Support for Customizable URL access/deny Rule Sets and additional customizable allow/deny categories & Sites
- URL, Internet resource access restriction capability based on Network, IP Address, Users, Groups etc.

4.6 Non-Functional Requirements

The non-functional requirements relating to performance, availability, deployment, implementation, operations and others are listed in the subsequent subsection. Based on the assessment of the requirements listed below, SI shall prepare System Requirement Specifications (SRS) and obtain a formal sign-off before proceeding with the design and implementation of the solution.

Technical Solution Architecture Requirements	
1.	The e-District solution needs to be architected using robust and proven software and hardware technologies like Service-Oriented Architecture (SOA) and open industry standards.
2.	The solution architecture should be built on sound architectural principles enabling fault-tolerance, high-performance, and scalability both on the software and hardware levels.
Software Architecture Requirements	
1.	Software architecture must support web services standards including XML, SOAP, UDDI and WSDL

2.	Software architecture must support appropriate load balancing for scalability and performance
3.	Software architecture must support flexibility in adding functionalities or applications.
4.	Software architecture components should utilize the high availability, clustering, and load balancing features available in the proposed hardware architecture to increase system performance and scalability features.
5.	Software architecture must support trace logging, error notification, issue resolution and exception handling.
Hardware Architecture Requirements	
1.	Hardware architecture at SDC must provide redundancy and high availability capabilities at the hardware level; this includes servers, etc. However, the hardware infrastructure for the DRC can be as per the SDC specifications.
2.	All servers and systems must be configured with no single point of failure.
3.	Hardware architecture should be capable of consolidating several applications / workloads in a number of servers as required.
4.	Servers must be placed within proper security infrastructure for the Solution.
5.	Hardware architecture must support existing Storage Area Network (SAN) & backup solution (at SDC)
6.	The technical solution architecture for e-District should be sound and complete with high performance, redundancy, and scalability.
Development, Testing, Staging, and Production Requirements	
1.	Appropriate development, test, and staging hardware environments should be provided and explained how they are related to production environment. This must be supported by explanations on how the development, test, and staging environment support the implementation activities of e-District Solution.
2.	Development and test environment should include configuration management capabilities and tools for system configuration, versioning scheme, documentation, change control processes and procedures to manage deployment of solution deployment.
3.	The test, development, and staging environment should include required workstations, desktops, and tools appropriate to support development, testing, and staging, and deployment tasks.
4.	The development, test, and staging hardware environments must include similar operating systems, software components, products, and tools to those of production environment.
5.	The development, test, and staging environments should be independent logically and physically from the production environment and of each other.
6.	The development environment should be used for development and should be configured to allow access for developers' workstations.
7.	The staging environment should be used for functional and user acceptance testing, stress testing, and performance benchmarking.
8.	The test environment should be used as a testing environment of e-District Solution and its software components and products. The test environment should be a scaled-down configuration of the production environment.
Security Requirements	

1.	A secure solution should be provided at the hardware infrastructure level, software level, and access level.
2.	Authentication, Authorization & Access Control 3 factors (User ID & Password, Biometric, and Digital Signature) security mechanisms should be implemented to enable secure login and authorized access to portal information and services.
3.	Confidentiality of sensitive information and data of users and portal information should be ensured.
4.	Appropriate mechanisms, protocols, and algorithms necessary to protect sensitive and confirmation data and information both during communication and storage should be implemented.
Monitoring and Management Requirements	
1.	The e-District Solution should provide monitoring and management of the entire Solution including all software components and application.
2.	The monitoring and management should monitor health of software and hardware infrastructure running the e-District Solution covering operating system, database, software components, applications, servers, and other related software and hardware components. It should provide proactive monitoring, alerting and reporting.
Performance and Scalability Requirements	
1.	The design of the e-District Solution should be scalable to handle increasing number of users.
2.	e-District Solution should provide measurable and acceptable performance requirements for users, for different connectivity bandwidths.
3.	The e-District solution should provide optimal and high performance Portal Solution satisfying response time for slow Internet connections and different browsers.

