Annexure IX

Revised

SECTION V – SCHEDULE OF REQUIREMENTS

Table of contents

1. Intent

The Director General of Unique Identification of Authority of India (UIDAI) is inviting this **Bid** for "Hiring of Data Center Space and Facilities for Unique Identification Authority of India at Delhi / NCR."

1.1. Structure of Document

1.1.1. This document is divided into following three parts

- **Part I: Overview** – This part provides an overview of the current requirement at the UIDAI and provides an overall view of the Technical Requirements.
- **Part II: Schedule of Requirements** – This part provides the Schedule of Requirements related to the Data Center Space and Facilities.
- **Part III**: **Technical Specifications –** The Technical Requirements for establishing the Data Center in Delhi / NCR are stipulated in the respective sub-section.

1.2. Overview

1.2.1. This Bid Document has been prepared solely for the purpose of enabling Unique Identification Authority of India (UIDAI) to select a service provider for Data Center in Delhi / NCR.

1.2.2. The Bid Document is not recommendation, offer or invitation to enter into a contract, agreement or any other arrangement, in respect of the services. The provision of the services is subject to observance of selection process and appropriate documentation being agreed between the UIDAI and any successful Bidder as identified by the UIDAI, after completion of the selection process as detailed in this document.

1.2.3. UIDAI invites proposal from Data Center Service Provider (DCSP) for primarily undertaking inter-alia the activities for UIDAI in respect of co-hosting services spread over in the following manner.

The Bidder should offer a contiguous space of 2000 sq. feet of Data Center of Tier III space at the stage of bidding.

1.2.4. The above mentioned space should be readily available at the time of bidding.

1.2.5. UIDAI will at no point bear any additional cost for any Data Center facility that DCSP may have to incur on account of repair, upgrade, power, capacity enhancement etc. to support UIDAI equipments unless UIDAI requests for any additional power requirements or brings in additional major equipments that would impact the infrastructure allocated to UIDAI by DCSP for the period of the contract.

1.2.6. The DCSP has to factor in the infrastructure for the UIDAI requirement. UIDAI will not accept any plea from the DCSP for any additional costs. The

DCSP is expected to factor the power cost escalation in the commercial bid quoted. UIDAI will not bear any changes or escalations in the power tariff in the first one (1) years of the contract.

1.2.7. The DCSP should provide all necessary infrastructure components that would be necessary as per the defined requirements; manage and maintain the same throughout the period of the contract.

1.2.8. The Bidder shall hold a valid ISO 27001 Certification, for the facility. Alternatively, if the Bidder does not have a valid ISO Certification, then the Bidder should give an undertaking, as part of the response to this Bid, that the Bidder would obtain the ISO Certification within 4 months from Stipulated Sate of Signing of the Contract. The Bidder should also indicate any other accreditation rating received from an internationally accredited third party rating/ certification agency for the Data Centers at Delhi / NCR and also indicate alternate equivalent standards and practices being followed at these Data Centers.

1.2.9. The DCSP has to ensure that the desired objective of hosting the UIDAI IT infrastructure is completely met. The Bidder must be the owner of the proposed Data Center facility provided to UIDAI and sign Service Level Agreement for an uptime of 99.99%.

1.2.10. The proposed Data Center building should be owned by DCSP. In case the building is leased then the available period of lease should not be less than 7 years without any interruption from the stipulated date of opening of bid. The DCSP shall pay all taxes & comply with the rules and regulations as laid by the Government. Copies of the documents establishing the same should be furnished as stipulated in **Clause 4.1.7 of Section IV.**

1.2.11. The building/ property shall be insured on a comprehensive basis from all Natural, Manmade disasters or any other similar disasters. Copies of the Insurance documents should be furnished as stipulated in **Clause 4.1.7 of Section IV.**

SCHEDULE OF REQUIREMENTS

2. SCHEDULE OF REQUIREMENTS

2.1. Data Center Space

2.1.1. The DCSP should supply and install standard server racks of 42U height600mm wide and 1000mm deep, aluminium extruded with perforated doors in the front and rear. The DCSP should provide racks of one of the following makes: **APW President, Rittal, APC.**

2.1.2. Each rack should be provided with dual power source of minimum 7kVA rated capacity through at two separate/isolated feeds from UPS systems feeding two (2) separate power strips.

2.1.3. The 7kVA rating requirement mentioned above is estimated as an average requirement for UIDAI. The DCSP should provide for up to at least 6 racks with rated capacity requirements of 12.5kVA or above. (63 Amp Single/ Three phase dual supply).

2.1.4. The incoming power should be from two (2) separate feeders for individual UPS.

2.1.5. Each rack should be properly grounded; two PDU's and cable managers should be installed.

2.1.6. The space allocated to UIDAI shall be made secure by providing a metal cage with **Palm Geometry Access** at entry. One emergency exit door preferably at the diagonally opposite side.

2.1.7. The metal cage shall be properly secured to the floor and ceiling and should be of MS with not more than 1" spacing mesh.

2.1.8. The caged area earmarked for UIDAI should be provided with CCTV for surveillance and vigilance on 24/7 basis. The caging accounts for the DC space and also the Communication Room (if shared). However Access Control and CCTV surveillance and 24/7 vigilance is a mandatory requirement.

2.1.9. The space of 2000 sqft assigned to UIDAI shall be made ready for receiving equipment within a period of 30 calendar days from the Date of Issue of LOI. Subsequently, UIDAI would commence equipment installation related activities that is estimated to take another 30 days. This period of 60 days should be rent free.

2.1.10. Bidder should offer a contiguous space of 2000 SqFt of Data Center of Tier III standards, separately indicating scalability of additional space if available.

2.1.11. The additional space as indicated above, may be availed by UIDAI at its discretion.

2.1.12. In case the DCSP intends to rent out the above additional space to any other customer, he should check with UIDAI.

2.2. Communication Room

2.2.1. Dedicated communication room (some times referred as Meet Me Room) of 100 sq. feet shall be provided to accommodate minimum of two Internet service providers' equipments. The service providers should be ready with IP version 6 connectivity.

2.2.2. The DCSP shall also provide dedicated high bandwidth connectivity with termination equipment and route diversity from minimum two internet service providers. The service providers should be ready with IP version 6 connectivity. Such termination should be done in the dedicated communication room. The rates for the bandwidth need to be provided in the commercial bid.

2.2.3. Each communication rack provided by the DCSP should be 800mm in width and 1000mm in depth and 42U in height.

2.2.4. The Structured cabling for LAN should be provided and implemented by DCSP. This LAN should be designed for 10Gbps throughput. All the required passive components are to be provided by DCSP and with corresponding certifications for 15 years.. Each rack should have provision of 24 copper ports and 24 fiber ports. The active components will be supplied by UIDAI.

2.2.5. DCSP will conduct physical layer testing and test and confirm that all cross-connects are functioning normally to the patch panel in the Data Center.

2.2.6. DCSP will install and maintain the following within 24 hours of request from UIDAI:

i. Copper patch cords between devices in the UIDAI Area.
ii. Fiber patch cords between devices in the UIDAI Area;

2.3. Office Space

2.3.1. Seating space with LAN connectivity for minimum of 15 persons shall be provided for UIDAI and its representatives to monitor and upload the data.

2.3.2. The office space should have furniture like tables, storage units and space for printers and copier machines.

2.3.3. Minimum of 1 cabin should be provided for senior cadre to monitor the people deployed.

2.3.4. In case of additional space requirement for 15 more persons, the DCSP should have the space for scaling up and provide the same within the same building.

2.3.5. The office space shall have access control to allow only authorized personnel of UIDAI to enter.

2.4. Other Requirements

2.4.1. At UIDAI's request, DCSP will receive any UIDAI Materials on UIDAI's behalf. DCSP will store UIDAI Materials in the Secure Storage Space (store room) immediately upon delivery to the Facility and maintain a written log of a description, date and time of UIDAI Materials placed by Service Provider in the Secure Storage Space (store room).

2.4.2. DCSP will provide UIDAI all necessary assistance in preparing return materials authorization ("RMA") documentation and packing, returning and shipping such damaged UIDAI Materials to a location or manufacturer, service provider or other third party designated by UIDAI.

2.4.3. Along with the office space, a full sized (one number) Fire Retardant Filing Cabinet will have to be provided to store electronic media.

2.4.4. The keys of the Fire Retardant File Cabinet should be in the custody of UIDAI authorized personnel.

2.4.5. UIDAI may depute personnel from CISF at the DCSP location to strengthen the security of the data center. The DCSP should provide a No Objection Certificate along with the Bid for the same.

2.4.6. UIDAI would also conduct audit of the facility periodically to access the operations and to sign off the uptime report.

2.4.7. DCSP should have a Help-Desk operating on a 24/7 basis to login any calls and avail services under the scope of DCSP. Shared Helpdesk is acceptable.

2.4.8. UIDAI desires to avail Managed Services from DCSP. Bidder should confirm the availability of such services and also submit the standard deliverables for the following services. Operation window will be decided mutually. The NOC for these Managed Services should strictly be on-site. The Software required for the Managed Services would be provided and operated by the DCSP and would remain in their scope.

2.4.9. The staff strength required below is for steady state operations and is provided as a guideline for the bidders. Hence bidders may also submit an alternate staffing and **scaling** plan along with their proposal. Bidder may not require the entire staff proposed below on Day 1.

2.4.10. The Managed Services from DCSP shall be required to provide support for Build, Commission, Installations and operations of Racks, Cabling Servers

Storage, Networking, Firewalls, Routers, Intrusion Detection Devices, Softwares, OS, Databases, middle ware and hardware and networking components.

