M P State Electronics
Development Corporation Ltd.
(A Govt. of M.P. Undertaking)
State IT Centre, 47-A, Arera Hills, Bhopal 462011 M.P.
Tel: 0755 – 2518300, 2518500, 2518459; www.mpsedc.com

Ref: MP PARICHAI Project (MPSEDC/PARICHAI/RFP/2019/408)

Selection of System Integrator for Takeover existing, re-architect, Development, Implementation and Maintenance of MP PARICHAI Solution

Date –18thFeb 2019

Volume II

MPSEDC is already running a project named PARICHAI (formerly SRDH) in which it provides Aadhaar authentication services to various government departments / agencies, as Aadhaar authentication User Agency (AUA) of Unique Identification Authority of India (UIDAI). The provided services are governed by Aadhaar Act 2016 and subsequent regulations, guidelines issued by UIDAI, Govt. of India, Govt. of Madhya Pradesh, and any other directives issued by court of law. The PARICHAI supports in efficient service delivery to residents, support Departments towards better planning and monitoring of schemes and provides a platform for Aadhaar enabled service delivery to the State Government Departments. MPSEDC has published this RFP for selection of System Integrator (SI) who shall be responsible for takeover existing, re-architect, development, implementation and maintenance of the PARICHAI solution, after completion of the existing SI handling the solution.

Table of Contents

1 Contents

Abbreviations

Acronyms	Description
API	Application Program Interface
KYC	Know Your Customer
KYR	Know Your Resident
Aadhaar Act 2016*	THE AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016 * All terminology related to Aadhaar ecosystem will be as per the Act, irrespective of its definition in this RFP.
Requesting Entity (RE)	As per the Aadhaar Act 2016, a requesting entity means an agency or a person that submits Aadhaar number and demographic information or biometric information, of an individual to the Central Identities Data Repository (CIDR) for authentication.
ASA	Authentication Service Agency (also called Requesting Entity)
AUA	Authentication User Agency (also called Requesting Entity)
KSA	KYC Service Agency (equivalent to ASA or Requesting Entity)
KUA	KYC User Agency (equivalent to AUA or Requesting Entity)
Sub-AUA / Sub-KUA	Agency taking services of AUA for Aadhaar Authentication / eKYC as per Aadhaar Act 2016.
CIDR	Central Identity Data Repository
CSV	Comma-Separated Values
DAO	Data Access Object
DQ	Data Quality
DSCI	Data Security Council of India
EID	Enrolment Identity
EMD	Earnest Money Deposit

FRS	Functional Requirements Specifications.
HLD	High Level Design
HSM	Hardware Security Model
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IDE	Integrated Development Environment
MP	Madhya Pradesh
MPSEDC	Madhya Pradesh State Electronic Development Corporation
ORM	Object Relational Mapping
OTP	One Time PIN
PL	Project Leader
PM	Project Manager
PoA	Proof of Address
PoI	Proof of Identity
PSB	Public Sector Bank
PSU	Public Sector Undertaking
RASF	Remote Aadhaar Seeding Framework
RFP	Request For Proposal
SFTP	Secure File Transfer Protocol
SOAP	Simple Object Access Protocol
SOR	Schedule of Requirements
PARICHAI	Portal of Age, Residential address, Image Collecting Hub for Aggregate Information

SRS	Software Requirements Specifications
TBD	To be Determined
UI	User Interface
UID	Unique Identification
UIDAI	Unique Identification Authority of India.
UTF	Unicode Transformation Format
VTC	Village Town City
WAR	Web Archive
XML	Extensible Markup Language

1 Section I: Functional Requirements

The project PARICHAI envisaged with an objective to provide effective and efficient Government service to citizens. To effectively perform this activity, there is a need to uniquely identify the beneficiaries and gather information about schemes where the individual is registered as a beneficiary, **as per** UIDAI guidelines, Aadhaar Act 2016 and subsequent regulations, supreme court verdicts and any other directives from the government of India and / or State of Madhya Pradesh.

The uniqueness of identity of beneficiary can be obtained by Aadhaar. It will help departments create an authentic and de-duplicated data repository for their beneficiaries. This will support Government Departments towards better planning and monitoring of schemes and shall provide a platform for Aadhaar enabled service delivery to the State Government Departments. The PARICHAI is working as project under Madhya Pradesh State Electronics Development Corporation (MPSEDC) Limited, which is a government of Madhya Pradesh undertaking under Department of Science and Technology. MPSEDC is Aadhaar Authentication Agency (AUA), and provides Aadhaar Authentication services, Aadhaar eKYC services and Management Dashboard for overall monitoring to various departments of government of Madhya Pradesh in PARICHAI project. These functional modules shall formulate the functional offering of PARICHAI to the State Government Departments and agencies as identified by MPSEDC.

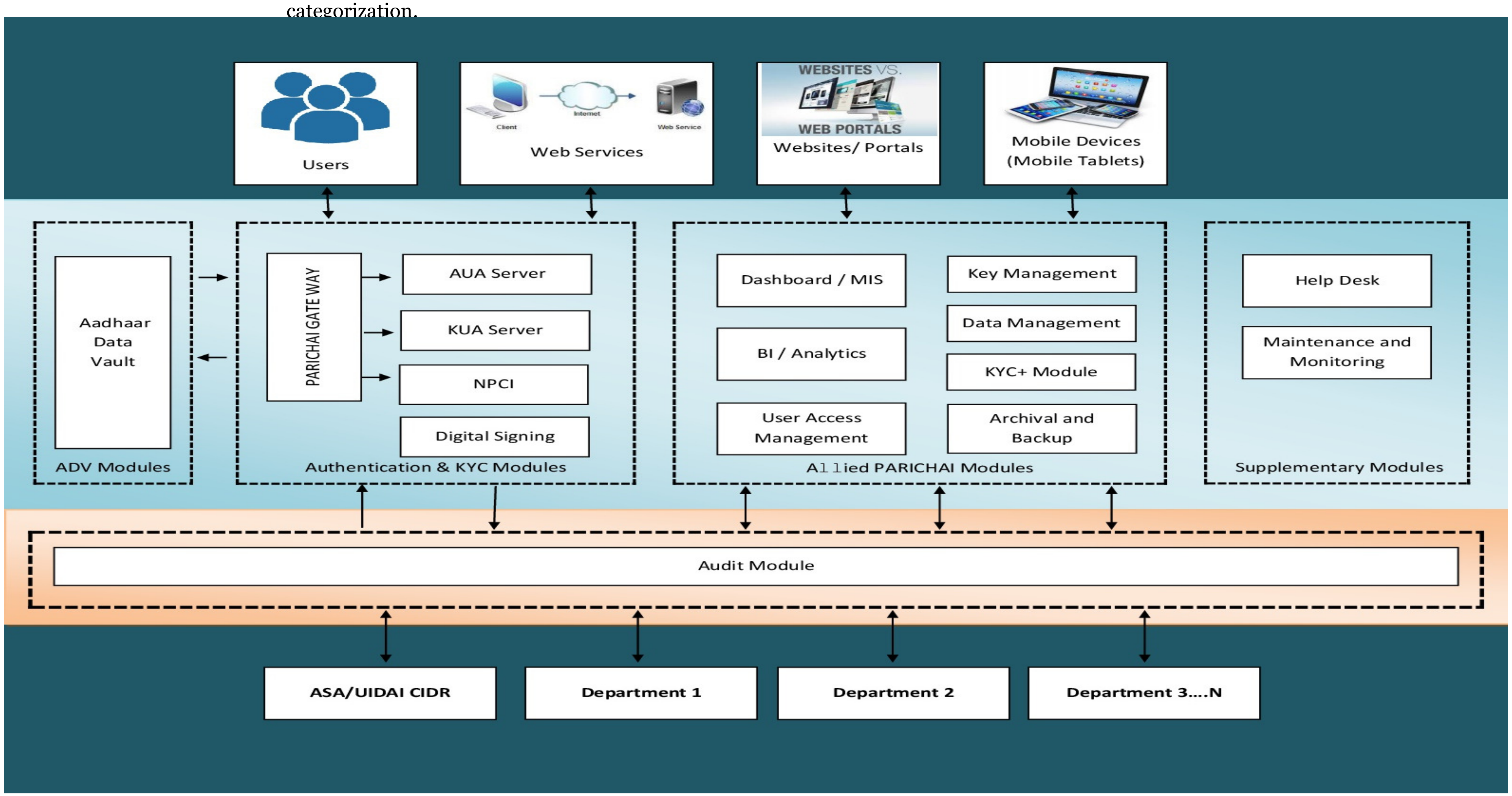
As a fundamental requirement of the PARICHAI application it is expected that the application shall be scalable in nature as that capable of delivering high-performance as and when the number of users and transactions increase up-to limit specified in this tender. The PARICHAI application would sustain the increased load by more number of modules being added in future. In this context, it is required that the application and deployment architecture should provide for scale-up and scale-out on the Application and Database Servers and all other solution components. Further, the application shall be modular in nature and would allow for secure wrapper services for accessing the available information via clearly defined RBAC (Role Based Access Control).