Implementation Requirements	
1	The SI will be required to deploy manpower and other project resources as per the terms & conditions of the Contract
2	The SI will be required to work closely with the SDA and perform detailed functional requirements and analysis of e-District Solution to confirm and document functional / system requirement specifications for the portal and its applications to fulfill its objectives.
3	The SI will be expected to carry the complete implementation and deployment of the e-District within the timelines specified in the RFP.
4	The SI is expected to develop, test, stage, and deploy all functional modules of the e- District software and any hardware components of technical & functional requirements
Project Management	
1	Selected bidder is required to provide an implementation plan illustrating all functional analysis, development, testing, staging, and deployment activities
2	Selected bidder is required to specify and describe the different phases and activities of the project. It is very important for the SDA that the Selected bidder provide a quality implementation plan covering all aspects of the project. The plan shall clearly specify the start and end dates (relative to contract signing) of each of the project phases specifying key milestones allowing visibility of project progress.
3	Selected bidder is required to use standard project management tools such as precedence diagrams, critical path charts, etc. to create and manage implementation plan and schedule. The table below shows the minimum stages and deliverables:

Stage	Activities	Deliverables
Design	• Detailed Software Solution Architecture design • Detailed Hardware Solution Architecture Design	• Design Specifications Documents of Software solutions • Design Specifications Documents of Hardware solutions

		• Data Schema design • User Interface Design • Integration & Interfaces Design • Prototyping design • Validation • Documentation	• User Interface Design Specifications • Integration Design Specifications • Data design and migration
	Development	• Software installation, configuration, and customization • Hardware installation and configuration • Development • Unit Testing • Documentation	• Development Plan • Updated Design Document • Installed software and hardware • Functional modules & Portal Solution • Problem reporting
	Testing	• System Testing • Integration Testing • Stress Testing • Load Testing • User Acceptance Test Results • Completed Test Cases • Data Migration tests • Documentation	• Complete Test Cases • Test Plan • User Acceptance Criteria • Problem reporting • Problem resolution testing • Data Migration Testing
	Deployment	• Training courses and sessions • Operations Planning • User Manual • Operations Manuals	• Knowledge Transfer and training plan • Operations Plan • Operations Policies and Procedures
4	Selected bidder is required to describe in detail project management processes, methodologies and procedures.		
5	Describe what SDA resources will be necessary for the project to succeed.		
6	Describe how SDA management will receive up-to-date reports on project status.		
7	Describe the change management procedures to handle such things as "out-of-scope" requests or changing business needs of SDA while the project is underway.		
8	Describe what procedures will be used to keep the project on track, and what escalation procedures will be employed to address any problems with project progress.		
9	Describe what quality assurance processes, procedures, formal reviews, etc. will be in place.		
10	Describe the proposed conflict resolution / escalation process between the Bidder and SDA to handle project or contractual disputes.		
11	Selected bidder is required to describe the proposed project structure identifying all project individuals including project manager, business analysts, software developers, QA engineers, hardware / network engineers, administrators, Change Management experts, and others.		
12	Selected bidder shall provide a comprehensive warranty that covers all components after the issuance of the final acceptance of e-District. The warranty should cover all materials, licenses, services, and support for both hardware and software. Selected bidder shall administer warranties with serial number and warranty period. Upon final acceptance of the SDA, all OEM warranties will be transferred to the SDA at no additional charge. All warranty documentation (whether expired or not) will be delivered to SDA at the issuance of the final acceptance certificate		
13	Selected bidder is required to provide Premium Level warranty and support through the vendor for all hardware and software used for e-District. Selected bidder' warranty must cover all equipment and work activities contained in the contract against all design, manufacturing, and environment faults until the issuance of the final acceptance.		

14	Selected bidder is required to commit to the following warranty terms: • All products / components / parts shall be covered under OEM warranty up to the Implementation Phase and AMC support shall commence after successful implementation. • The warranty shall include the repair or replacement of the products / components / parts during the warranty period by the bidder. The replacement products / components shall meet the related specifications without further repair or modification. • Selected bidder shall be liable for all costs including, but not limited to, the costs of material, labour, travel, transport and living expenses associated with the collection and return of the units covered by the warranty. • The date of manufacture or assembly of any equipment, parts or consumables, shall not be more than six months before delivery. • Selected bidder shall state the location of his repair Centre(s) for all items not being repaired onsite. • SDA has the right to require a replacement if the repair is deemed to be impractical. • Selected bidder ensures that replacement components shall be available for any failed component during the warranty period. • Selected bidder shall guarantee the availability of spare parts and technical assistance for all components (or appropriate alternatives) to ensure the equipment would run for at least five (5) years, without major changes, at the completion of final acceptance. Six months advance notice is required on any discontinued part(s) with a suggestion for alternatives. • Selected bidder need to define the process & methodology in their proposal, for achieving the response time of engineers to respond to an incident and also for resolving such incidents as per the SLA. • Selected bidder is required to provide additional training if the satisfaction levels/ learning does not reach 80% in evaluation/feedback from trainees, and expected to provide additional training, if required. • The e-District application & infrastructure being provisioned by the bidder shall be insured. The Goods supplied under the Contract shall be fully insured against loss or damage incidental to manufacture or acquisition, transportation, storage and delivery for the entire project term. Selected bidder is required to explain their warranty, maintenance procedures, and support to meet the terms and requirements outlined above.
Operations Requirements	
1	The selected bidder is expected to provide the following in support of e-District operations: Selected bidder shall provide procedure documentation for all operations procedures, and SLA's (based on ITIL best practices) for all the hardware and applications provided including backup procedures, system update procedures, security procedures, failure recovery procedures, upgrade procedures, remote access procedures, user manual, SOP's etc. All such procedures and documents must be submitted for review and approval by the SDA prior to adoption. Such documentation shall be updated by the during the project term by the bidder as and when required along with the necessary approval. Selected bidder will be required to provide SDA with weekly statistics reports on the various services provided to users a mechanism as well as track and log all related statistical reports on the various delivery channels and access patterns. Selected bidder will be required to provide SDA with weekly portal performance reports showing health of system operations.