Sl.No	Resources	Numbers of personnel	Key personnel of MSP
1	***Operation and Maintenance - Data Center***		
	Project Manager	1	1
	Shift Manager	3	1
	Inventory Manager (one per Shift)	3	-
	Electrician (one per Shift)	3	-
	Network engineer	2	1
	Storage engineer	4	2
	System administrator	10	3
	Database administrator	4	2
	Application administrator	6	3
	Security engineer	4	2
	NOC engineer	4	2
	Service engineer	8	2
	Quality Assurance staff	2	1
2	***No. of seats in Non DC (Office Space)***		
	Seats with Telephone Connection, PC covering the following configuration: Intel Core 2 Duo processor, 2 GB RAM, 300 GB HDD, 15" Colour TFT Monitor, keyboard, mouse, etc. with OS as Windows XP or higher version and MS Office 2007.	15	

Note :-

1. The Bidder should note that the proposed MSP team as per the table above, should be on MSP's payroll
2. The Bidder should submit the proposed MSP team CV's and the same would be used for evaluation set under Section II of Clause 31.6

2.5. Job Descriptions:

Profiles of manpower requirements for the Managed Services at the Data Center

Sr. No	Personnel Required	Qualification	Area of Specialisation	Certifications required	No. of Resources
IT Personnel					
1	Network Engineer	BE – Computers/Electronics MCA with minimum experience of 3 years as Network Engineer	Should have proven expertise in the following areas 1. NMS – Familiarity with SNMP (V1/V2), CIM, JMX standards 2. Configuration, Installation , trouble shooting of routers, switches (Cisco NEXUS 7600) and firewalls 3. Port configuration 4. Configuration of TCP/IP (V4/V6), RIP/OSPF/BGP/STP protocol parameters. 5. Interface with ISPs for troubleshooting WAN link issues 6. Security protocol (SSL, Kerberos) 7. Proactive management and Preventive maintenance of L2/L3 components 8. Setup, Manage, Configure –HIDS, NIDS, SYSLOG, VPN, RADIUS servers	Cisco Certified Network Professional (CCNP)	2
2	System admin/ Consultant	BE– Computers/ Electronics MCA with minimum experience of 3 years as system administrator	Should have proven expertise in the following areas 1. Installation , Configuration of Linux OS 2. Analysis of system resource utilization 3. Capacity, planning and management, performance tuning, system upgrades, bug fixes and implementation of software patches. 4. Installation and configuration of	Redhat Certified Architect (RHCA)	10

			virtual machines, troubleshooting system issues, supporting application/middleware installation-reconfiguration, adding/deleting users from the system, and generating reports. 5. Configuration and implementation of SAN, creation and management of file systems, volume groups. 6. Experience of atleast 1 year in installation, management and administration of blade servers is a must.		
3	Database Administartion	BE – Computers/Electronics MCA with minimum experience of 5 years as database administrator	Should have proven expertise in the following areas 1. Monitoring and maintenance of databases, installation of database software patches/upgrades, monitoring of database backups, database replication techniques, standardization and implementation of databases to improve the management of production and test environments, support users by resolving problems with applications' databases. 2. Monitor and allocate volumes, analysis of utilization and resources, performance tuning, monitor db replication, coordination of system upgrades or fixes. 3. Should have extensive experience in administering databases of 10+ TB . 4. Should have a minimum of 3 years experience as a DBA on a Unix/Linux platform (MySQL/Oracle). 5. Setup, Manage and tune databases in a clustered	MySql	4

			environment.		
4	Storage engineer	BE – Computers/Electronics with minimum experience of 3 years as storage administrator	Should have proven expertise in the following areas 1. Monitoring and maintenance of SANS, configuration and monitoring of Fibre Channel Switches/Fabric, installation of disk arrays, patches/upgrades, firmware upgrades, snapshots and backups, standardization and implementation of storage to improve the management of production and test environments, support users by resolving problems with storage. 2. Should be familiar with storage management products (EMC/HP/IBM/NetAPPs), identifying and resolving storage and i/o bottlenecks. 3. Allocate volumes, create and manage zones, LUN, manage fabric security, analysis of utilization and resources, performance tuning, capacity planning, monitor storage based replication, coordination of system upgrades or fixes with system and database administrators.	NA	4
5	Application Administrator/Support Engineer	BE – Computers/Electronics with minimum experience of 3 years as Application Administrator/Support Engineer	Should have proven expertise in the following areas 1. Installation of Application and Patches on the Web, Application Server and Messaging Middleware 2. Monitoring of applications and application logs for errors, failures 3. Should be familiar with J2EE packaging, deployment and monitoring of application using standard and open source tools	NA	2

			4. Should be able to diagnose and identify application and system related issues 5. Should interact with the application development teams for resolution and closure of application related issues 6. Should be familiar with scripting languages with javascript, perl, python 7. Should be familiar with application performance monitoring and profiling tools like JConsole, JProbe, PurifyPlus etc.		
6	Project Manager	BE/MCA – Computers/Electronics/Electrical with minimum experience of 5 years as Project Manager	Should have proven expertise in the following areas 1. Should have atleast 12 years experience in the IT industry with exposure to Data Centre Management, Infrastructure Management and Application Management 2. Should be familiar with ITIL processes 3. Should create, manage and track project plans for the managed services activity 4. Should provide weekly managed services reports 5. Should interact with the other service providers for resolving issues 6. Should possess good written and spoken communication skills in English 7. Should be conversant with Microsoft Project, PERT/CPM techniques 8. Should have managed atleast 1 similar project in a Managed Service Provider Environment with atleast 100 servers, 5 TB of	PMP Certified	1

			Storage, used ITIL processes		
7	Security Engineer	BE/MCA – Computers/Electronics/Electrical with minimum experience of 5 years as Security Engineer	1. He should have specialization on a range of solutions, including, but not limited to, SSL, making appropriate use of PKI, intrusion detection / prevention, VPN, single sign-on, firewalls, and all elements of application-level security 2. He should have a minimum of 5 years experience in designing and implementation of similar infrastructure. 3. Should be well versed with security aspects of linux environments (especially RHEL) and its hardening procedures 4. Should have hands expertise with industry leading security and management tools		1
Data Center Personnel					
1	Shift Manager	B.E./ Diploma in Electrical/ Mechanical	1. Should have experience of about 5 to 7 years in Data Center operation and maintenance. 2. Should be technically sound and have hands on experience in trouble shooting. 3. Should have good interpersonal skills to handle vendors and junior staff and should be able to multi task.	NA	1

2.6. Scope of work for managed services

2.6.1. Overview Of UIDAI System Architecture

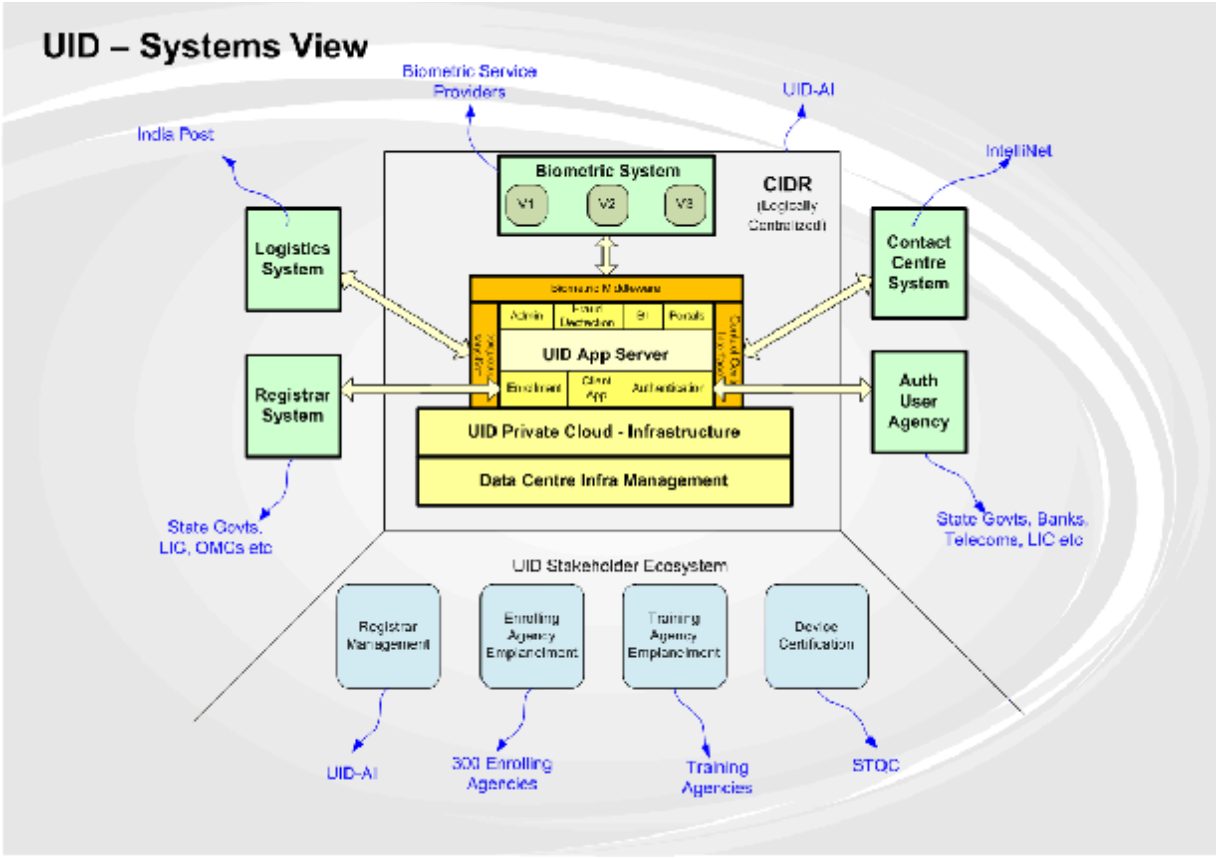


Figure 1 UID System View

A high level system view of the UID is shown in Figure 1.

2.6.1.1. **List of Components**

The main components of UID System are,

a) UID Application
b) Biometric System
c) UID Private Cloud – Infrastructure
d) Data Centre
e) Logistics System
f) Registrar System
g) Contact Center
h) Auth User Agency
i) Registrar Management
j) Enrolling Agency Empanelment
k) Training Agency Empanelment
l) Device Certification

Users	High Level Responsibilities
External	
Registrar	• Registers self and other system users, sub-registrars, introducers with CIDR • Submit batch enrolment requests to CIDR • Receive Status messages on UID enrolment requests such as 'Submitted', “Delivered' etc. • View individual status, statistical reports • Perform off-line authentication • Receive complaints from applicants and submit to CIDR • Pre-load resident demographic data to CIDR so that they can enrol later easily. • Provide authentication services as an agency
Sub Registrar	• Submit batch enrolment requests to Registrar or directly to CIDR • View individual status, statistical reports • Receive complaints from applicants and submit to CIDR.
Enrolment Agency	• Operate an enrolment station for residents to come and enrol. • Submit enrolment data on the network to a facilitation center or a regional office. • Submit the batch data of enrolments to CIDR on a media via a logistics provider
Resident	• Enrols through an enrolment agency with or without an introducer. Receives UID through Logistics provider • Apply for updates to personal information in CIDR • Submit grievances to Registrar, Contact Center
Authentication User Agency	• Register self with UIDAI and CIDR • Submit Authentication Requests (as calls) to CIDR and receive responses • Make payments against bills from UIDAI
Logistics Operator	Inbound: • Collect media from Enrolment Stations and deliver to CIDR • Update CIDR and Registrars on the status Outbound: • Receive UID data from CIDR, print and deliver • Update CIDR and Registrars on the status
Contact Center	• Receive Calls from residents who have applied and residents yet to apply and • Provide information/guidance about UID, process, enrolment stations, introducers, documentation