It is proposed that the software architecture of the PARICHAI application would be service oriented i.e. the architecture and solution components built upon it should be viewed as a set of independent services that can be composed to provide a solution. The SOA platform will help in data exchange within PARICHAI Services / modules in real-time mode, loose coupling with ease of maintenance and change, rapid composition of complex services, achieve scalability through modularity, and improved business visibility.

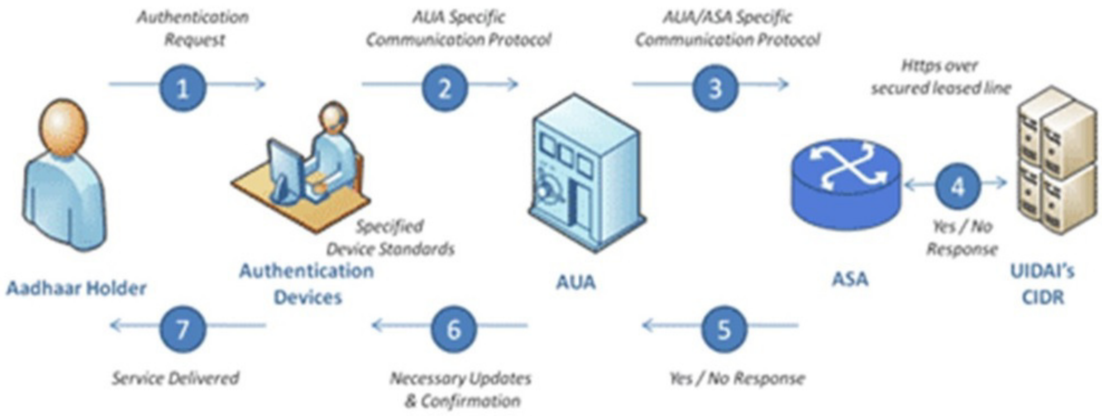
Business Intelligence and Analytics is also one of the key components of the PARICHAI solution and has been proposed to enable analysis of the aadhaar transactions for purpose such as fraud analytics etc., identifying hidden trends and create meaningful insights from it. This shall help the State Government in creating effective controls for the Schemes, develop new schemes, reach out to the intended beneficiary and assist in proactive service delivery. The trends developed shall be shared with the State Government Departments to enable them in taking information based decision.

Solution needs to be in high available without any single point of failure irrespective of hardware or software.

In this regard the functional architecture of the PARICHAI application has been prepared. The functional architecture is broadly segregated into three major types of modules. These modules relate to Authentication, eKYC, Management and Monitoring. The Diagram below presents the snapshot of various modules and its categorization.



Authentication and KYC Modules (Core Modules): These modules are proposed as core part of PARICHAI application, enable the system to provide Aadhaar Authentication and Aadhaar based electronic KYC. So as to provide these services to the State Government Departments, the MPSEDC needs to function as a live AUA and live KUA. The modules would work as a routing agent which shall check the validity of each authentication/eKYC request and route the requests in the Aadhaar ecosystem to Central Identities Data Repository (CIDR) through ASA/KSA. The response received from UIDAI shall be captured at PARICHAI and forwarded to respective State Government Department acting as a Sub-AUA.


Authentication Request
1
AUA Specific Communication Protocol
2
AUA/ASA Specific Communication Protocol
3
Https over secured leased line
4
Yes / No Response
Specified Device Standards
Aadhaar Holder
Authentication Devices
AUA
ASA
UIDAI's CIDR
7
Service Delivered
6
Necessary Updates & Confirmation
5
Yes / No Response

Aadhaar Authentication ecosystem

Aadhaar Data Vault Module: The Aadhaar Data Vault (ADV) module has to be created as per UIDAI circular सं .के– 2017 / 205 / 11020 –यूआईडीएआई) ऑथ (I-dated 25.07.2017. Existing reference keys in current Aadhaar data vault must be retained in created ADV, along with same logic for the creation of new reference keys. That is, any aadhaar number should create same reference key in every case.

Allied Modules: The allied PARICHAI modules have been proposed as part of the application to maintain, manage, view and analyse core authentication & eKYC modules of the solution. These application modules shall help MPSEDC and State Government Department users to manage the entire lifecycle of the PARICHAI solution. These modules shall help MPSEDC in provide KYC+ services, Management Dashboards and creation of BI / Analytical reports etc.

Supplementary Modules: These modules will help monitor PARICHAI solution with respect to change and event. And it will have HelpDesk ticketing software for addressing grievances of the departmental users.

1.1 Expected Transactions and user base:

Expected Transaction from key PARICHAI Modules (indicative in nature):

Module	Expected maximum transactions per hour*
Authentication	5,00,000
eKYC with ADV interaction (Internal)	3,00,000
Digital Signing (Encryption & Signing)	16,00,000
Encrypted Aadhaar to Reference key & vice-versa (External)	5,00,000

* SI has to demonstrate this much load handling capacity of the system for each module during user acceptance testing (prior to go-live), using simulators for all third party integration points. Simulators should be prepared by the SI's development team, and will be in scope of this tender.

Indicative User base (for the Departments)

Sl. No.	Module	Business Users	Power Users
1.	BI/Analytics Module	10	5
2.	Dashboard / MIS Module (PARICHAI Portal)	200	5
3.	Data Management Module	10	5
4.	KYC + Service	300	5
5.	Key Management	5	5
6.	Data Management	5	5
7.	HelpDesk	200	5
8.	Event Management	500	5

Sl. No.	Module	Business Users	Power Users
9.	Change Management	10	5

The subsequent sections elaborate on the functional requirement of the PARICHAI solution and are not exhaustive in nature. The System Integrator is expected to finalize the FRS during the implementation after the consultation with Stakeholders. The requirements have been categorized as 'Mandatory'/ 'Desirable'. All mandatory requirements need to be provided by the System Integrator as part of the solution. Non-compliance to any mandatory requirement shall not be considered and the bid shall be declared as Non-responsive. Non-responsive bids shall not be considered for further evaluation.

1.2 General Functional Requirements for PARICHAI Solution

#	Business/ Functional Requirement	Mandatory / Desirable
1.	The PARICHAI solution shall consist of multiple functionalities and all these functionalities should be seamlessly integrated with one another.	Mandatory
2.	All development work should have Software Development Life Cycle (SDLC) along with necessary tools for release management and Quality Assurance (QA).	Mandatory
3.	The solution should have the ability to handle transactions as per the work flow and limits defined in "Expected Transactions and user base" section.	Mandatory
4.	The PARICHAI Solution should be capable of sending **real-time** alerts/SMS/email to predefined designated officers in the event of crossing pre-defined conditions such as (not limited to) errors exceed threshold limit, service unavailability and any other conditions as specified by MPSEDC. Pre-defined conditions should be configurable through administrative GUI console.	Mandatory
5.	The PARICHAI solution should have user friendly screen and ease of use	Mandatory
6.	The solution should have the ability to download/upload information from/to user's laptop, desktop etc. or remote server. Offline synchronization is not required	Mandatory
7.	The solution should have the ability to support multiple windows and multi sessions	Mandatory

8.	Ability to dictate field's mandatory and/or optional status – prompting users for the required data	Mandatory
9.	Ability to display error messages, during data entry that clearly indicating the exact nature of the error and the field in the error and possible solutions.	Mandatory
10.	Indexing of key information fields is essential in order to facilitate searching.	Mandatory
11.	Ability to modify search results according to user specifications. This applies to search results producing windows/screens with large volumes of information – the user should be able to adjust tabular views to suit his/her requirements.	Mandatory
12.	Ability to generate reports • single report at a time • multiple reports at a time • ad hoc and regular reports at a time	Mandatory
13.	Ability to generate reports at • real time / on line basis • in background (when evaluation is time-consuming) • via batch processing • specific date • regular time interval • any other specific business condition	Mandatory
14.	Ability to have different levels of access for different roles and designations	Mandatory
15.	Ability to maintain audit trail of changes such as the time of change, the user ID, old and new value with field description	Mandatory
16.	Ability to support the following functions: • Portability • Interoperability • Scalability • High Performance • Serviceability • Manageability • Flexibility	Mandatory
17.	The system should be platform independent (accessible from mobile, laptop, desktop etc.)	Mandatory
18.	The system should also be browser independent	Mandatory