	Selected bidder will be required to provide SDA with Helpdesk resources for recording all the day to day problems and other technical incidents occur during the O&M phase. This shall also record the resolution of such incidents & problems. Selected bidder will be required to commit to Service Level Agreements (SLAs) that show, among other metrics, appropriate escalation procedures and guarantee corrective actions within a pre-determined time. Selected bidder is required to respond to required levels of accuracy, quality, completeness, timeliness, responsiveness, cost-effectiveness, productivity and user satisfaction that are equal to or higher than the SLA system requirements.
	Quality Assurance & Acceptance Requirements
1	Selected bidder is required to develop and implement quality assurance processes and procedures to ensure that the e-District development and operations are performed to meet the quality standards that are relevant to each area in all project phases.
2	Selected bidder is required to use various tools and techniques that can make tests run easily and the results are automatically measured. In this way, testing tools provide a more cost-effective and efficient solution than their manual counterparts. Plus, they minimize the risk of human error during testing
3	In order to ensure that such a QA mechanism is effective and acceptance of e-District, the following tests are required for acceptance: Unit Testing: Basic validation of developed components by developers. Functional / Internal Integration Testing: Validation of developed components against functional requirements and design specifications. System Testing: Validation of both functional and technical requirements for the integrated Solution. This could include external integration if required or it can be separated into testing phases. UAT: User Acceptance Testing (UAT) validation of the Portal Solution and assurance that it meets both functional and technical requirements Stress and Performance Testing: Load testing enabling understanding of performance and behaviour of Portal Solution under large number of users and high-load conditions.
4	Selected bidder is required to describe their QA and testing approaches and procedures as well as testing tools for conducting various tests in support of the acceptance of the Portal Solution. Selected bidder is expected to follow minimum CMMi level 3 processes.
5	Furthermore, Selected bidder to describe their documentation standards e.g. Documentation description, documentation identification, content, nomenclature etc. as well. Sample documents to be enclosed as part of the technical proposal.
Quality Assurance & Acceptance Requirements	
1	Selected bidder is required to develop and implement quality assurance processes and procedures to ensure that the e-District development and operations are performed to meet the quality standards that are relevant to each area in all project phases.
2	Selected bidder is required to use various tools and techniques that can make tests run easily and the results are automatically measured. In this way, testing tools provide a more cost-effective and efficient solution than their manual counterparts. Plus, they minimize the risk of human error during testing.
3	In order to ensure that such a QA mechanism is effective and acceptance of e-District, the following tests are required for acceptance: • Unit Testing: Basic validation of developed components by developers. • Functional / Internal Integration Testing: Validation of developed components against functional requirements and design specifications. • System Testing: Validation of both functional and technical requirements for the integrated Solution. This could include external integration if required or it can be separated into testing phases. • UAT: User Acceptance Testing (UAT) validation of the Portal Solution and assurance that it meets both functional and technical requirements • Stress and Performance Testing: Load testing enabling understanding of performance

	and behaviour of Portal Solution under large number of users and high-load conditions.
4	Selected bidder is required to describe their QA and testing approaches and procedures as well as testing tools for conducting various tests in support of the acceptance of the Portal Solution. Selected bidder is expected to follow minimum CMMi level 3 processes.
5	Furthermore, Selected bidder to describe their documentation standards e.g. Documentation description, documentation identification, content, nomenclature etc. as well. Sample documents to be enclosed as part of the technical proposal.