	• Receive batch status information from CIDR • Submit canned queries to CIDR to update local database • Provide the status of UID application to residents
Internal Users	
UIDAI/CIDR Staff	• Register self with CIDR • Manage all accounts • Oversee policy implementation and SLAs & operations of Managed Service Provider • Detect and act on frauds and security breaches • Generate periodic reports for public and ad-hoc reports • Oversee billing and accounting • Manage Exceptions • Review MIS reports
Technical Helpdesk	Manage all exceptions in UID workflow
TP Audit	• Inspect audit information with respect to usage, security, data confidentiality
UIDAI	• Act as the governing body to manage the entire life cycle of the UID system

2.6.1.2. **UID Application**

a) Overview of applications hosted in CIDR

The application hosted by CIDR can be broadly categorized under the core applications and supporting applications are described in the Figure below. In the core category we have the enrolment and authentication applications services. While the supporting category consists of applications required for administration, analytics, reporting, fraud detection interfaces to Logistics Provider and Contact Center and the portal.

i. The ***Enrolment Application*** services the client enrolment request for providing a UID. The enrolment application orchestrates the enrolment workflow by integrating various sub-systems such as address normalization, third party de-duplication, and UID generation. Manual Exception Workflow is required to resolve Enrolment requests that cannot be resolved automatically. Basic Letter Printing and Delivery functionality is available for servicing exceptions to normal workflow.

ii. The ***Authentication Application*** provides the identity authentication services. Various authentication request types such demographic, biometric, simple or advanced authentications are supported. The UID number submitted is used for 1:1 match for the resident's record. The inputs are then matched against the resident information found in the biometric database.

iii. The ***Fraud Detection Application*** is deployed to detect and reduce identity fraud. For example identify fraud scenarios that the application needs to

handle are: misrepresentation of information, multiple registrations by same resident, registration for non-existent residents, or authentication as someone else.

iv. The ***Administrative Application*** takes care of user management, roles and access control, business process automation, and status reporting. It ensures a trust network across both internal and external entities. The external entities could be registrars, sub-registrars, enrolment agencies, field agencies, introducers, and authentication clients. For example the application is required to manage user accounts for the registrar users or introducers who vouch for identity of individuals who lack proper documentations. The internal entities could be system administrators, customer service agents, biometric and fraud detection agents. The application will allow administrators to track status of use cases, and provide mechanism to escalate failures or delays.

v. The Analytics and Reporting Application provides enrolment and authentication statistics for both public and partners. It supports visual representation of statistics and allowing drill down at region levels. All the information available for this application is only at the aggregate level thus ensuring individual identity is completely protected.

vi. The Information Portal provides an administrative and information access for internal users, partners and for public. Besides the above Application, interface application for Logistics and Contact Center are also present in the CIDR.

vii. The Contact Center Interface Application provides query and status update functionality.

viii. The Logistics Interface Application interfaces to the Logistics Provider for letter printing and delivery. It is used for sending and receiving raw data, sending UID data for letter printing and delivery and receiving periodic status updates on the inbound and outbound sides.

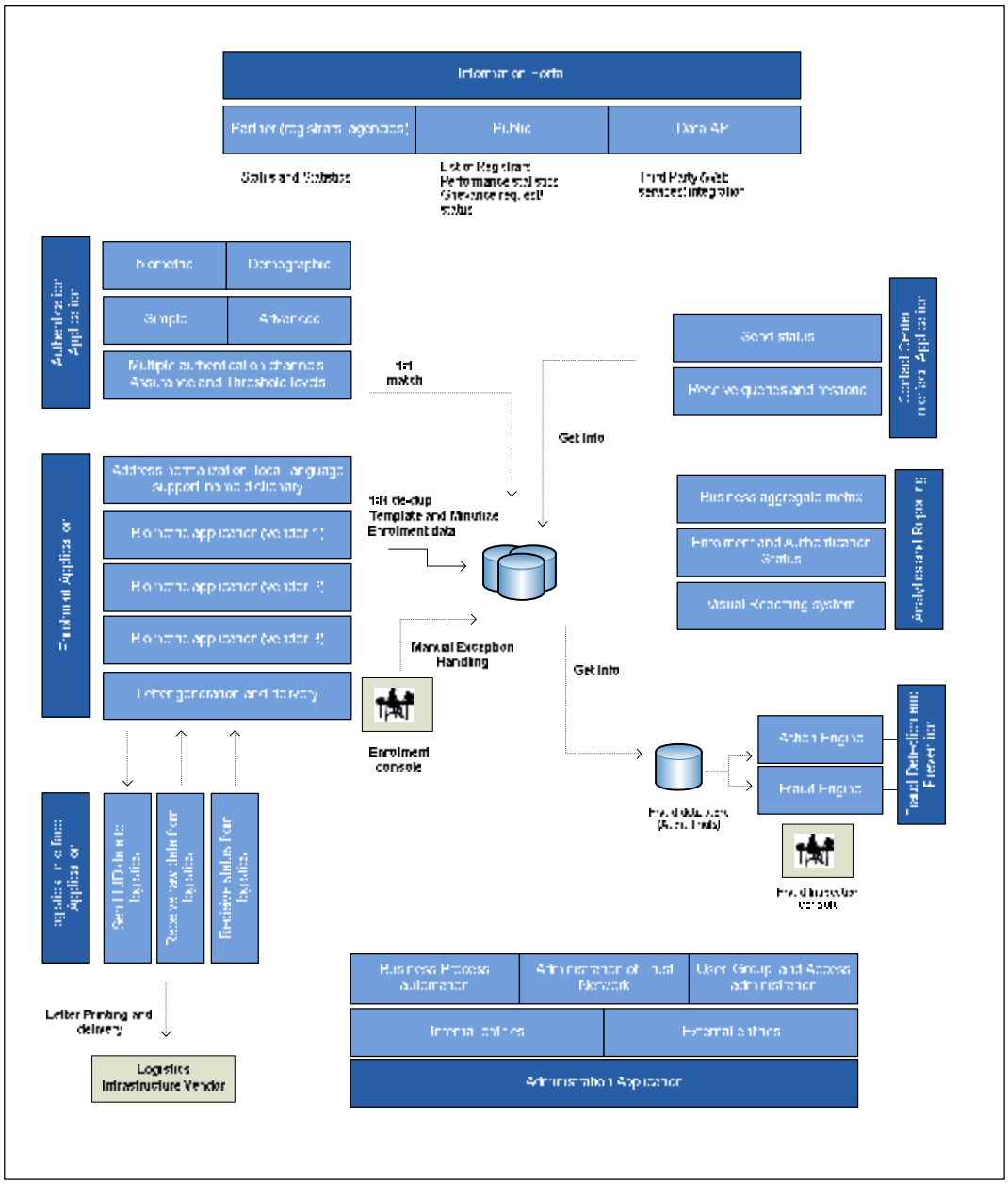


Figure 2 Applications hosted in CIDR

b) Overview of Network Architecture

Initially it is proposed to have a CIDR Data Centre and Disaster Recovery site (which is passive) with three options for Partners/Registrars to upload data. These being:

I. Manual loading of data through disks
II. Internet enabled data upload
III. Dedicated connectivity between Registrar/Partners and CIDR Data Centre.

The UID/Biometric verification service shall be provided over the internet. Both Primary Data Centre and additional Data Centre will house network connectivity to UIDAI Regional Offices, Registrars/Partners network and Internet connectivity as specified or approved by UIDAI.

The UID/Biometric verification service shall be provided over the internet and partner/registrar network. The CIDR will have Primary Data Centre in Bangalore and CIDR-DR in NCR. Both Primary Data Centre and additional data centres will house network connectivity to UIDAI Regional Offices, Registrars/Partners network and Internet connectivity as specified or approved by UIDAI. CIDR Data Centre Wide Area Network Infrastructure is partitioned as Internet, Registrar/Partner, and UIDAI network Edge based on the business needs like security, manageability and scalability. It is envisaged that in due course the topology of the CIDR will change to an active-active data centres.

Note: When migrating to an active-active multi-site Data Centre topology additional links are required for each Data Centre

c) CIDR Local Area Network

The CIDR Data Centre has to designed and defined by the Network Architecture principles. The network infrastructure should support multitude of applications in a secured manner to meet the business requirements. CIDR Data Centre network consists of independent secured functional modules such as-

(i) Server network
(ii) Biometric network
(iii) Backup and Restore network
(iv) Storage network
(v) Security and Management network
(vi) Network Operation Center

All Segments are interconnected to the Data Centre Core Data and SAN switches. The core switches provides all features and functions as specified including the functional isolation and security. The core devices are deployed in a redundant and high available mode with multiple connections core to access network devices. All network elements are redundant to provide the desired uptime agreed with UIDAI. The Data Centre along with a dedicated storage and data network can support unified fabric for server IO consolidation. Due to business requirements, application isolation between various vendors or supplier is provided using high end firewalls. The vendor should be choosing the appropriate connectivity interface types which are interconnecting various devices and complement to build the secured network architecture.

d) Wide Area Network

The UIDAI CIDR Wide Area Network (WAN) edge has three major different types of connectivity with physical and logical isolation. The isolation between each layer is based on the business requirements. Internet and Registrar/Partner networks are used for verification services or enrolment. Internal UIDAI network is accessed by UIDAI authorized employees/partners.

CIDR consists of two DMZ's, one for Enrolment Data and other for verification. Internet and Partner/Registrar network and DMZ's are terminated at Internet distribution layer with appropriate security and isolation (traffic, Access and network) between networks as required. This layer also houses the VPN infrastructure/service and depending on the business needs the VPN/Dual authentication system can be activated.