19.	The Web application accessible to the business user should be able to switch from English to Hindi and vice versa.	Mandatory
20.	The web based application should comply with Guidelines for Indian Government Websites (GIGW), W3C and WCAG2.0 Level A	Mandatory
21.	All the activities and transactions in the PARICHAI ecosystem should be logged	Mandatory
22.	Systime should be maintained and logged in the system as and wherever necessary	Mandatory
23.	The PARICHAI solution should be in compliance with UIDAI specifications and standards published by UIDAI / any legal entity / Government (GoI, GoMP) from time to time. **This being legal requirement and beyond control of MPSEDC, must be entertained by SI (irrespective of project phase) without any change request.**	Mandatory
24.	The application should have single window login. Any subsequent login attempts without a logout should fail.	Mandatory
25.	In case on inactivity from the logged user's terminal for certain duration, the system should automatically log out. The duration should be configurable.	Mandatory
26.	All sensitive data (such as passwords, aadhaar numbers etc.) shall have to be stored in encrypted format, and should travel over network in encrypted format only. The system should protect the integrity and authenticity of the data.	Mandatory
27.	The PARICHAI System should allow all alerts, notifications, exceptions, reports, issues, etc. to be displayed on GUI & Dashboard, sent through email and messages.	Mandatory
28.	System should have a help facility for each of the modules	Mandatory
29.	System should have transliteration capability or should be able to understand and operate on English, Hindi as well as vernacular languages as specified by UIDAI.	Mandatory
30.	The system should use proven transliteration capabilities from leading providers such as CDAC, Google, etc.	Desirable
31.	The system should be able to handle any font and any Indian language data in Unicode.	Mandatory
32.	The system should be built as a Services Oriented Architecture	Mandatory
33.	The system should have feasibility of integrating with any third party application (for example hand held device, mobile, application, app store application, web based application etc.) whenever required.	Mandatory
34.	Each module of PARICHAI solution should independently exist and can be integrated or replicated, which can be easily plugged in with other web-based / GUI application.	Mandatory
35.	The system should be able to expose the application as a Web Service for integrating with any third party application	Mandatory

36.	The system should have provision of Data masking.	Mandatory
37.	The system should have capability to conduct Two Way transliteration.	Mandatory
38.	The interface for all the Business Users and all the modules must be GUI based interface.	Mandatory
39.	The solution should also be created and installable as a mobile application in Android and iOS (latest version) devices.	Mandatory
40.	The PARICHAI solution should use same error codes as in existing system. However, error codes can further be added to it (if different to existing), compliant to same format / convention.	Mandatory
41.	PARICHAI solution's core modules should generate audit logs in every case which should be available in Audit module in GUI interface.	Mandatory
42.	The system should log transactions (may be on file-system) even during unavailability of database, and later reconcile / insert those logs (within 24 hours) in database once available.	Mandatory

1.3 PARICHAI Core Modules

Authentication and KYC Modules proposed as part of PARICHAI application collectively enable the system to provide Aadhaar Authentication; Aadhaar based electronic KYC services. Key Modules included as part of the Authentication & KYC are explained in this section.

1.3.1 Generic Requirement

Sl. No.	Business/ Functional Requirement	Mandatory / Desirable
43.	The SI should validate the request coming from Sub AUA, sign and encrypt the authentication request through digital signature certificate in High Availability mode	Mandatory
44.	All requests and responses along with authentication transaction logs should be logged in compliance with Aadhaar Act and UIDAI guidelines.	Mandatory
45.	All logs should be maintained for certain time period (ranging from 6 months to two years online, and up-to seven years including offline / archived data). The logs shall capture details of authentication transaction but not corresponding Personal Identity Information (PID).	Mandatory
46.	Auth and eKYC modules should be available in PARICHAI GUI console i.e. portal.	Mandatory
47.	The system should be able to receive the request in JavaScript Object Notation	Mandatory

	(JSON) from Sub AUA	
48.	The system should ensure that the received request from sub-AUA is compliant with the standards and specifications prescribed by UIDAI and complete	Mandatory
49.	The system should formulate and route request for ASA / UIDAI as per ASA's specification and UIDAI's released latest API. *Aadhaar number should not be captured during request flow.*	Mandatory
50.	System should have capability to integrate with multiple ASAs (min. 2, max. 5) in sequence as decided by MPSEDC. This sequence can be changed on-the-fly at PARICHAI's super-administrator (power user) GUI console, without requiring restart of the services.	Mandatory
51.	System should have capability to route requests to multiple ASAs through one-click available at PARICHAI's super-administrator (power user) GUI console, without requiring restart of the services.	Mandatory
52.	System should have feature to automatically switch to another ASA after a threshold count of errors reached, where this threshold should be configurable at PARICHAI's super-administrator (power user) GUI console, without requiring restart of the services. This should try ASAs in sequence.	Mandatory
53.	For the response that is received from ASA, should be forwarded to specific sub AUA from where the request originated	Mandatory
54.	The system should have capability to do multi-factor authentication as per authentication API.	Mandatory
55.	In case of PARICHAI portal, PID should be created at client level.	Mandatory
56.	The system should have error handling facility and alert mechanism once threshold of error reaches.	Mandatory
57.	Reporting of Auth and eKYC module shall be integrated with the Dashboard module	Mandatory

As per UIDAI recent norms, AUA and KUA terms have been made obsolete. Now, both are called "requesting entity". However, for legacy purpose this document uses word AUA for Auth and KUA for eKYC requests.

1.3.2 AUA Server

The Authentication Module shall be used by MPSEDC to provide various types of Aadhaar Authentication services to the sub-AUAs. During the authentication process the aadhaar number of the resident along with its other variable (such as finger print or name, address, etc.) that has been captured during the enrolment of the individual is sent to the UIDAI for authentication.

The Authentication module shall be responsible for handling various authentication requests being sent from Sub-AUAs i.e. the State Government Departments of Madhya Pradesh (or agencies identified by MPSEDC) to MPSEDC (as AUA). These requests shall be sent to CIDR through the ASA channel. A “Yes/No” response shall be provided back to the sub-AUAs.

The detailed functional requirements are mentioned below.

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
58.	The Auth XML should be sent to ASA and response JSON to sub-AUA, over the secured network	Mandatory
59.	The Aadhaar authentication should carry out the following Aadhaar Demographic Authentication The system should route all demographic authentication requests i.e. requests with an aim to authenticate resident’s details like Name, Address, Dob, etc. are authenticated from the UIDAI’s CIDR)	Mandatory
60.	The Aadhaar authentication should carry out the following Aadhaar Biometric Authentication • The system should route all biometric authentication requests from registered departmental applications (Sub-AUAs) to CIDR and back; • The system should implement Authentication API • The system should authenticate residents fingerprint, iris, face etc.	Mandatory
61.	The Aadhaar authentication should carry out the following Aadhaar OTP Authentication • The system should route all OTP authentication requests from registered departmental applications (Sub-AUAs) to CIDR and back • The system should implement OTP Authentication API • The system should authenticate residents with registered mobile numbers.	Mandatory
62.	The AUA server should also be able to conduct Buffered Authentication • At places of poor network connectivity, authentication request may be “buffered” (or queued) on the device until a configurable period of time (presently 24 hours) then sent to CIDR for authentication when connectivity is restored / available	Mandatory
63.	The system should handle Authentication API errors correctly.	Mandatory
64.	The system must ensure that explicit resident consent is received to authorize the PARICHAI solution to check the authenticity of the user, with proper disclosure information in local language being shown to resident. The system should store resident’s consent and disclosure information in all cases of authentication.	Mandatory

1.3.3 KUA Server

Verification of the Proof of Identity (PoI) and Proof of Address (PoA) is a key requirement for access various services including payment products, bank accounts, insurance products, telecom products, government services, LPG connections, etc. To avail such services, the residents today provide physical PoI and PoA documents. Hence, the e-KYC service provided by UIDAI through which the KYC process can be performed electronically with explicit authorization and consent by resident has been launched. As part of the e-KYC process, the resident authorizes UIDAI (through Aadhaar authentication using either biometric/OTP) to provide their demographic data along with their photograph (digitally signed and encrypted) to service providers. The real-time e-KYC service makes it possible for service providers to provide instant service delivery to residents, which otherwise would have taken a few days for activation based on the verification of KYC documents, digitization, etc.

The detailed functional requirements are mentioned below.

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
65.	The eKYC XML should be sent to ASA and response JSON to sub-AUA, over the secured network	Mandatory
66.	The response from CIDR has to be forwarded to the sub AUA after adding reference key (in case of success), generated from the Aadhaar Data Vault. Response to sub-AUA may include the complete eKYC information or partial as per classification of sub-AUA being Global or Local respectively.	Mandatory
67.	The system should decrypt the KYC details provided by CIDR and shall forward the KYC details including his name, address, photograph, DoB, etc. to the Government department in a secured manner.	Mandatory
68.	The system must ensure that explicit resident consent is received to authorize the PARICHAI solution to retrieve the resident data, with proper disclosure information in local language being shown to resident. The system should store resident’s consent and disclosure information in all cases of eKYC.	Mandatory

1.3.4 Audit Module

As part of the UIDAI Security Guidelines it is essential to maintain the audit logs in the PARICHAI application. The Audit Module would not only store the Transactional logs of the authentication, and eKYC transactions but shall also store audit logs relating to creation, access and updation of data in the PARICHAI data repository. Further, the module shall also support in storing of information which shall help the reporting modules create compliance reports required by State Government, UIDAI or ASA/KSA.

The detailed functional requirements are mentioned below.

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
69.	The system shall maintain audit logs for all authentication, e-KYC, BFD related transactions by capturing Desirable details of the transaction including last 4 digits of Aadhaar number (or as allowed as per UIDAI guidelines), date, time, IP, Sub-AUA code, Key, etc. Audit logs for at least 6 months shall be maintained as per the guidelines of UIDAI.	Mandatory
70.	The system should have graphical user interface (GUI console) to view these audit logs.	Mandatory
71.	The system should also ensure to log any data updation, creation, access, etc. which takes place on the meta-data repository / any other administrative controlled parameter. The module shall be used by the MPSEDC or Government Departments to track the changes in the data and the requestor/approval details.	Mandatory
72.	The module should also ensure storage of any such data /logs which shall be required by State Government, UIDAI and KSA/ASA. These logs shall support in creation of the compliance reports required by audit agencies.	Mandatory

1.3.5 Digital Signing and Security Module

Digital signing module in the PARICHAI shall be used to perform two primary functions i.e. to decrypt the eKYC packets that shall be received from the CIDR, Digitally sign each Authentication which are forwarded to CIDR. The detailed functional requirements are mentioned below.