4.7 CSC Rollout Status (As on July 2014)

Sl #	State	SCA	Divi-sions / Zones	Name of Districts	Total CSCs to be set up	Roll Out	CSCs Con-nected	BSNL (1)	VSAT (2)	Data Card BSNL (3)	Oth-ers (4)
1	Odisha	Zoom De-velopers	Zone 1	Balasore	492	333	306	88	0	48	170
2	Odisha	Zoom De-velopers	Zone 1	Bhadrak	219	219	110	32	0	7	71
3	Odisha	Zoom De-velopers	Zone 1	Jajpur	296	196	132	57	0	1	74
4	Odisha	Zoom De-velopers	Zone 1	Ken-drapara	257	236	144	80	0	0	64
5	Odisha	Zoom De-velopers	Zone 1	Mayur-bhanj	658	445	346	140	0	0	206
6	Odisha	SREI Sahaj	Zone 2	Cuttack	325	254	205	107	92	6	0
7	Odisha	SREI Sahaj	Zone 2	Jagatsing hpur	215	144	123	98	21	4	0
8	Odisha	SREI Sahaj	Zone 2	Khurda	258	161	153	114	31	8	0
9	Odisha	SREI Sahaj	Zone 2	Nayagarh	282	164	149	118	22	9	0
10	Odisha	SREI Sahaj	Zone 2	Puri	286	167	136	86	45	5	0
11	Odisha	Zoom De-velopers	Zone 3	Angul	318	137	118	17	0	16	85
12	Odisha	Zoom De-velopers	Zone 3	Deogarh	146	51	30	16	0	2	12
13	Odisha	Zoom De-velopers	Zone 3	Dhen-kanal	202	133	77	35	0	5	37
14	Odisha	Zoom De-velopers	Zone 3	Keonjhar	354	235	191	80	0	0	111
15	Odisha	Zoom De-velopers	Zone 3	Sunder-garh	294	239	196	99	0	0	97
16	Odisha	SREI Sahaj	Zone 4	Bargarh	201	217	180	117	50	13	0
17	Odisha	SREI Sahaj	Zone 4	Bolangir	299	198	167	120	36	11	0
18	Odisha	SREI Sahaj	Zone 4	Boudh	198	71	61	30	28	3	0
19	Odisha	SREI Sahaj	Zone 4	Jhar-suguda	58	85	67	28	35	4	0
20	Odisha	SREI Sahaj	Zone 4	Sam-balpur	220	150	138	88	43	7	0
21	Odisha	SREI Sahaj	Zone 4	Sonepur	160	108	105	66	36	3	0
22	Odisha	BASIX	Zone 5	Gajapati	270	170	163	8	0	0	155
23	Odisha	BASIX	Zone 5	Ganjam	535	469	449	93	0	0	356
24	Odisha	BASIX	Zone 5	Kan-dhmal	424	146	110	8	0	0	102
25	Odisha	BASIX	Zone 5	Rayagada	445	190	181	14	0	0	167
26	Odisha	SREI Sahaj	Zone 6	Kalahandi	373	254	232	36	193	3	0
27	Odisha	SREI Sahaj	Zone 6	Koraput	338	271	249	35	210	4	0
28	Odisha	SREI Sahaj	Zone 6	Mal-kangiri	174	115	107	6	97	4	0
29	Odisha	SREI Sahaj	Zone 6	Naba-rangpur	150	179	161	17	142	2	0
30	Odisha	SREI Sahaj	Zone 6	Nuapada	111	110	99	13	86	0	0
		TOTAL			**8558**	**5847**	**4885**	**1846**	**1167**	**165**	**1707**

Annexure: A - Comparison of list of services

Sl No.	Service Categories	Sub – Services for State Wide Rollout as per RFP	Included under Pilot Application
1	Certificates	1. Issuance of Birth Certificate (Above 1 Year Case)	No
		2. Issuance of Death Certificate (Above 1 Year Case)	No
		3. Issuance of Disability Certificate	Yes
2	Social Security	4. Sanction of Assistance under NFBS	Yes
		5. Sanction of Indira Gandhi National Old Age Pension Scheme	Yes
		6. Sanction of Indira Gandhi National Disability Pension Scheme	Yes
		7. Sanction of Indira Gandhi National Widow Pension Scheme	Yes
		8. Sanction of Funds under MBPY	Yes
3	Revenue Court & Cases	9. Registration of Societies	No
		10. Certified Copies of RoR	Yes
		11. Conversion of Land Under OLR-8 (A)	Yes
		12. Certified copies of other Documents	No
4	Ration Card Related Services	13. Mutation of Ration Cards (Addition/Deletion of Names)	Yes
		14. Issue of Fresh/Duplicate ration card	Duplication of Ration Card was only included as a service
		15) Change of FPS/Dealer	No
5	RTI/Grievances	16) Grievance Registration to Collector	No
6	Health	17. Application for Registered Medical Practitioner Certificate	No
7	ST & SC Development	18. Application for Study Loan for ST/SC students	No
		19. Scholarship for ST/SC students	No
8	School & Mass Education Department	20. Issue of Conduct certificate	No
		21. Application for scholarship for students under S&ME Dept.	No
9	Higher Education Department	22. Application for Scholarship services for students under Higher Education Department	No
10	Employment	23. Application for registration to Employment Exchange.	No