Access to CIDR Data Centre is controlled and monitored through CIDR Edge security and all UIDAI internal networks are connected to CIDR edge with appropriate isolation. Each layer is embedded with network security for access control, monitor, detect and alert the network anomalies in real-time. The service provider has to standardize the design and review configurations in consultation with UIDAI on a continuous basis. The network is embedded with VPN services both for VPN with dual factor authentication as well as site to site VPN for enabling the private networks within network. Perimeter security has to be enabled at every appropriate level as required to protect the business.

e) Logistics Network

The Logistics Network is the UID letter dispatch center which has been outsourced. This network provides the ability to print the voluminous UID letters at a single location. The logistics center will house at one of the regional office or at head office or any other location selected by UIDAI. The location selection and identification is subject to UIDAI decision.

f) CIDR Network and Components

a. **Purpose -** This section of the document describes the network architecture for the CIDR Network.

b. **Types of Users -** The UIDAI CIDR services various users rendering different types services to UIDAI. In brief the typical user categories are:

c. **Enrolment Agencies -** These are organization/teams engaged by UIDAI for Capturing, Collecting and delivering the Enrolment Data to the UIDAI locations as desired by UIDAI.

d. Registrars/Partners - These are organization/teams using the UIDAI services for identity verifications. They are service accessors who will connect directly either to CIDR and DR either point to point link or MPLS cloud. Based upon the approved vendor connection request and authorization by UIDAI the service provider will interconnect. Partners/Registrars are supposed to adhere to policies defined by UIDAI.

e. **Demilitarized Zone (DMZ)** - Demilitarized zone is part of the overall CIDR Data Centre architecture. In the current architecture there are two DMZ's. One is for Enrolment data collection and other is for verification DMZ. Both the DMZ's are part of overall security architecture. Both the DMZs are connected to the same infrastructure but are logically isolated.

f. **Militarized Zone (MZ)** - The militarized zone is the core CIDR Data Centre. The CIDR is isolated using CIDR Edge security layer. The CIDR Edge security layer isolates the external network and internal Data Centre network. The Data Centre network is terminated on the Data Centre core layer. The Data Centre core layer switches are high performance, high available switches and provides the logical separation within. The CIDR (MZ) is created different modules with function dependent and they all terminated on core switches.

There are two different types of core switches one for Data and other for SAN. The Data Centre is 10G enabled end to end for production network.

g. Communication Room - The communication room houses the CPE devices like STM and the Service Provide cable termination. The STM output will Ethernet interface for termination on WAN network elements. All communication rooms are equally important and critical to business of CIDR Data Centre. The communication room should be with right security and environmental condition like cooling, humidity with uninterrupted power source. The communication room should host at least four different service provider terminations and should expandable as required. The communication room should provide the structured and adequate connectivity (fiber and copper) to Wide Area Network Edge.

h. Information Flow through the LAN - Information flow is from three different types of users as detailed in types of users section**.**

Enrolment agencies will transfer the enrolment data CIDR data center either through internet or through UIDAI regional offices. The Enrolment Data will be made available securely to biometric engine

Partners/Registrars are the UID service users of CIDR and the information is in the form of network queries for verification

UIDAI employees and partners authorized will have direct access to CIDR and also the vendor team who requires providing assistance will have time/role based secure access.

CIDR messaging infrastructure is used for delivering the electronic UID letters.

i. NOC Network - The NOC is a dedicated framework for monitoring all network elements within UIDAI network. NOC and is the extension of the network security and management framework. The location of the NOC will be either housed in CIDR or any of the UIDAI location subject to UIDAI approval. The NOC center will monitor the availability and all other elements of the network. It involves monitoring, escalations, coordination and resolution of the issues as required.

2.6.1.3. Server

a. Overview

This section of the document describes the server architecture for the UID system. It explains various applications and server groups of the system.

Primarily there are 4 groups of servers as follows:

- Servers in the DMZ
- Servers in the MZ consisting of
- Servers for UID Application
- Servers for Biometric De-duplication
- Servers for Management Applications
- Servers for other supporting services

The applications are as follows:

i. DMZ Application

The DMZ supports the following application components:-

- Load Balancer – this is an appliance attached to the switch and hence covered under Network architecture.
- Web Server – this acts as the front end to portal application
- FTP server – to receive the uploads of Raw Data from Regional offices and registrars
- Anti-virus application – to scan the input enrolment data file for viruses.

ii. UID Application

As already explained earlier, the main functions are:

- Enrolment
- Authentication
- Fraud Management
- Business Intelligence or Analytics
- Manual workflow for handling enrolment exceptions

iii. Biometric Solutions

There are 3 vendor solutions each performing,

- 1:N deduplication
- UID authentication

b. Key Assumptions

S. No.	Variable	Value
1	Peak enrolments per day Peak enrolments per second	1 Million+ 24+ per second

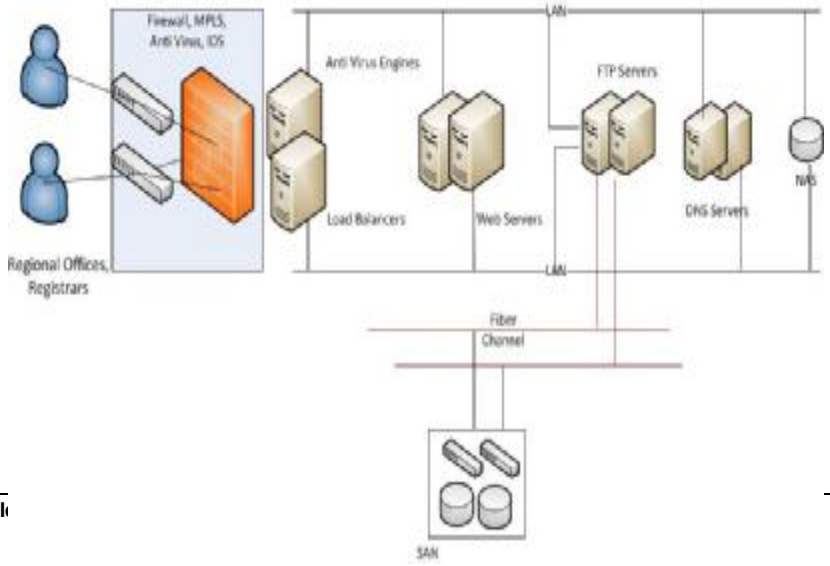
S. No.	Variable	Value
2	Raw data size per enrolment (in MB)	5 MB
3	Raw data input rate (computed)	>=1 Gbps
4	Number of days of raw data storage in DMZ	5 days (Data may arrive from the remote sites via media in bulk, there may be lag in processing)
5	Operational data per enrolment	1 MB
6	Peak authentication requests per day	10 Million+
7	De-duplication network bandwidth	>=1,920 Mbit/Second
8	Estimated memory per core in GB	8 GB
9	Number of Network Service Providers	>=2

c. Deployment Architecture for DMZ

The functionality of DMZ application consists of

1 Web Application for login + user authentication
2 Anti-virus scanning for enrolment file
3 Load Balancing for FTP
4 FTP server for receiving raw data of 5MB/Enrolment
5 File content/Format validation
6 Writing to the DMZ SAN. The SAN is expected to store or buffer atleast 5 million enrolment requests
7 The DMZ'z for enrolment and UID verification are separately deployed

Figure 3 CIDR High Level Deployment View



d. Web Server

The Web Server performs the usual function of allowing authorized users to login and use the services of the CIDR. Please refer to the DMZ deployment architecture. The protocols supported are Http 1.0, Http 1.1, https, ftp.

The web servers for enrolment and UID authentication are separately deployed in 2 different DMZ for security reasons.

e. Anti-virus Engine

This is an important high performance, load balanced application. The AV engine scans all the input files and protects against all kinds of viruses, trojan horses etc. Constant, supervised upgrade is required to provide the best possible protection.

f. FTP Server

The FTP Server is primarily used for receiving the enrolment data batch files and serving the same to the UID application for further processing. The protocols supported are Ftp, secure ftp, ftp/https.

g. CIDR MZ Deployment Architecture

The edge switches in DMZ are directly connected to the central core switch which connects all the applications.

(i) There are separate server farms for UID applications, deduplication engines and management applications.
(ii) All the applications are connected by a highly available network.
(iii) The SAN switch connects the SANs to the applications
(iv) Management network is separate from the data network.
(v) Backup & restore function is also connected to the same network.
(vi) Each de-duplication engine from a vendor is deployed behind its own firewall.

h. Management Applications

(i) Management Servers

The management servers are listed below:

1) Service Desk used for Change Management, Problem/Incident Management
2) Management Servers for Server, Network, Storage Management
3) Identity and Access Management Server
4) Servers and Equipment for Backup and Restore
5) Servers used for Logging and Auditing
6) Servers for Asset Management
7) Any other servers in the Operations Center

i. Database Servers

Please refer to Database Architecture Section. There are various databases and file systems which will be using their own servers

j. Backup servers

Backup servers are used for the backup and restoration applications which in turn are used for backing up the file systems and databases.

k. DC Infrastructure Services

This section describes servers associated with DNS, NTP, RADIUS, TFTP, and Replication Server.

l. DNS

This is a well known service used for IP address management. It resolves a UID domain name to an IP address.

m. NTP

NTP is a well known protocol is used for clock synchronization across the UID system.

n. RADIUS

RADIUS servers use the AAA concept to manage network access. AAA stands for “authentication, authorization and accounting”.

RADIUS serves three functions:

(i) to authenticate users or devices before granting them access to a network,
(ii) to authorize those users or devices for certain network services

and

(iii) to account for usage of those services.

o. Trivial File Transfer Protocol (TFTP)

TFTP is typically used at the startup time of a diskless device, workstation, and computer to transfer a boot image. It is also used to transfer small amounts of data between hosts on a network.

p. Replication Server

In the UID system as part of the DR strategy, a replication server may used to synchronize the DR site with Primary DC data. This is a Highly Available server with its own large storage and keeps track of the replication with Replication Manager Software.

Different Databases have their own Replication Manager software.

More information on the role and configuration is available as part of BCP/DR document for the UID system.

q. Logistics Support Servers

(i) Messaging Servers

The Messaging Server is mainly meant to send to mails out to Applicants, Registrars etc. It mainly supports SMTP with POP3, IMAP and HTTPS protocol support. The Logistics support will involve file replication server to Regional Offices for printing. In addition Printing and Mailing can be part of the logistics support both at CIDR and Regional Offices.

(ii) SMS Gateway

This gateway is mainly meant for receiving SMS and sending SMS messages. On the SMSC side it supports SMPP, CIMD protocols and on the DC side it supports SMPP, SMTP, HTTP and FTP protocols.

(iii) Replication Server

Replication Server is used to replicate UID information to regional offices so that they can be printed and issued to respective applicants.

(iv) Print services

The CIDR can also host an array of print servers and printers & associated equipment so that UID can also be mailed from the central location.

(v) Server Hardware

The server hardware is based on the following configuration:

1. 64 bit hardware
2. x86 based architecture
3. blade servers multi-processors, each processor having 4 or more cores, memory of upto 4 GB per core
4. Redundant SAN connectivity (4/8 GBps) from each blade server
5. 1 Gbps connectivity for Management and 10Gbps for Data
6. Ethernet Switches/SAN switches within Chassis to optimize the Rack to External cabling and connectivity

2.6.1.4. Storage

a. Intent

This section of the document describes the storage architecture for the UID system.

b. Overview of Storage Architecture

Storage is one of the key components of CIDR Infrastructure where all the critical data is stored. Storage cost increases with data growth. It not only impacts the hardware costs but also manageability costs. Storage has to be architected, designed to meet the business requirements.