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
73.	The system shall use this module for decrypting the packet received from UIDAI through MPSEDC's private key.	Mandatory
74.	The AUA / KUA server should digitally sign all the auth and eKYC requests towards CIDR, and forward those to CIDR. The modules shall be used for large scale signing of auth and eKYC requests, programmatically.	Mandatory
75.	The module should support in establishing SSL connection between the communication systems.	Mandatory
76.	The SI should coordinate with the HSM vendor / OEM for any HSM related issues.	Mandatory

1.3.6 PARICHAI Gateway

PARICHAI gateway is a bridge between AUA and sub-AUA for aadhaar authentication / eKYC services. This module is similar to payment gateway. In this module sub-AUA post some predefined parameters values and redirect to PARICHAI module. It will fetch eKYC / authenticate user based on request forwarded to UIDAI & send response to sub-AUA as options selected in module and on basis of classification of sub-AUA.

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
77.	The system should comply with UIDAI circulars & guidelines issued time to time.	Mandatory
78.	The system should take parameters like license key, sub-AUA code, aadhaar number, consent, disclosure info etc. in request.	Mandatory
79.	The system should send response to respective sub-AUA as per sub-AUA's classification and option selected in PARICHAI gateway module.	Mandatory
80.	The system should have capability to send and display complete eKYC and limited eKYC both, as per the case / classification of sub-AUA.	Mandatory
81.	The system should have option to select, out of displayed values, which value should be further forwarded to sub-AUA's application / system (external to PARICHAI solution).	Mandatory
82.	The system should flow all data in network over secured socket layer. For case of aadhaar number, additional encryption should be there in compliance with the UIDAI guidelines.	Mandatory
83.	The system should generate PID at client level for all non-biometric / demographic authentications (like OTP based etc.).	Mandatory
84.	The system should integrate with UIDAI-listed registered biometric devices (fingerprint, IRIS, face-recognition etc.). Devices shall be provided by MPSEDC. However, all technical coordination with the device vendor has to be done by SI.	Mandatory
85.	The system should be platform independent and work for all browsers.	Mandatory
86.	The system should support English, Hindi / state's regional language.	Mandatory
87.	The system should support multi-factor authentication as per UIDAI's aadhaar authentication / eKYC API and PARICHAI's API.	Mandatory
88.	The system should add reference key (in case of success), in response forwarded to the sub AUA after generated from the Aadhaar Data Vault.	Mandatory
89.	The system should generate transaction and audit logs which should be seamlessly integrated with the PARICHAI solution's audit module.	Mandatory

1.3.7 Aadhaar Data Vault Module

Aadhaar Data Vault is "single, secured and centralized" database system which is isolated from solution's any other database, and created as per UIDAI circular सं .के – 2017 / 205 / 11020 – यूआईडीएआई) ऑथ (I-dated 25.07.2017. It is applicable only for Global AUA, which MPSEDC is.

ADV will only have aadhaar number and a unique reference key generated against each aadhaar in such manner that actual aadhaar number could never be derived from its reference key. Aadhaar number in ADV is stored only after encrypting from the keys placed in highly secure hardware security module (HSM) devices.

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
90.	The system should be compliant as per UIDAI circular सं. के– 11020 / 205 / 2017 – यूआईडीएआई (ऑथ-I) dated 25.07.2017; and any other future guidelines (whenever issued). Any change in ADV to accommodate it as per future guidelines should be done without any additional change request, as it is legal binding and beyond control of MPSEDC.	Mandatory
91.	The system should store encrypted aadhaar number by hardware security module (HSM) in secured and isolated environment.	Mandatory
92.	The system should only be accessed by APIs.	Mandatory
93.	Existing reference keys in current Aadhaar data vault must be retained in created ADV, along with same logic for the creation of new reference keys. That is, any aadhaar number should create same reference key in every case.	Mandatory
94.	The system should generate unique reference key for each aadhaar number, by which aadhaar number never be derived.	Mandatory
95.	For aadhaar-reference key pair generated, the system should have web service API to return aadhaar number which exists within this MPSEDC's ADV, only after interaction with Hardware Security Module (HSM). This service will be used for cases where request comes from MPSEDC's sub-AUA only, and should be in compliance with UIDAI guidelines.	Mandatory
96.	The system should have insert, delete and update APIs for interaction with ADV.	Mandatory
97.	The system should log each request in compliance with UIDAI guidelines.	Mandatory
98.	The system should be capable of fetching statistical reports (as and when required) from the logs.	Mandatory
99.	The system's APIs should interact with auth, eKYC, PARICHAI gateway request or	Mandatory

	any other core modules of PARICHAI solution.	
100.	The system should generate statistical reports for transactions dept-wise, day-wise, month wise or any other custom periodicity.	Mandatory
101.	The system should have web service API with distinct reference key count as output.	Mandatory
102.	In all cases, aadhaar number should flow over network in encrypted format.	Mandatory
103.	The system should have capability to generate one-way hash.	Mandatory

1.3.8 NPCI Module

National Payments Corporation of India (NPCI) has provided MPSEDC a web service to check whether an aadhaar number is linked with the bank account, for utilizing Aadhaar enabled payment system (AEPS). AEPS is a bank led model which allows online interoperable financial transaction at PoS (Point of Sale / Micro ATM) through the Business Correspondent (BC)/Bank Mitra of any bank using the Aadhaar authentication. NPCI module of PARICHAI solution should leverage these web services provided by NPCI.

Sl. No.	Business/ Functional Requirement	Mandatory / Desirable
104.	The system should call NPCI web services (whenever invoked by user either through web service or PARICHAI portal – GUI based) and return input aadhaar number's bank linkage status, as provided by NPCI.	Mandatory
105.	The system should store transfer data over network via secured socket layer (SSL).	Mandatory
106.	The system should generate unique transaction ids for each transaction, and log key input and output parameters of each request , as per required by MPSEDC.	Mandatory
107.	The system should have defined error codes and exception handling capabilities.	Mandatory
108.	The system should be capable of fetching statistical reports (as and when required) from the logs.	Mandatory
109.	The system's APIs should interact with other core modules of PARICHAI solution.	Mandatory
110.	The system should generate statistical reports for transactions dept-wise, day-wise, month wise or any other custom periodicity.	Mandatory
111.	The system should have capability to send request to alternate NPCI URL on-the-fly, if any one of the request URL is down for a particular duration / threshold failure.	Mandatory

1.4 PARICHAI Allied Modules

1.4.1 Generic Requirement

Sl. No.	Functional/ Business Requirement	Mandatory / Desirable
112.	The application should have capabilities to provide workflow based on the department's requirement	Mandatory
113.	The application should also have ability to display the reports in various graphical formats which can be exported / printed in readable excel and pdf format.	Mandatory
114.	System should allow the user to schedule the activities and maintain the calendar with reminders.	Mandatory
115.	System should allow configuration of rules for seamless automation of process and the data flow across the Modules.	Mandatory

1.4.2 Dashboard / MIS Module

Dashboard Module in PARICHAI would have the ability to display information in an intuitive format and conduct meaningful analysis of the data. Dashboards would be typically used by Department officials and MPSEDC Senior Management. These dashboards shall display trends, patterns, exceptions affecting using visual tools such as graphs, charts etc.

The dashboards shall be easy-to-use, easily personalize-able and can alert decision maker when business metrics approach and exceed accepted ranges and targets. Dashboards may also provide basic controls that can alter the view of the data.

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
116.	The system should consolidate data from multiple sources into useful and interactive views.	Mandatory
117.	System should be able to present reports in customizable figures, charts and graphs of different formats.	Mandatory
118.	System should allow users to drill, aggregate, and filter departmental data directly on a dashboard.	Mandatory
119.	The systems should allow users to see information filtered and personalized based on logged user's identity, function or role - based on predefined rules.	Mandatory

120.	System should be able to provide the key decision makers with visibility into critical KPIs across the organization on a single screen. The system should also allow drilldown of dashboard and KPI.	Mandatory
121.	The system should be able to provide KPI level consolidation and analysis based on various parameters.	Mandatory
122.	The system should provide Enterprise Reporting and shall be used to generate operational reports in pre-designed structured formats that focus on listings of data at the detailed level.	Mandatory
123.	The system should permit the user to set the refresh interval for his/her dashboard and/or its components	Mandatory
124.	At any time, the system should allow the end user to save any output as pdf, excel, csv, flat file etc.	Mandatory
125.	The tool should provide Geographical map views to provide a quick understanding of geospatial data.	Desirable
126.	The solution should have the features such as Reporting, Analysis, Dashboard etc.	Mandatory
127.	The system should be able to access and consolidate data from all the source systems available in PARICHAI, for meaningful analysis which can help in Decision Support.	Mandatory
128.	The system should allow save / download reports in offline mode which can be easily shared and viewed later, independent of PARICHAI connectivity.	Mandatory
129.	The solution should provide a web based interface so as to allow access from anywhere using any browser. The access should be based upon user-id and password	Mandatory
130.	The system should provide mobile application which should be installable in Android and iOS (latest version) devices.	Mandatory

1.4.3 BI / Analytics Module

The BI and Analytics module has been proposed as part of PARICHAI to carryout various analyses for the MPSEDC and State Government Departments. The module shall enable MPSEDC in modelling the data in multiple dimensions to derive hidden insight, trends, patterns, anomalies, etc. from data sets received from multiple source systems. This module shall analyze large quantities of data (in TBs) to extract unknown interesting patterns and use those identified patterns to create trends which are of interest to the State Government Departments. Key Functionality of this module is mentioned below:-

Ad-hoc query module shall enable the users to rapidly generate business queries and reports from the data repository based upon the requirements. This module shall support ad-hoc querying, through intuitive, graphical interfaces that shields users from technical complexities and allows users to leverage business terminology instead of the more technical database names.