Annexure: B – Service Wise Total Number of Transactions (As on 31st July 2014)

S. No	District Name	Issuance of Resident Certificate	Issuance of Income Certificate	Issuance of Caste Certificate	Issuance of Solvency Certificate	Issuance of SEBC Certificate	Issuance of OBC Certificate	Issuance of Legal Heir Certificate	Certified Copy of RoR	Total Transactions
1	Bargarh	1852	1080	1399	0	724	618	0		5673
2	Angul	2804	892	922	2	607	609	44		5880
3	Balasore	15081	7096	4030	1	2301	1243	88		29840
4	Bhadrak	3961	949	191	0	153	177	8		5439
5	Boudh	2956	1871	3081	0	1307	752	10		9977
6	Deogarh	8004	6559	5572	0	1540	2228	16		23919
7	Jajpur	14290	6297	7338	4	2106	2146	117		32298
8	Kalahandi	4165	2694	3593	0	428	1086	0		11966
9	Kendrapara	4439	1669	1413	0	660	535	10		8726
10	Balangir	12324	2432	3843	0	865	993	32		20489
11	Cuttack	3026	573	109	0	85	47	0		3840
12	Dhenkanal	9637	3627	5624	7	1849	3340	13		24097
13	Jagatsinghpur	7940	2988	2251	1	1661	910	35		15786
14	Jharsuguda	875	748	1065	0	89	22	0		2799
15	Keonjhar	16257	8790	11442	1	3344	1562	84		41480
16	Koraput	5206	3763	6692	1	461	336	19		16478
17	Nayagarh	12142	4133	4400	10	3116	4014	93		27908
18	Puri	3110	341	223	0	195	106	1		3976
19	Rayagada	6575	6985	5227	1	395	407	41		19631
20	Nabarangpur	2757	2318	3857	2	239	151	18		9342
21	Kandhamal	7045	5532	9423	0	1121	212	22		23355
22	Nuapada	4246	1907	2773	8	389	690	67		10080
23	Khordha	3246	1301	781	0	397	234	18		5977
24	Sundargarh	8619	6175	6663	3	594	385	9		22448
25	Gajapati	4873	3038	3331	1	590	325	19		12177
26	Subarnapur	7540	3633	6805	1	1093	1909	38		21019
27	Malkangiri	2277	1610	1633	1	37	7	62		5627
28	Sambalpur	6778	3370	3546	1	810	1126	12		15643
29	Mayurbhanj	148616	87838	58491	95	21943	43579	2391	8051	371004
30	Ganjam	152370	116464	134815	50	22268	8295	2993	9281	446536

Annexure: C – Office Jurisdiction

District	Sub-Division	Tahsil	BDO	RI Office
Sundargarh	3	18	17	112
Jharsuguda	1	5	5	32
Deogarh	1	3	3	20
Sambalpur	3	9	9	55
Keonjhar	3	13	13	80
Angul	4	8	8	55
Bhadrak	1	7	7	75
Jajpur	1	10	10	80
Dhenkanal	3	8	8	50
Balasore	2	12	12	85
Nuapada	1	5	5	32
Bolangir	3	14	14	86
Subarnapur	2	6	6	38
Boudh	1	3	3	22
Kandhamal	2	12	12	74
Cuttack	3	15	14	128
Khurda	2	10	10	71
Puri	1	11	11	107
Kendrapara	1	9	9	92
Jagatsinghpur	1	8	8	76
Bargarh	2	12	12	84
Kalahandi	2	13	13	80
Nawrangpur	1	10	10	66
Rayagada	2	11	11	81
Gajapati	1	7	7	44
Koraput	2	14	14	233
Malkangiri	1	7	7	44
Nayagarh	1	8	8	50
28	**51**	**268**	**266**	**2052**