The CIDR storage Infrastructure is used to Receive, Process, and Store enrolment data for processing the UID and other associated applications/tools. The present storage solution caters to 10cr enrolments and can scale as business grows.

The proposed storage architecture is based on unified storage solution. The unified storage solution should support FC/ISCSI and NAS. The unified storage solution should support tiered storage to map the storage solution with the business requirements. The proposed storage should support native snapshot, snap clone and storage data replication features. The storage solution should capable to provide synchronous and asynchronous replication across IP and Fiber Channel networks. The storage array based solution should provide host/server independent replication for optimal Disaster Recovery operation.

c. Data Centre Storage

The proposed storage solution has embedded unified storage and is host/operating system independent. The storage solution supports NFS, CIFS protocols as required for various compute environments as per business demand. The storage should be capable of supporting the tiered model for cost

optimization and able to support the thin provisioning. The Storage Subsystems should support industries leading vendor Storage Management Solution and provide global view of storage and associated devices.

The storage solution is designed and built on the storage architecture principles as defined. The storage solution is able to provide protection against disk failures, controller, Storage Operating System (High Available Ready) and its associated features and functions. The storage solution should capable of providing online upgrade on all elements of SAN.

Storage subsystems are capable of provisioning and housing multiple types of disk based on business requirement (example – SATA for low performance, FC/Solid state disks for high performance storage) and data type. The storage solution is capable of staging/cloning features as they needed for data backup and data replication. Security has been implanted in every element of the storage solution/ architecture.

The proposed storage solution supports the individual system, clustered, cloud environments, applications and operating system as per business demand. Storage should support on demand storage and through put using various RAID technologies as business demands and also provide protection against failure. Storage system should support dual protection and also hot standby for protection against multiple failures. The system is not a fool proof but provides protection. The storage system should support all applications and platforms as per CIDR business demands. The storage should be scalable as business demands and may scale in Peta Bytes.

As per business requirement replication software is either host based or storage controller based on the business and application requirement and storage system should be capable of supporting.

The present design contains the multiple islands of SAN/Storage based on the business or functional isolation/segregation. The storage needs have been classified based on performance, security and data retention.

The present proposed Storage Area Network (SAN) device acts as interconnect between storage and System. The proposed network architecture is embedded with unified data and storage elements as well Fiber Channel based storage. The present Storage Networking devices are high performance and highly scalable. The present Storage Networking devices are capable to meet the stringent Data Centre requirements like

(i) High availability
(ii) Security
(iii) Scalability
(iv) Ease of management
(v) Transparent integration of new technologies

Storage Networking should support the 1/2/4/8 Gbps Fiber Channel and as well as 10 Gbps technology. The storage networking should be capable of supporting logical and modular architecture. Storage Networking provides the logical

partitioning of the network to provide the security and isolation between environments. The storage networking devices should provide port level, zone level access controls to protect UID data. Storage Fabric should be expandable and scalable as needed. The storage networking solution should provide the FCIP/FC based data replication or mirroring of data without any data loss/corruption. The storage systems provides the replication/mirroring monitoring framework and operation framework for start, stop, reinitiate as required the mirror/replication operation using a GUI based tool selected by UIDAI.

Based on the business requirements storage have been classified as listed below:

(i) DMZ Raw Storage
(ii) DFS Raw Storage
(iii) Operational Data storage
(iv) De-duplication high performance disk storage
(v) Staging disks for backup
(vi) Staging disks for replication
(vii) Management Data Storage
(viii) Regional Data Centre Storage(Facilitation Centre Storage)

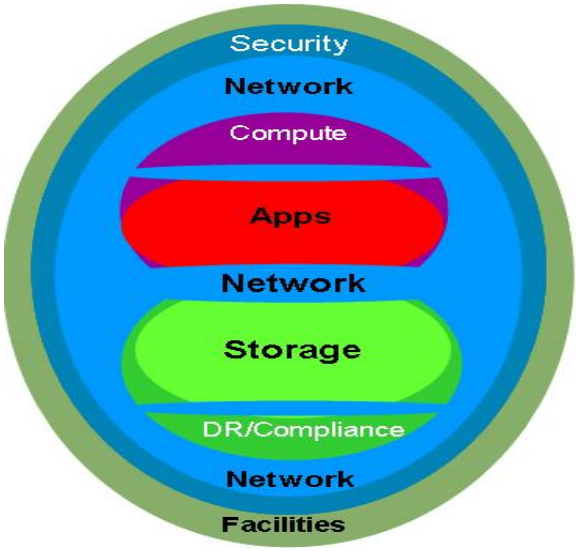


Figure 4 Storage overview

The CIDR Data Center will have combination of Storage Area Network (SAN), Network Attached Storage (NAS) and local storage. The storage solution should be flexible and transparent to the users of the storage in meeting the capacity requirements. Solution should be expandable as business demands must be implemented at every component level of the storage to meet the requirements of continuous availability of the UID application.

The above figure indicates the overall storage overview and depicts the storage at CIDR. Storage at CIDR is at the core of the CIDR with layered approach. This ensures the security, availability and manageability as required. It also shows various relations with other critical components of the CIDR and their relations

d. Storage Requirements

i. DMZ Raw Storage

DMZ raw storage represents temporary storage area for storing incoming raw enrolment data. The temporary storage is designed to store at least 5 days of data.

ii. DFS Raw Storage

Distributed File System storage stores multiple copies of decrypted and validated raw image data of enrolments. Two copies of decrypted and validated enrolment data will reside in the DFS Storage SAN.

iii. Operational Data Store

The Operational data store stores internal form of biometric data in the databases. These databases reside on the Operational Data Store SAN.

iv. De-duplication high performance disk storage

De-duplication high performance disk storage stores the data to implement enrolment and authentication processes of the UID application.

v. Staging disks for backup

This represents temporary storage for backup.

vi. Storage system

1. LUN (Logical Unit Number) configuration should be flexible and support thin provisioning. The LUN provisioning should be GUI based and can support various capacities as per business demand.
2. Storage should support Dual/Multiple paths to storage Networking and should be grown as business demands and should include large physical memory for cache
3. Storage systems should be of high capable, high performance, high available devices at every element of the storage system
4. Support for configuration of multiple raid types co-existence within the same array and also provide the security between each and every host as per business requirements
5. Support configuration for zoning/logical partitioning of the storage network and provide the inter zoning routing

6. Support Fabric, Switches, Tape Libraries, Host servers, Host Bus Adapters and comprehensive network adapters from industry leading vendors

vii. Availability
   1. No single point of failure
   2. Support hot swappable disks, power supplies

viii. Redundancy
   1. Support for Redundant power supplies, batteries and cooling fans
   2. Support for Redundant controllers
   3. Support for Redundancy at network switch level
   4. Support for Redundancy for host bus adapters
   5. Support for load balancing along with fail over among multiple data paths should be supported on multiple operating systems

ix. Upgrade
   1. Support for Firmware upgrades for storage components without any downtime for the UID application and servers accessing the storage

x. Data Protection
   1. Support for Storage to storage replication and snapshot backup methods
   2. Support for Tape backup methods
   3. Support for point in time copy and full volume copy for storage arrays.

xi. Performance
   1. Use of Cache for performance optimization
   2. Storage configuration should support performance based on file system, distributed file system, databases and other users of the storage

xii. Virtualization
   1. Support for virtualization methods

xiii. Interoperability
   1. Storage solution should support multiple operating systems – Linux, AIX, Windows, HP-UX and Solaris and clustering methods
   2. Support for backup and restore methods for different databases like – Oracle, MYSQL,
   3. Support for backup and restore methods for distributed file systems
   4. Support for backup and restore methods for file systems
   5. Support for data replication for multiple storage vendors in both synchronous and asynchronous modes

6. Should support storage solution from multiple vendors for NAS, SAN and local storage

xiv. Security

1. Implement security policies to prevent unwanted access from unauthorized systems and users
2. Support for data encryption to secure data

xv. Technology Stack

The technology stack components used are listed in the following table.

Technology mappings to architecture elements	
Architecture element	**Technology mapping**
Operating System	Redhat Enterprise Linux virtual machines hosted on Redhat Enterprise Virtualization platform
Language Runtime	Sun JDK 1.6.0
Message Oriented Middleware – Publish/Subscribe, Queues, Message persistence	RabbitMQ – provides high throughput messaging, distributed deployment across data centres and availability, reliability options like message persistence and transaction support
Application Container – manage business components implemented as POJOs	Spring Framework – provides lightweight container for Java objects, Security via Acegi, AOP, Remoting, and implementation of Dependency Injection for better maintainability
Enterprise Service Bus – declaratively chain components, multi-transport support	Mule ESB – Integrates well and runs inside Spring, Implements the SEDA model suitable for event driven applications like UID enrolment server
RDBMS Persistence – storing relational data	MySQL – SQL compliant and replaceable with equivalent open source or commercial alternative
Distributed File System persistence – storing huge biometric and audit records	Hadoop Distributed File System (HDFS) – supports deployment on Linux and on commodity grade disks
Large storage	SAN using commodity disks
Compute Grid – Parallel processing of compute intense task on large clusters of low capacity machines	GridGain – supports easy set up and use of a compute grid. Integrates well with Spring and other frameworks in the stack
Batch Processing – execution of scheduled and repeating jobs like File processing and re-submissions of failed enrolment packets	Spring Batch – elaborate framework managing jobs, steps within jobs and tasks within. Provides support for file system read-write jobs
Application monitoring – gathering and publishing application health parameters to monitoring systems	HypericHQ – provides Java based agents that may be embedded into application runtime for gathering application health parameters

2.6.1.5. Database

a. Intent

The applications hosted by CIDR use a combination of online transaction processing databases for enrollment and authentication applications, data warehouses for business intelligence applications and distributed file systems for storing and quickly retrieving the raw enrollment images. Following sections briefly describe the data stores (data bases) and outlines their requirements for CIDR applications.

b. List of Datastores

The UID application datastores are broadly classified into,

(i) DMZ Data Storage
(ii) UID Application databases
(iii) Biometrics databases
(iv) Management databases

c. DMZ Data Storage

DMZ storage uses file system to temporarily buffer the incoming batches of raw enrollment data. The DMZ storage has to be sized appropriately to buffer up to 5 days of enrollment data. A regular File System is used to store the temporary enrollment data.

d. UID Application Database

i. Raw Image Storage is used to store multiple copies of raw enrollment images into a distributed file system. A Distributed file system is used for enabling multiple nodes to quickly retrieve and save the raw enrollment images.
ii. Relational Databases are used by enrollment and authentication applications. To support the continuous availability of enrollment and authentication applications, high availability solutions like Data Replication and Database Clustering will be deployed as part of these databases.
iii. Analytics DB will be used by Business Intelligence applications. Here data warehouses and data marts will be created. This will serve different users like Registrars, Sub-Registrars and enrollment Agencies and interested public to drill down and view the aggregated enrollment and authentication statistics

e. Biometric Application Database

The biometrics application will be supported by three vendor solutions in the beginning phase of the UID application. The UID application will be integrated with the biometric application using the Automatic Biometric Interface Solution (ABIS) interface.