Sl. No.	Business/ Functional Requirement	Mandatory / Desirable
131.	The system should allow creation of ad-hoc queries to generate reports.	Mandatory
132.	System should have capability to store such ad-hoc queries, which can be later called to fetch the data based on same requirement, or be modified slightly to fetch similar set of data.	Mandatory
133.	The solution should have the capability to combine multiple sources of information into one report.	Mandatory
134.	System should have sophisticated data search capability to identify a hidden trend/pattern across multiple source systems	Mandatory
135.	The system should be carry out category based analysis of the data	Mandatory
136.	The system should be able to store data in location hierarchy wise (for example, location data for State may be broken down into district. This district data must be stored block wise and block wise and block data may be stored village wise). All such data must be aggregated based on geography.	Mandatory
137.	The system should have facility to generate Billing report (monthly / quarterly basis) based on type of transactions and cost per unit: • for sub-AUAs, and • for ASAs / UIDAI separately.	Mandatory

1.4.4 User Access Management

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
138.	The system must allow the user to create / update / delete user and user profile.	Mandatory
139.	The System must allow the user to limit access to cases / specified users or user groups.	Mandatory
140.	The system should provide for role-based control for the functionality within the system.	Mandatory
141.	The System must allow a user to be a member of more than one group.	Mandatory
142.	The System must allow only admin-users to set up user profiles and allocate users	Mandatory

	to groups.	
143.	The System must allow changes to security attributes for groups or users (such as access rights, security level, privileges, password allocation and management) to be made only by super-user.	Mandatory
144.	System should allow the user to access only those functionalities that he/she is authorized to access.	Mandatory
145.	System should allow a maximum of three attempts to login. This should be followed by a period of non-access.	Mandatory
146.	System should allow the user to regenerate a lost password/reset password with set of hint questions	Mandatory
147.	The system should enforce the strong password policy as decided by MPSEDC	Mandatory
148.	System should store passwords in encrypted format in the database	Mandatory
149.	System should allow creation of new users, transfer of postings for existing users and any other actions that affect their authentication and authorization settings.	Mandatory
150.	System should allow changes in roles/ authorization with the transfer / promotions	Mandatory
151.	System should have super-admin module for MPSEDC only, which can perform power user activities such as department on-boarding and management, rule configuration, license key management, PARICHAI gateway management, audit trail, login as user, user and role creation and modification etc.	Mandatory

1.4.5 Key Management

This module will store all type of keys being in use in PARICHAI solution such as internal generated sub-AUA license keys, UIDAI generated AUA license keys, device keys, Digital Signature (DSC) encryption keys etc.

Sl. No.	Business/ Functional Requirement	Mandatory / Desirable
152.	The solution should be able to manage all type of keys for all the required internal and third party applications.	Mandatory
153.	The solution should manage keys as per Key Management Interoperability Protocol (KMIP) protocol.	Mandatory
154.	The solution should have graphical (GUI) console for the management / administrative operations.	Mandatory
155.	The solution should have option to designate different authorized user for	Mandatory

	different keys.	
156.	The solution should have option to trigger email having new keys. This should be configurable to auto or manual.	Mandatory
157.	The solution should have mechanism to automatic alert via email and / or sms on any change action related to keys (such as key change, authorized user change etc.)	Mandatory
158.	The solution should have mechanism to automatic alert via email and / or sms before pre-defined days from date of key expiry.	Mandatory
159.	The solution should have mechanism to automatic alert via email and /or sms on any event as defined by MPSEDC	Mandatory
160.	The solution should have "key management store" which should contain all old and new keys, along with key related attributes like date of key change and type of key etc.	Mandatory
161.	For internal applications (within PARICHAI solution), keys should synchronize automatically across all required modules / application without any downtime, whenever same gets changed in key management store.	Mandatory
162.	The solution should have audit trail to record all actions pertaining to keys along with systime of change and user who performed the change, IP address of machine from where user logged in etc. These audit trails should be accessible to administrator (power user) profile only, through their GUI console.	Mandatory
163.	The solution should have business user with view rights only to part of key as decided by MPSEDC, in general case.	Mandatory

1.4.6 Data Management

Data Management shall enable database and meta-data management. Key functionalities for Data Management are provided in the table below:

#	Business/ Functional Requirement	Mandatory/ Desirable
164.	System should be integrated with other service delivery modules included eKYC, Authentication etc.	Mandatory
165.	System should be able to store data as per Relational Database Management (RDBMS) principle. However, for supplementary data which do not have direct impact on service level agreements and service availability, system may have provision for non-RDBMS.	Mandatory

#	Business/ Functional Requirement	Mandatory/ Desirable
166.	All non-RDBMS / open source systems' built in the system should have support and maintenance from recognized entity (not open forums).	Mandatory
167.	All meta-data should be maintained and duly updated, as and when required.	Mandatory
168.	All supplementary data should be maintained and duly updated, as and when required. Following data (not limited to) can be treated as supplementary data: 1. Contact details of user departments / third party vendors etc. 2. Application documents like APIs, release notes etc. 3. Project Documents like SRS, FRS, DFD etc. 4. Infrastructure documents like Architecture, Network diagram etc. 5. Backup related documents 6. Trouble reports, Root cause analysis reports etc. 7. Adhoc reports etc. 8. Any other documents as specified by MPSEDC	Mandatory
169.	The system should have GUI console to manage supplementary data (both document and records).	Mandatory
170.	System should have the capability of creating roles based rules to update / populate and view data.	Mandatory

1.4.7 KYC+ Module

This module will store KYC+ data only which is consented and allowed as per law. This data may be used for efficient planning of the schemes by the government.

Sl. No.	Business/ Functional Requirement	Mandatory / Desirable
171.	System should have provision to integrate and collate data from various data entry modules of PARICHAI solution like Auth, eKYC, gateway etc.	Mandatory
172.	System should have capability to uniquely identify record based on allowed common identifier and group together. Grouped data should have source and timestamp from source clearly evident.	Mandatory
173.	System should have provision to collate data either real-time or through scheduled mechanism.	Mandatory
174.	System should have view provision (page-wise, where page-size can be configured)	Mandatory

	through GUI console.	
175.	System should have search option using various fields as decided by MPSEDC.	Mandatory
176.	System should have provision to select source system (individual or all) and whether real-time required or schedule, with single or multiple inputs. This feature should be available through GUI console.	Mandatory
177.	System should store data in encrypted format, with encryption keys stored separately.	Mandatory
178.	System should generate statistical reports for the data within module.	Mandatory

1.4.8 Archival and Backup Module

Solution should have mechanism to periodically archive and backup different types of data generated, as per policy decided by MPSEDC. This module should have following functionalities.

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
179.	System should have provision to integrate and collate data from all modules of the solution, as per frequency decided by MPSEDC.	Mandatory
180.	System should have provision to periodically archive data online (in filesystem storage, not backup tapes), automatically as per configuration.	Mandatory
181.	System should have provision to periodically archive data online in backup tapes), automatically as per configuration.	Mandatory
182.	System should have graphical console to change backup and archival configuration, see status of ongoing backup processes and completed processes, with details such as location of data storage, type of data, source whose data backed up, time of backup etc.	Mandatory
183.	System should have view provision (page-wise, where page-size can be configured) through GUI console.	Mandatory
184.	System should have search option using various fields as decided by MPSEDC.	Mandatory
185.	System should have provision to select source system (individual or all) and whether real-time required or schedule, with single or multiple inputs. This feature should be available through GUI console.	Mandatory
186.	System should have provision to restore data to original location, on single click in graphical console.	Mandatory
187.	System should have capacity to take backup from various source type like database, filesystem etc.	Mandatory

	All required licenses (if any) should be brought by SI from Day one.	
188.	System should store data in encrypted format, with encryption keys stored separately.	Mandatory
189.	System should generate statistical reports for the data within module.	Mandatory

1.5 Supplementary Modules

1.5.1 HelpDesk Software

Helpdesk system would automatically generate the incident tickets and log the call. Such calls are forwarded to the desired system support personnel deputed by the SI. These personnel would look into the problem, diagnose and isolate such faults and resolve the issues timely. The helpdesk system would be having necessary workflow for transparent, smoother and cordial PARICHAI support framework.

The SI must bring adequate license for help desk or can bring other Help desk system which shall meet the below mentioned requirements. For the Helpdesk System, **the bidder should support at least 5 concurrent members' users at the same time.**

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
190.	The Helpdesk system should provide flexibility of logging incident manually via GUI / web interface	Mandatory
191.	The HelpDesk system should be publicly accessible for departmental users to login and register grievance. Adequate licenses (if required) should be supplied from Day one. (At least 400 users)	Mandatory
192.	The HelpDesk tool and team (sitting at MPSEDC) should be adequately provisioned to handle users as in above point.	Mandatory
193.	The Helpdesk system should have role based access having (not limited to): 1. Administrator – to configure Tool, create users, role etc. 2. Ticket Raiser* – to raise tickets, who can see / track a. only tickets raised by himself (Dept User), or b. all tickets raised by his Dept. Users (Dept. Admin) * He/She must not be able to see: o other departmental tickets o internal / technical communication on the ticket i.e. He should only see what HelpDesk member replies.	Mandatory

	3. HelpDesk – to view, assign and close tickets 4. Support (L1, L2 etc.) – to view tickets assigned to them by HelpDesk and respond suitably (i.e. escalate to higher level or close and respond to HelpDesk)	
194.	The HelpDesk system should have group based access where users of same nature can be clubbed into single group. Groups like (not limited to): 1. L1 support, L2 support etc. 2. Dept1, Dept2 etc. 3. Internal (Onsite SI's Team), Internal PMU etc.	Mandatory
195.	The web interface console of the incident tracking system would allow viewing, updating and closing of incident tickets.	Mandatory
196.	The trouble-ticket should be generated for each complaint and given to asset owner immediately through email.	Mandatory
197.	Helpdesk system should allow detailed multiple levels/tiers of categorization on the type of incident being logged.	Mandatory
198.	It should provide classification to differentiate the criticality of the incident via the priority levels, severity levels and impact levels.	Mandatory
199.	It should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location	Mandatory
200.	It should allow the helpdesk administrator to define escalation policy, with multiple levels & notification, through easy to use GUI / console.	Mandatory
201.	System should provide a knowledge base to store history of useful incident resolution	Mandatory
202.	It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.	Mandatory
203.	The web-based FAQs/ Help would allow users to access his /her knowledge article for quick references.	Mandatory
204.	Allow categorization on the type of incident being logged	Mandatory
205.	Provide audit logs and reports to track the updating of each incident ticket	Mandatory
206.	Proposed system should be ITIL compliant and should have all the components as per required in the ITIL principle / philosophy (such as change management, event management, incident management etc.).	Mandatory
207.	It should be possible to do any customizations or policy updates in flash with zero or very minimal coding or down time	Mandatory
208.	It should be able to log and escalate user interactions and requests.	Mandatory

209.	It should provide functionality to add / remove a knowledge base solution based on prior approval from the concerned authorities	Mandatory
210.	It should be capable of assigning call requests to technical staff manually based on predefined rules, and should support notification and escalation over email, web etc.	Mandatory
211.	It should provide status of registered calls to end-users over email	Mandatory
212.	The solution should provide web based administration so that the same can be performed from anywhere	Mandatory
213.	It should have a customized Management Dashboard for senior executives with live reports from helpdesk database	Mandatory
214.	It should be possible to highlight requests based on probability of violation of SLAs.	Mandatory
215.	It should support tracking of SLA (service level agreements) for call requests within the help desk	Mandatory
216.	It should maintain the SLA for each ticket. The system should be able to generate report on the SLA violation or regular SLA compliance levels.	Mandatory

1.5.2 Maintenance and Monitoring Software

The solution should provide the comprehensive capability for management, maintenance and monitoring of all the overall PARICHAI solution (including all components and sub-components) for this project. The bidder is required to provide necessary hardware and sufficient licenses to meet such requirement.

The SLA Monitoring function of the solution is an important requirement of this Project. Equally important from the point of the SI is that the payments by MPSEDC on account of the performance are linked to a measurement of the of SLA parameters. In this context the SLA Monitoring component of solution will have to possess the capabilities mentioned in the below mentioned table.

The SI should bring necessary tools and licenses shall to meet the below mentioned requirements.

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
Basic Requirements		
217.	Solution should be inclusive with hardware, OS, patches, etc.	Mandatory

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
218.	Solution should provide for future scalability of the whole system without major architectural changes.	Mandatory
219.	Should be SNMP v1, v2, v3 and MIB-II compliant.	Mandatory
220.	Filtering of events should be possible, with advance sort option based on components, type of message, time etc.	Mandatory
221.	Should support Web / Administration Interface.	Mandatory
222.	Should provide compatibility to standard RDBMS.	Mandatory
223.	Solution should be open, distributed, and scalable and open to third party integration.	Mandatory
224.	Should provide fault and performance management for multivendor TCP/IP networks.	Mandatory
Access and User Management		
225.	Should be able to provide secured windows based consoles / secured web-based consoles for accessibility to software.	Mandatory
226.	Should have web browser interface with user name and Password Authentication.	Mandatory
227.	Administrator/ Manager should have privilege to create/modify/delete user	Mandatory
228.	Should provide an integrated performance view for all the managed systems along with the various threshold violations alarms in them. It should be possible to drill-down into the performance view to execute context specific reports	Mandatory
229.	Should provide the following reports for troubleshooting, diagnosis, analysis and resolution purposes: Trend Reports, At-A-Glance Reports, & capacity prediction reports	Mandatory
230.	Should be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits	Mandatory

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
Polling Cycle		
231.	Support discriminated polling	Mandatory
232.	Should be able to update device configuration changes such as re-indexing of ports	Mandatory
Fault Management		
233.	Should be able to get fault information in real time and present the same in alarm window with description, affected component, time stamp etc.	Mandatory
234.	Should be able to get fault information from heterogeneousdevices — storage, switches, servers etc.	Mandatory
235.	Event related to servers should go to a common enterprise eventconsole where a set of automated tasks can be defined based onthe policy.	Mandatory
236.	Should have ability to correlate events across the entirecomponents of solution.	Mandatory
237.	Should support automatic event correlation in order to reduceevents occurring in solution.	Mandatory
238.	Should support advanced filtering to eliminate extraneous data /alarms in Web browser and GUI.	Mandatory
239.	Should be configurable to suppress events for key systems/devices that are down for routine maintenance or planned outage.	Mandatory
240.	Should be able to monitor on user-defined thresholds for warning/ critical states and escalate events to event console of enterprise management system.	Mandatory
241.	Should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis.	Mandatory
242.	Should have self-certification capabilities so that it can easily add support for new traps and automatically generate alarms.	Mandatory
243.	Should provide sufficient reports pertaining to asset and change management, alarms and availability of critical network resources as well as network response times for critical links.	Mandatory
244.	The tool shall integrate storage, server and database performance / event information and alarms in a single console and provide a unified event view/reporting interface for network and system components. The current	Mandatory

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
	status/performance state of the entire network and system infrastructure shall be visible in an integrated console	
245.	Should provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them. It should be possible to drill-down into the performance view to execute context specific reports	Mandatory
246.	Should provide the following reports for troubleshooting, diagnosis, analysis and resolution purposes: Trend Reports, At-A-Glance Reports, & capacity prediction reports	Mandatory
247.	Should be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to setcorresponding upper and lower threshold limits	Mandatory
248.	Manual discovery can be done for identified network segment, single or multiple devices	Mandatory
Presentation		
249.	Should be able to discover links with proper colour status propagation for complete network visualization.	Mandatory
250.	Should support dynamic object collections and auto discovery. The topology of the entire Network should be available in a single map.	Mandatory
251.	Should give user option to create his /or her map based on certain group of devices or region.	Mandatory
Agents		
252.	Should monitor various operating system parameters such as processors, memory, files, processes, file systems etc. where applicable using agents on the servers to be monitored.	Mandatory
253.	Provide performance threshold configuration for all the agents to be done from a central GUI based console that provide a common look and feel across various platforms in the enterprise. These agents could then dynamically reconfigure them to use these threshold profiles they receive	Mandatory
System Monitoring		
254.	Should be able to monitor/ manage large heterogeneous systems environment continuously	Mandatory

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
255.	For windows server, should be able to monitor and manage Event log monitoring, Virtual and physical memory statistics, Paging and swap statistics, Operating system, Memory, Logical disk, Physical disk, Process, Processor, Paging file, IP statistics, ICMP statistics, Network interface traffic, Cache, Active Directory Services	Mandatory
256.	Should be capable of view/start/stop the services on windows servers	Mandatory
257.	For Unix / Linux server, should be able to monitor the statistics CPU Utilization, CPU Load Averages, System virtual memory (includes swapping and paging), Disk Usage, No. of Inodes in each file system, Network interface traffic, Critical System log integration	Mandatory
Infrastructure Services		
258.	IIS / Tomcat / Apache / Web server statistics, HTTP service, HTTPS service, FTP server statistics, POP/ SMTP Services, ICMP services, Database Services – Monitor various critical relational databasemanagement system (RDBMS) parameters such as databasetables / table spaces, logs etc.	Mandatory
Application Performance Management		
259.	End to end Management of applications (J2EE/.NET based)	Mandatory
260.	Determination of the root cause of performance issues whether inside the Java application in connected back-end systems or at the network layer	Mandatory
261.	Automatic discovery and monitoring of the web application environment	Mandatory
262.	Ability to monitor applications with a dashboard	Mandatory
263.	Ability to expose performance of individual SQL statements within problem transactions	Mandatory
264.	Monitoring of third-party applications without any source code change requirements	Mandatory
265.	Proactive monitoring of all end user transactions; detecting failed transactions; gathering evidence necessary for problem diagnose	Mandatory
266.	Storage of historical data is for problem diagnosis, trend analysis etc	Mandatory