2.6.1.6. Biometric Service Providers

a. Biometric Solution

The Biometric Solution Providers (or BSPs) will design, supply, install, configure, commission, maintain and support biometric components of the UID System. In CIDR there can be upto 3 BSPs operating simultaneously.

b. Two biometric components are utilized in the UID System. The biometric components are:

i. Automated Biometric Identification Subsystem (ABIS): ABIS will be used in the Enrolment Server as a part of the multi-modal biometric de-duplication solution. In the early release, ABIS will also be used in the Authentication Server for verification. The ABIS will maintain its own database of proprietary fingerprint and iris templates for de-duplication (and face templates at the discretion of the vendor), and must be able to respond to verification requests accompanied by fingerprint and/or iris images, as well as ISO/IEC 19794-2:2005 format fingerprint minutiae files. Vendors will work with the UIDAI to provide further specification within 19794-2 to promote interoperability with future verification clients.

ii. Multimodal SDKs: SDKs will be used in the enrolment client, manual check (for duplicates), authentication server (for later releases) and the analytics module. The SDK may contain signal detection, quality analysis, image selection, image fusion, segmentation, image pre-processing, feature extraction and comparison score generation for fingerprint, iris and face modalities.

- The biometric solution components used in the UID system are:
- Multi-modal de-duplication in the enrolment server
- Verification subsystem within the authentication server
- Enrolment client
- Manual checks and exception handling
- Biometric sub-system monitoring and analysis

c. The functional requirements of the five areas are described, followed by the overall functions of the two biometric components.

a. UID System Requirements of the biometric components
b. Multi-modal Biometric de-duplication in the Enrolment Server

Considering the expected size of the de-duplication task, the UID enrolment server will utilize:

1. Multi-modal de-duplication. Multiple modalities – fingerprint and iris will be used for de-duplication. Face photograph is provided if the vendor desires to use it for de-duplication. *While certain demographical information is also provided, UIDAI provides no assurance of its accuracy*. Demographic information shall not be used for filtering during the de-duplication process, but this capability shall be preserved for potential implementation in later phases of the UID program. Each multi-modal de-duplication request will contain an indexing number (ReferenceID)[1] in addition to the multi-modal biometric and demographic data. In the event one or more duplicate enrolments is found, the ABIS will pass back the ReferenceID of the duplicates and the scaled comparison scores upon which the duplicate finding was based. The scaled fusion score returned with each duplicate found will have a range of [0, 100], with 0 indicating the least level of similarity and 100 as the highest level of similarity.
2. Multi-vendor. Multiple complete multi-modal solutions from more than one vendor will be used as shown in Figure 5. The UID Application will determine routing of a particular de-duplication request. It may determine to route a particular de-duplication request to more than one biometric solution. If it routes a de-duplication request to more than one solution, it is responsible for determining the final outcome of the de-duplication request. In other words, fusion of the scores across the multiple ABIS is not within the scope of this RFP. The UID ABIS API specifies the interaction between UID Application and ABIS.

   The middleware included in the UID application (being developed by ASDMSA) is meant to provide vendor independence and standardization. The key features of the middleware is

   a. Routing and mediation.
   b. Guaranteed delivery
   c. Fault tolerance and load balancing
   d. Open standard based messaging (AMQP) using open source RabbitMQ
   e. Transparent connectivity to analysis and system monitoring modules of UID applications
   f. Support of web 2.0 based UID ABIS API and CBEFF data format standard

[1] ABIS will not be aware of the UID #, nor will it be aware of how UID #maps to reference ID or records in the reference DB.

g. Encapsulation and isolation of ABIS components

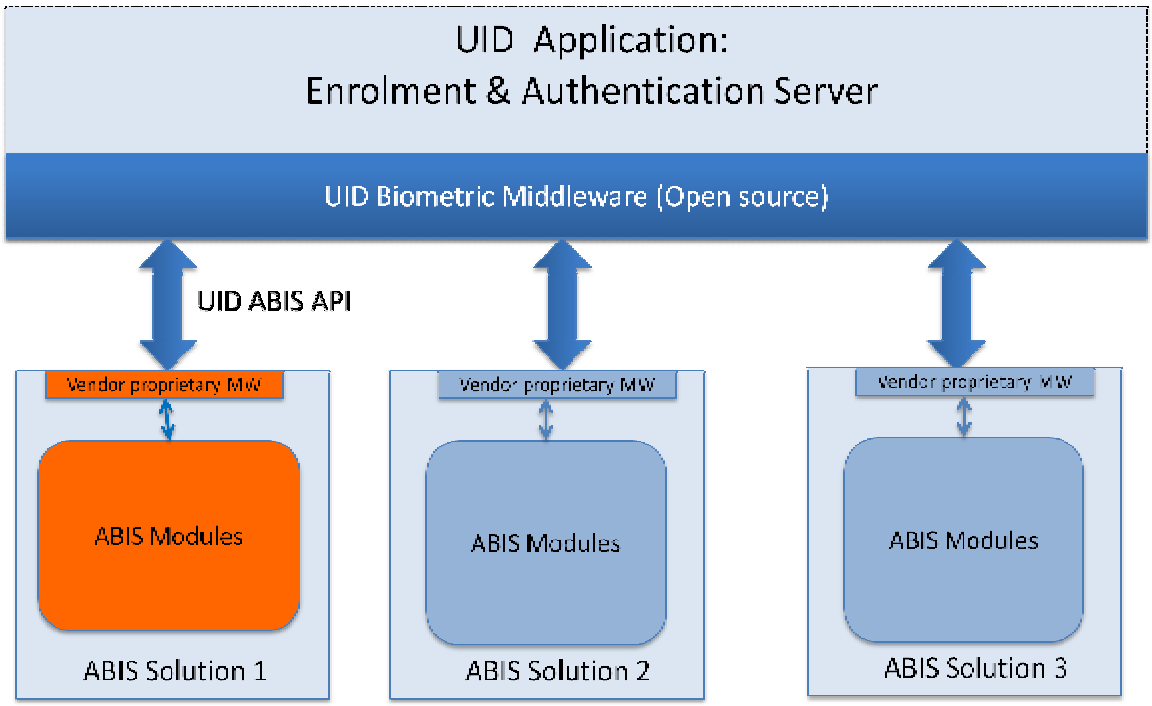


Figure 5 UID Application and ABIS Integration

c. Verification Subsystem of Authentication Server

In the first release of the UID server, the biometric verification module, as shown in Figure 6, provides verification *within* the authentication server. The solution should be capable of 1:1 verification comparisons of enrolled references with incoming ISO/IEC 19794-compliant fingerprint, iris or face images or 19794-2 compliant fingerprint minutiae sets without proprietary extended data. Figure below illustrates both the verification and de-duplication subsystems to be supplied by the BSP.

For the purpose of distributed authentication by UIDAI at a later stage, the biometric verification module may be constructed using SDK. While the functionality of the verification subsystem will not change, the internal architecture may change. The templates will be maintained in memory resident database by the UID authentication server application (not in scope of BSP). If the incoming requests contain a biometric image, the Authentication server will use SDK to extract the feature. SDK will also be used to generate comparison score of the sample. The decision for distributed authentication will rest with UIDAI and will be binding on the BSP

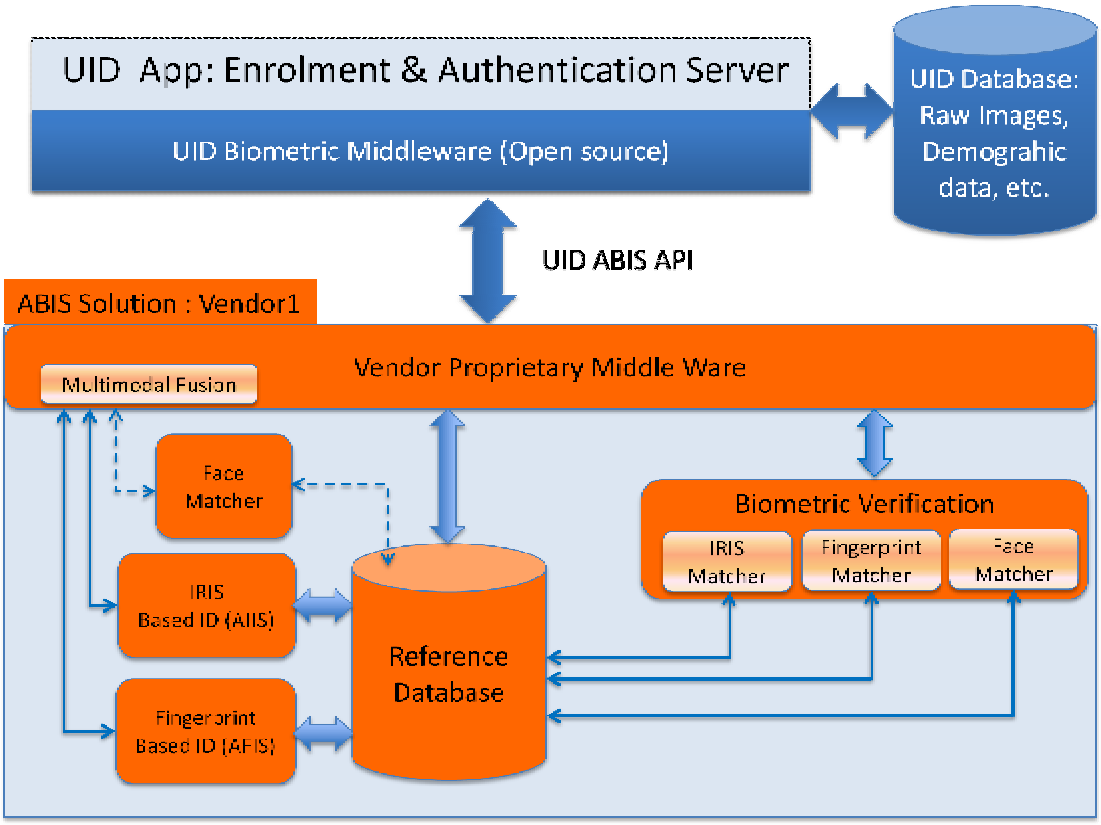


Figure 6 ABIS Solution

2.6.1.7. Analytics

The Business Intelligence Application intends to serve the following segments of the users

- Managed Service Provider - The Provider who manages the software operations, maintenance and providing services to the partners and registers for capture, Generation and Authentication of UID.
- Partners and Registrars
- General Public
- External Application developers
- Statisticians and Analysts
- Users within UIDAI

a. Primary Goals

Given the mandate of the UIDAI, the product must serve the following needs:

- Make the aggregated data accessible for Public use under RTI act. However the PII data will be completely **inaccessible.**
- Provide comprehensive Analytics and reports for the Service Providers of UID

- Provide comprehensive Analytics and reports for the UID regulatory body.
- Provide comprehensive Analytics and reports for the general public.