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
267.	Monitoring of application performance based on transaction type	Mandatory
268.	Ability to identify the potential cause of memory leaks	Mandatory
Reporting		
269.	Should able to generate reports on predefined / customized hours	Mandatory
270.	Should be able to present the reports through web and also generate PDF / CSV / reports of the same.	Mandatory
271.	Should provide user flexibility to create his /or her custom reports on the basis of time duration, group of elements, custom elements etc.	Mandatory
272.	Should provide information regarding interface utilization and error statistics for physical and logical links.	Mandatory
273.	Should create historical performance and trend analysis for capacity planning	Mandatory
274.	Should be capable to send the reports through e-mail to predefined user with pre-defined interval.	Mandatory
275.	Should have capability to exclude the planned-downtimes or downtime outside SLA	Mandatory
276.	Should be able to generate all sorts of SLA Reports	Mandatory
277.	Should be able to generate web-based reports, historical data for the systems and network devices and Near Real Time reports on the local management console.	Mandatory
278.	Should be able to generate the reports for Server, Application, infrastructure services and other items in Data Center environment	Mandatory
279.	The Reporting and Analysis tool should provide a ready-to-use view into the wealth of data gathered by Management system and service management tools. It should consolidate data from all the relevant modules and transform it into easily accessible business-relevant information. This information, should be presented in a variety of graphical formats can be viewed interactively	Mandatory
280.	The tool should allow customers to explore the real-time data in avariety of methods and patterns and then produce reports toanalyze the associated business and service affecting issues	Mandatory

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
281.	The presentation of reports should be in an easy to analyzegraphical form enabling the administrator to put up easilysummarized reports to the management for quick action(Customizable Reports). The software should be capable ofsupporting the needs to custom make some of the reports as perthe needs of the organization.	Mandatory
282.	The software should be able to provide a time snapshot of the required information as well as the period analysis of the same in order to help in projecting the demand for bandwidth in the future.	Mandatory
Availability Reports		
283.	Availability and Uptime – Daily, Weekly, Monthly and Yearly Basis	Mandatory
284.	Trend Report	Mandatory
285.	Other various types of reports such as Maximum Time To Repair, Mean Time To Repair reports , Mean Time Between Failures (MTBF) etc.	Mandatory
Performance Reports		
286.	Device Performance – CPU and Memory utilized	Mandatory
287.	Interface errors	Mandatory
288.	Server and Infrastructure service statistics	Mandatory
289.	Trend report based on Historical Information	Mandatory
290.	Forecasting report based on Trend Report	
291.	Custom report	Mandatory
292.	SLA Reporting	Mandatory
293.	Computation of SLA for entire solution	Mandatory

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
294.	Automated Daily, Weekly, Monthly, Quarterly and Yearly SLA Reports	Mandatory
Data Collection		
295.	For reporting, required RDBMS to be provided with all licenses	Mandatory
296.	Should have sufficient Storage capacity should to support all reporting data for 5 years of operations.	Mandatory
Integration		
297.	Should be able to receive and process SNMP traps from infrastructure components such as router, switch, servers etc.	Mandatory
298.	Should be able integrate with Helpdesk system for incidents	Mandatory
299.	Should be able to send e-mail or Mobile –SMS to pre-defined users for pre-defined faults.	Mandatory
300.	Should trigger automated actions based on incoming events / traps. These actions can be automated scripts/batch files	Mandatory
Miscellaneous		
301.	The Systems and Distributed Monitoring (Operating Systems) of solution should be able to monitor: Each processor in the system should be monitored for CPU utilization. Current utilization should be compared against user-specified warning and critical thresholds	Mandatory
302.	The Systems and Distributed Monitoring (Operating Systems) of solution should be able to monitor: Each file system should be monitored for the amount of file system space used, which is compared to user-defined warning and critical thresholds	Mandatory
303.	The Systems and Distributed Monitoring (Operating Systems) of solution should be able to monitor: Logs should be monitored to detectfaults in the operating system, the communication subsystem and in applications. The function should also analyze the files residing on the host for specified string patterns.	Mandatory
304.	The Systems and Distributed Monitoring (Operating Systems) of solution should be able to monitor: The System Management function should provide real-time collection of data from all system processes. This should identify whether or not an important process has stopped unexpectedly.	Mandatory

Sl. No.	Business/ Functional Requirement	Mandatory/ Desirable
	Critical processes should be automatically restarted using the System Management function.	
305.	The Systems and Distributed Monitoring (Operating Systems) of solution should be able to monitor: The System Management function should monitor memory utilization and available swap space.	Mandatory
306.	The Systems and Distributed Monitoring (Operating Systems) of solution should be able to monitor: User-defined events in the security,system, and application event logs must be monitored.	Mandatory
SLA Monitoring		
307.	Should integrate with the application software component of portal software that measures performance of system against the SLA parameters such as • Response times; • Uptime; • Meantime for restoration of solution etc;	Mandatory
308.	Should compile the performance statistics from all the IT systems involved and compute the average of the parameters over a quarter, and compare it with the SLA metrics laid down in the RFP.	Mandatory
309.	Should compute the weighted average score of the SLA metrics and arrive at the quarterly service charges payable to the SI after applying the system of penalties and rewards	Mandatory
310.	Should be under the control of the authority that is nominated to the mutual agreement of SI & MPSEDC so as to ensure that it is in a trusted environment.	Mandatory

The SLA monitoring component of the should be subject torandom third party audit to vouchsafe its accuracy, reliability andintegrity.

2 Section II: Non-Functional Requirements

2.1 General Requirements

Sl. No.	Functional/ Business Requirement	Mandatory/ Desirable
311.	The solution should be highly scalable and capable of delivering high performance as & when transaction volumes/ users increases without compromising on the response time as mentioned in the SLA	Mandatory
312.	Overall Architecture should be based on high availability including the digital signing module.	Mandatory
313.	The application software should be compatible with all the standard operating system such as Windows, Linux, UNIX, etc	Mandatory
314.	The solution shall run on native browser with additional plug inn's that should be freely downloadable and should support at the minimum IE, Firefox Mozilla Google Chrome etc.	Mandatory
315.	The system should provide multi user login facility and open work group environment where users can access same information at the same time in secured manner	Mandatory
316.	The solution should provide for services being started/stopped from the administrative console	Mandatory
317.	User Interface should require only standards compliant browsers with standard support for JavaScript and HTML.	Mandatory
318.	The solution will initially be required to cover a range of process modules mentioned in the RFP, but it should allow addition of more modules or more users in any module as and when required.	Mandatory
319.	The solution should provide facility of remote access to the system administrator for security management, troubleshooting, etc.	Mandatory

320.	The solution should be capable to integrate with SMS gateway.	Mandatory
321.	It should support all standard transport protocols like http, https, ftp, ftps, imap and smtp, etc.	Mandatory
322.	The system should provide capabilities to define “Time based Actions” so that enable, disable and delete actions can be driven by date attributes.	Mandatory
323.	The user interfaces should be friendly and GUI/browser based	Mandatory
324.	The system should support completely web based administration and authoring	Mandatory
325.	The solution proposed should be supported by OEM. If any open source is proposed, then the SI should provision for timely OEM support of the problem. Community support is not allowed.	Mandatory

2.2 Security Requirements

Sl. No.	Functional/ Business Requirement	Mandatory/ Desirable
326.	The application should support SSL & digital certificate	Mandatory
327.	The solution should be capable of providing one user multiple roles and vice versa	Mandatory
328.	The solution should be capable of providing automatic timeout for user (log out)	Mandatory
329.	The solution should support password encryption while transmission	Mandatory
330.	The system should password management mechanism and password policies including: o Password expiry o Password complexity o Password history and reuse policy o Forced password change on first log on	Mandatory

331.	The session limits must exist for the application. For each session type, there must be limits on the number of sessions per user or process ID and the maximum time length of an idle session	Mandatory
332.	Should not require opening of any special protocols for connecting the user client to the web/ application server. All communication should be on secured HTTPS and SFTP	Mandatory
333.	The system should support role based access control, user based privileges	Mandatory
334.	The system should have the option to encrypt data before transferring over a network	Mandatory
335.	The system should support audit trails. The basic audit details like the user name, date and time, operation performed (update or insert) for each transaction should be available easily, without having to run queries or reports.	Mandatory
336.	The solution should have the ability to restrict users from unauthorized access by allowing only the authorized users with valid profile/password to access only the allowed transaction, as well as be capable of logging off unauthorized users	Mandatory
337.	The system should be able to define audit trails, audit logs and transaction logging requirements (what, when, who has changed).It shall ensure that the audit files are stored in un-editable formats	Mandatory
338.	The system should be designed with redundant and fail over capabilities	Mandatory
339.	The data should be stored in secured manner. The role based access should be implemented.	Mandatory
340.	All sensitive information (such as bank account numbers) should be encrypted while being stored. The cost of such encryption should be included in the bid.	Mandatory
341.	All activities configurable or functional in the application and/or database and/or host either directly or indirectly should be based on approval based mechanism and should be properly logged/recorded into the system. Any such change should be followed by a process flow approval mechanism.	Mandatory

2.3 Reporting/MIS Requirements

Sl. No.	Functional/ Business Requirement	Mandatory/ Desirable
342.	The solution should be capable of scheduling MIS for execution / refresh and/or distribution and/or publish	Mandatory
343.	The solution should be capable of distributing MIS through email as Body or attachment, if required	Mandatory
344.	The solution should permit viewing of MIS through web. The solution should allow users to send MIS report to specified user(s) at scheduled times	Mandatory
345.	The solution should have interface to search and filter the data of the report	Mandatory
346.	The solution should provide encryption and exception reporting mechanism	Mandatory
347.	The solution should be able to convert MIS reports to MS-Excel, MS- Word & PDF format directly	Mandatory
348.	The solution should provide graphical interface for creating custom formulas	Mandatory

2.4 Requirements of IT infrastructure

Sl. No.	Functional/ Business Requirement	Mandatory/ Desirable
349.	The solution should be highly scalable and capable of delivering high performance as & when transaction volumes/ users increases without compromising on the response time.	Mandatory
350.	The Production IT Infrastructure should have ability to withstand all single point of failure by providing clustering features	Mandatory

351.	The IT Infrastructure should support the use of fault tolerant multiprocessor architecture & cluster processing	Mandatory
352.	The IT Infrastructure should support auto-switching to available server in case of server failure	Mandatory
353.	The solution shall be supported on client with mobile based platform	Mandatory

3 Section III: Profile of the Key Resources

The Roles and Responsibilities of the resources to be deployed on the PARICHAI project are mentioned below.

Sl. No.	Role	Responsibility (Indicative)
1.	Project Manager (Education & Qualification as per Vol 1)	• Manage project from initiation to closure • Liaison with stakeholders to develop high level project schedule, plan for implementation of the project • Work with MPSEDC and stakeholders to complete project charter outlining scope, goals deliverables, required resources, budget and timing • Complete work breakdown structure to estimate effort required for each task • Manage all the manpower resources provided by the Systems Integrator • Shall behave as the Single Point of Contact for MPSEDC and Departments • Provide a project schedule to identify when each task will be performed • Track the present status of the project and fix any issues/ bottlenecks • Clearly communicate expectations to team members and stakeholders • Act as a mediator between stakeholders and team members • Resolve any issues with appropriate stakeholders and resolve problems throughout project life cycle • Manage all documents and approved with project change request forms • Track and report on project milestones and provide status reports to MPSEDC
2.	Solution Architect (Education & Qualification as per Vol 1)	• Understand the objectives of the project and devise the optimal solution to meet the objectives • Understand PARICHAI and departmental strategy and design the systems solutions to meet needs of the end user • Design the solutions, considering functionality, data, security, integration, infrastructure and performance etc. • Co-ordinate with Business Analyst, and various technical resources to produce a technical specification for custom development and systems integration requirements • Provide current best practices • Understand and support the software development and support PARICHAI development team in developing solutions

Sl. No.	Role	Responsibility (Indicative)
		• Monitor performance & efficiency of the system on daily basis • Address any technical issues that might arise on account of CIDR, Department, technology, etc. • Reporting to concerned MPSEDC Official on issues and their probable resolution • Strategize the rollout of the solution • Liaison with stakeholders to develop high level project schedule, plan for implementation projects. • Develop the various technical standards that need to be followed for the successful implementation of the project. • Mentor and provide technical training to SI resources as and when required. • Resolve various technical issues related to development, testing and maintenance of the solution
3.	Business Analyst (Education & Qualification as per Vol 1)	• Understand the existing PARICHAI application • Understand the requirement of the client and translate the same into technical requirement document. • Elicit requirements using interviews, document analysis, requirements workshops, surveys, site visits, business process descriptions, use cases, business analysis, task and workflow analysis. • Participate in process flow analysis and process design along with the Solution Architect and technical team • Take inputs from various stakeholders on the business requirement of the Department • Co-ordinate with technical resources for custom development and systems integration requirements • Produce a detailed systems functional design document to match customer requirements • Assist the client in UAT efforts • Participate in training design, documentation and delivery efforts • Clear doubts of the technical team on the requirements as captured. • Liaison with the solution architect to design the most optimal solution • Report to concerned MPSEDC Officials on status • Critically evaluate information gathered from multiple sources, reconcile conflicts • Decompose high-level information into details, abstract up from low-level

Sl. No.	Role	Responsibility (Indicative)
		information to a general understanding • Distinguish user requests from the underlying true needs.
4.	Data Analyst (Education & Qualification as per Vol 1)	• Collect, compile and analyze data from various sources such as Department, CIDR etc. • Draft and prepare standard and/or ad hoc reports • Understand MPSEDC's requirement and design the schema and data retrieval mechanisms • Develop and/or maintain and enhance existing databases and reports • Integrate the CIDR and Departmental Data for matching and seeding • Maintain the data on regular basis • Encrypt the data on need basis • Carry out performance tuning with timely implementation of features such as indexing, partitioning etc. • Maintain the schema in accordance to the design • Maintain test environment, pre-production environment and production environment in accordance with the guidelines as issued from UIDAI from time to time • Coordinate with ASA, KSA for prompt response to the Auth and KYC requests • Maintain all the logs that are developed in the system • Carry out the archival practices that are required from time to time • Maintain the system in accordance to the laid down standards and procedures
5.	BI Developer / Designer (Education & Qualification as per Vol 1)	• Coordinate with Business Analysts and customers to develop business requirements and specifications documents. • Understand the BI requirements of PARICHAI and Departments • Access the various data points that are required to meet the requirement • Devise strategy to get the respective data from source systems. • Develop the various modules in accordance with FRS, SRS such as Extraction, Standardization, Authentication e-KYC etc. • Develop standard reports and functional dashboards based on business requirements. • Maintain business intelligence models to design, develop and generate

Sl. No.	Role	Responsibility (Indicative)
		both standard and ad-hoc reports. • Generate reports for MPSEDC users and departmental users based on their needs • Incorporate any changes in reports if suggested by the end user • Determine business intelligence solutions as per the needs of MPSEDC and Departments • Ensure accuracy of the reports that are displayed to the end user • Identify and resolve data reporting issues in a timely fashion
6.	Senior and/or Java / Dot Net Developer & PL/SQL Developer (Education & Qualification as per Vol 1)	• Develop the system based on requirements of MPSEDC and Departments • Develop custom made software application where proposed tool/COTS do not provide the functionality • Test the application and remove bug as reported by any third party such as STQC • Take ownership and maintain the existing PARICHAI application • Make improvements and changes in the existing PARICHAI application • Customize the tools and the COTS products according to the business needs • Maintain the application to meet the SLAs • Write all relevant documents such as Test Reports, Deployment Script, User Manual/SOP, Technical Manual, Traceability Matrix etc. • Maintaining the systems once they are up and running • Remove all bugs in production environment • Implement Change Requests, if any • Maintain the code in accordance with software standards
7.	Oracle / Microsoft / Other Database Administrator & Server Administrator with experience in Virtualization	• Install and Configure Infrastructure (hardware and software) • Maintain Infrastructure • Perform daily operations • Support development team in configuration wherever required • Report infrastructure utilization and other required by Project Manager and MPSEDC • Implement Infrastructure Changes, Patches, Upgrades etc. • Coordinate with OEM for support tickets

Sl. No.	Role	Responsibility (Indicative)
	/ Cloud & Network Administrator & Backup and Storage Administrator (Education & Qualification as per Vol 1)	• Take backup of the data (both application and infrastructure i.e. database, operating system, virtual machine etc.) as per backup policy • Restore data as and when required by Project / MPSEDC • Submit monthly, daily reports of system utilization and maintenance tasks done • Capacity planning based on system utilization trends • Advise MPSEDC as and when required for infrastructure related • Check with OEMs availability of new patches, their assessment, recommendation and installation in the infrastructure • Troubleshoot problems related to Infrastructure • Apprise <MPSEDC beforehand for any actions to be taken related to infrastructure augmentation etc. to avoid future failure / unavailability.
8.	Security Expert (conversant with cyber and aadhaar laws & regulations) (Education & Qualification as per Vol 1)	• Always updated with Security guidelines of UIDAI, Govt., Law, Orders etc. • Guide team to maintain system according to industry standard security policies and other Aadhaar guidelines • Ensure all security policy in place and being implemented on ground • Report any non-adherence directly to MPSEDC • Recommend security measures to be taken time-to-time to MPSEDC and Project

End of Vol - II