In addition the product also seeks to achieve the following:

- Provide an extensible infrastructure platform to deliver the above goals.
- Provide an custom data model to meet the needs of UIDAI and its stakeholders reporting needs

b. Secondary Goals

Consistent with the primary goals of the product, the product also seeks to provide for the satisfaction of the following secondary goals

- Provide basic and advanced metrics regarding the progress and status of the overall project
- Provide relevant metrics with appropriate actionable workflows that weeks to address issues identified by a metric or a group of metrics as a whole
- Provide appropriate levels of security to access of information desired across various user group segments within the UID ecosystem
- Provide a web based information portal for the delivery of all such information

c. Other Considerations

Other consideration that may come into the purview of this system would be the following

- Archival and restoration of prior period transactional type information
- Any other requirements to satisfy needs of the Right to Information Act

d. Exceptions

The proposed Analytics and reporting system will not extract or hold any data relating to resident demographics, biometric fingerprints or iris scans

The Proposed implementation architecture for UIDBI shall consist of the following components.

i. **UIDBI Atomic Data Warehouse consisting** of atomic data obtained synchronously or asynchronously from the UID-Server, time-variant, consolidated, aggregated minimally to provide such information for downstream needs, such as data marts, Charting applications, sandbox etc.

ii. **UIDBI Data marts** consisting of subject area specific or other subsets specific data derived from the UIDBI data warehouse through a process of aggregation, along with relevant dimensionality

iii. **UIDBI EAI** consisting of tools and applications to provide for extraction of data from source systems into the UIDBI Data Warehouse

iv. **UIDBI Analytical and reporting delivery platform** consisting of tools and platform to deliver all relevant metrics, dashboards, portals, reports, action-response work-flows etc.
v. **UIDBI Metadata layer** consisting of tools to define, maintain and browse the definitional layer of the UIDBI through its complete lifecycle. This needs to be revisited based on the toolsets capability to provide for such capability.
vi. **UIDBI security and administration layer**, integrated with the UID main security and administration layer inclusive of ACLs
vii. **UIDBI Sandbox** to provide secure downloads from the UIDBI Database for purposes of advanced analytics and modeling
viii. **UIDBI Data distribution platform** used to provide data in various forms for use by internal and external applications.

e. Overview Of The Proposed Solution Architecture

UID requires a highly scalable, n-tier, reliable and open technology components to meet the UIDBI requirements.

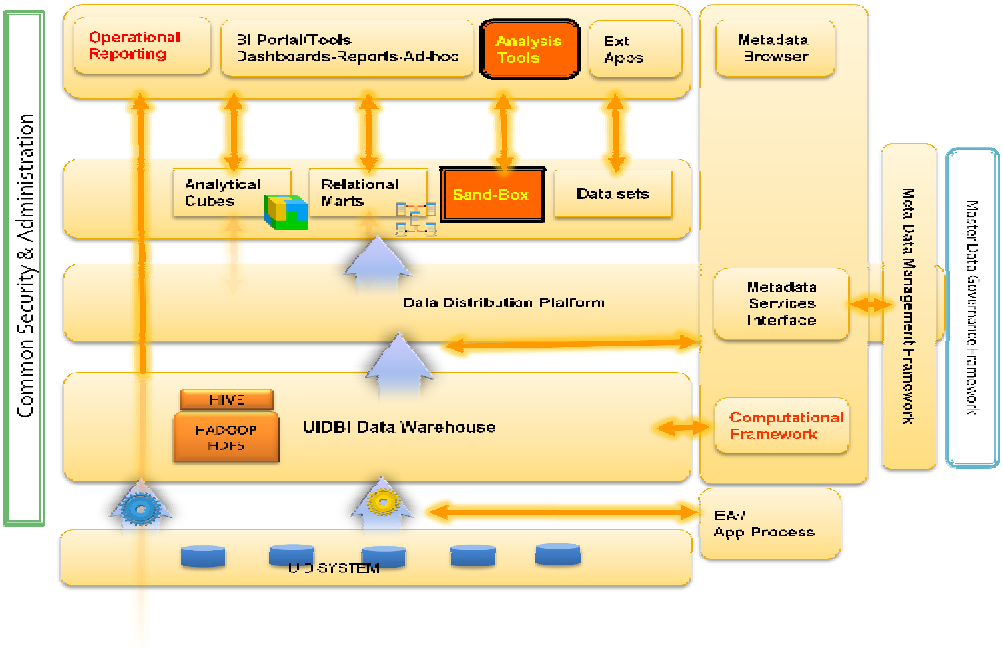


Figure 7 UID Analytics and Reporting Subsystem

f. Analytics and Reporting

The UID - Analytics and Reporting subsystem (UIDBI) provides an extended set of metrics to monitor the progress, usage and status of the UID ecosystem. The output is proposed to be delivered as a distinct set of metrics

through various portals viz. Partner portal, Public information portal, Data portal etc..

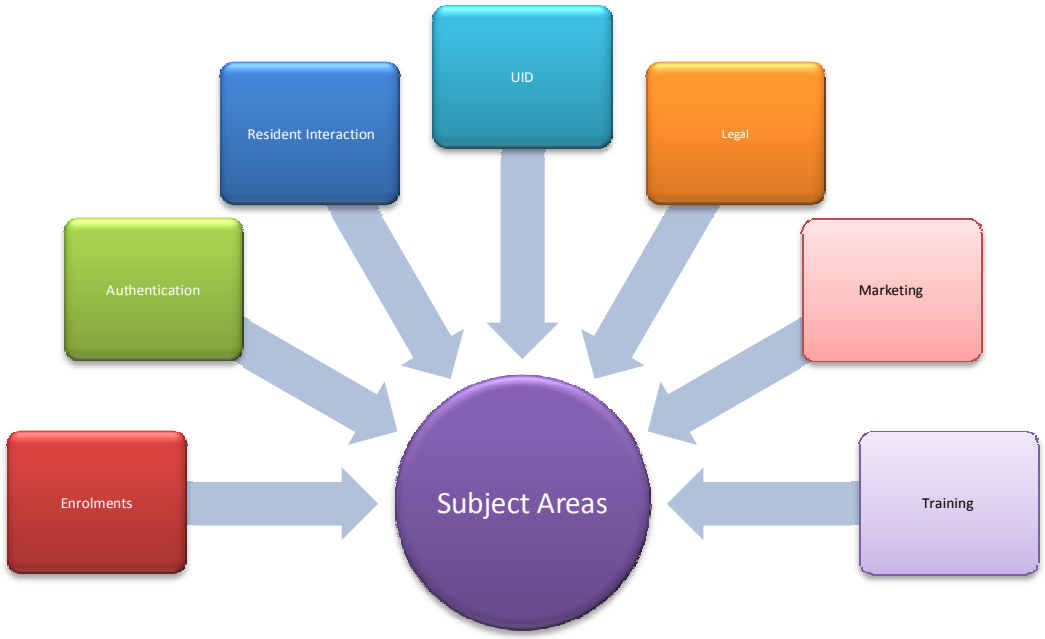


Figure 8 UIDBI Subject Areas

g. Information Portal

The information portal will provide an overall dashboard to track the performance of the UID system, in addition to providing a variety of standard reports. This is divided into the following portals.

i. Partner Portal

The UID project is based on a partnership model consisting of Registrars and their respective enrolling agencies on the ground. There are other entities such as device suppliers, trainers, letter delivery agencies, pre-enrollers etc all of whom play an important role in enrolling 1.2 billion residents. The partner portal will cater to the needs of the partner community.

This portal will provide them with overall statistics for use cases that involve them, as well as allow them to track individual cases.

These users will be able to track:

- Administration, and User management – creation / deletion of the user records
- Aggregate Pre-Enrolment stats for them – number, latency, validation issues. (for Registrars, Sub-Registrars, and Enrolment Agencies)

- Aggregate Enrolment statistics for them – number, latency, approvals, rejection reasons (for Registrars, Sub-Registrars, and Enrolment Agencies)
- Aggregate Authentication statistics for them – number, latency, success / failures (for authentication clients)
- Track individual resident cases – pre-enrolment, enrolment, and authentication – that they are involved in.

ii. Public Portal

The UID being a project of national importance will need to continually share various design, development, implementation and operational aspects with the public. The grievance redressal system needs to also be integrated into the public portal in order to redress complaints and grievances faced by residents in the process of enrolment or authentication. The UID information portal will address the above needs. This portal will also provide all users with information about the UID system, and allow them to drill down on the performance by region, etc. It will not allow users to track individual cases.

However, a method will be provided to get in touch with the UID for specific questions, as well as addressing grievances.

All users will be able to see:

1. List of Registrars, Enrolment Agencies, etc.
2. Number of UIDs issued by time (day, month, year), and region (country, state, district, city)
3. Performance Metrics – At an aggregate level – the number of Registrars, latency to allocate UIDs, number of complaints, etc.
4. Authentication requests – count, latency, success / failures.
5. Grievance requests filed with the UIDAI, and the responses.

iii. Data Portal

We want to expose all publishable public information through a “Data Portal” where all data is exposed in machine readable formats. This portal allows 3rd party developers to develop web 2.0 applications based on this data.

2.6.1.8. External Interfaces

a. Registrar System

Registrars will have their own IT infrastructure to interact with Aadhaar System. The functionalities include

- Getting updates during enrolment process -
- Uploading bulk demographic data
- Act as an AUA

As we have seen earlier, a copy of the enrolment data flows from the Enrolment Stations to the Registrar System. The CIDR also updates the Registrar System with the assigned UIDs.

In order to keep the confidentiality of the data being sent to the registrar system, the data will be encrypted using the public key provided by the registrar. It follows that the Registrars have to manage their <Private Key, Public Key> pair securely and put the necessary infrastructure in place. The interacting Registrar systems have to be hardened. UIDAI may provide security guidelines to Registrars to assist in the implementation but the ownership will always reside with the Registrars.

UIDAI will define interfaces for the Registrar System to interact with CIDR. There will be no libraries to be integrated with. Since the Registrars also maintain a copy of their enrolments data, they have to take enough precautions to secure the data.

In order to integrate Aadhaar authentication with applications like PDS, NREGA or similar applications in private sector, UIDAI will provide a library of API using which the new applications can be developed and deployed. Please see the figure under the section ‘Authentication User Agency’.

b. Logistics

Logistics service will be provided by Department of Posts. As shown in Figure 9 , there are two parts to this.

(i) Inbound Logistics – to receive the raw enrolment images + data in magnetic media and through the network from the Regional Offices or Facilitation Centers. All the incoming data is processed by the CIDR DMZ Application.
(ii) Outbound Logistics – Delivering the UID to applicants and getting the Status Update

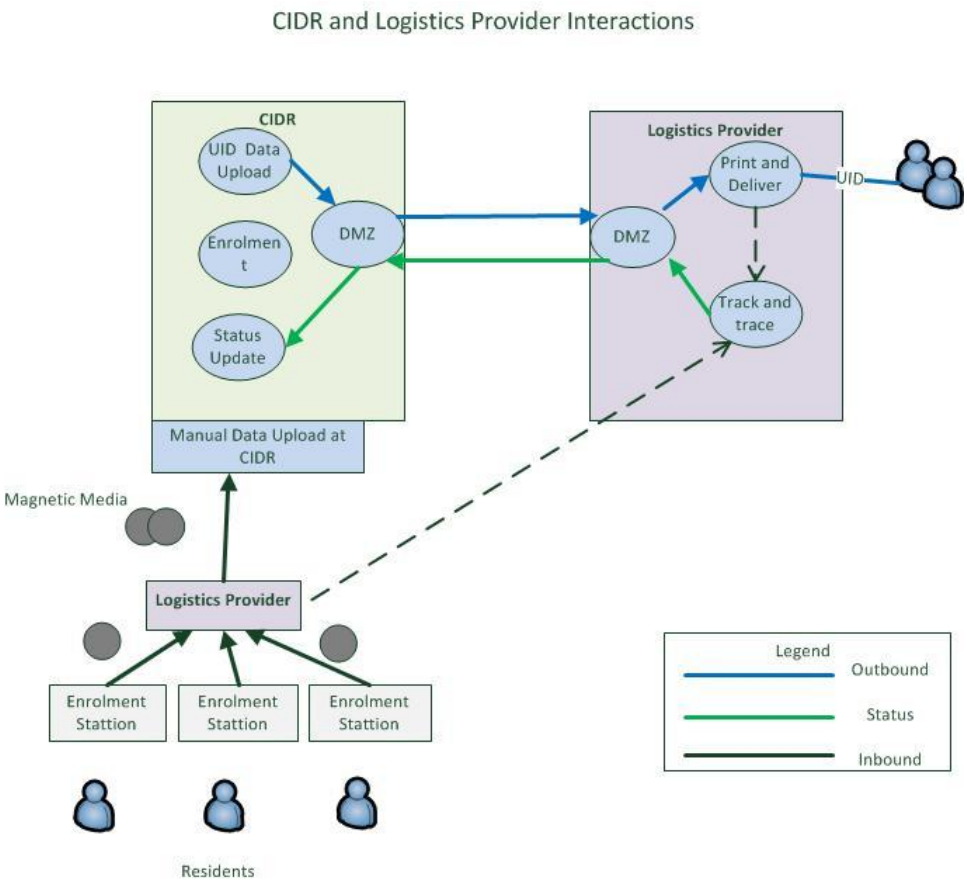


Figure 9 CIDR and Logistics Provider Interactions

Responsibilities of Logistic Service Provider includes,

i. Logistics setup for enrolment agencies to send the enrolment data/manifest to the RO/data centre.
ii. Provide printing infrastructure and connectivity to the CIDR. The printing infrastructure electronically receives the UID allocation letter to be printed and mailed to the enrolled residents.
iii. Mail the printed UID letter to the enrolled resident.
iv. Provide an online track and trace system to track the status of the enrolments and UID generation.
v. Support the call centre provider to track the enrolment status.

c. Authentication User Agency

Authentication User Agencies (AUA) are responsible for handling and processing authentication requests from service providers. Before providing a service to a resident the service provider needs to verify authenticate the identity of the resident. It forwards the authentication request to an AUA which contacts the CIDR which finally verifies the identity. The local service provider

finally delivers the requested service following the authentication. This AUA ecosystem is described in the following figure:

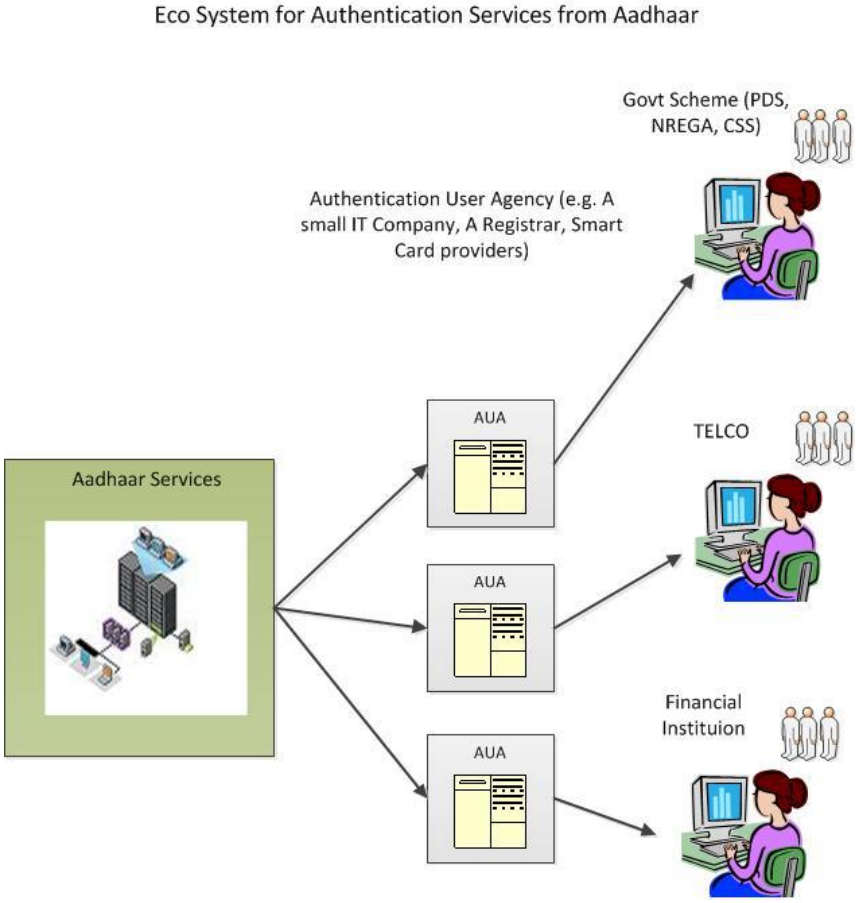


Figure 10 Aadhar Authentication eco system

d. Contact Center

The Contact Center provides a central point of contact to residents and other entities that will partner with UIDAI during the enrolment and post enrolment stages. The Contact Center will provide services in multiple languages for residents, registrars, enrolment agencies and resident service agencies.

The Service Provider for Contact Center will setup, operate and maintain the contact center including the agents. The Service provider for Contact Center will be expected to,

- Scale operations at the required pace to match volumes of interactions
- Provide analytics support to UIDAI
- Assist in driving performance improvements
- Take end to end responsibility of driving resolution of queries and services

- Analyze the various interactions with the stakeholders, identify and develop process models

The RFP for Contact Center contains the detailed requirements for Contact Center. Please refer to this document from UIDAI website. UIDAI has selected Intellinet as the service provider for setting up and operating the Contact Center.

The Contact Center Architecture diagram is shown in Figure 11 .

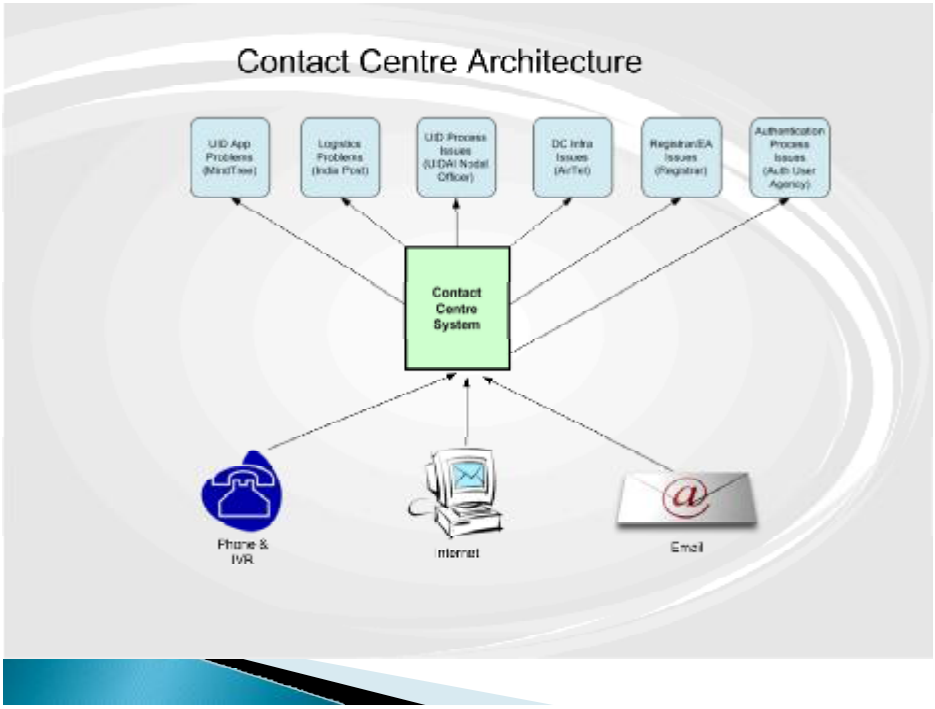


Figure 11 Contact Centre Architecture

e. Eco system Stakeholders

i. Registrar Management

Registrars are public and private organizations who are currently engaged in providing services to the residents, and who operate on behalf of the UIDAI to provide UIDAI services (such as enrolment) to their constituents. Example profiles of registrars include state governments, ministries and departments in the central government, banks and other financial institutions, telephone companies, etc.

Registrar Management includes,

- Providing Training for performing enrolment and authentication services
- Signing MOU with new public and private organizations
- Providing System and Connectivity to perform enrolment and authentication services
- Handling complaints from residents
- Handling accounting and billing

ii. Enrolment Agencies Empanelment

The widespread implementation of the UID project needs the reach and flexibility to enroll residents across the country. To achieve this, UIDAI is partnering with a variety of agencies and service providers (acting as Registrars, Sub-registrars and Enrolling Agencies) to enroll residents for UID.

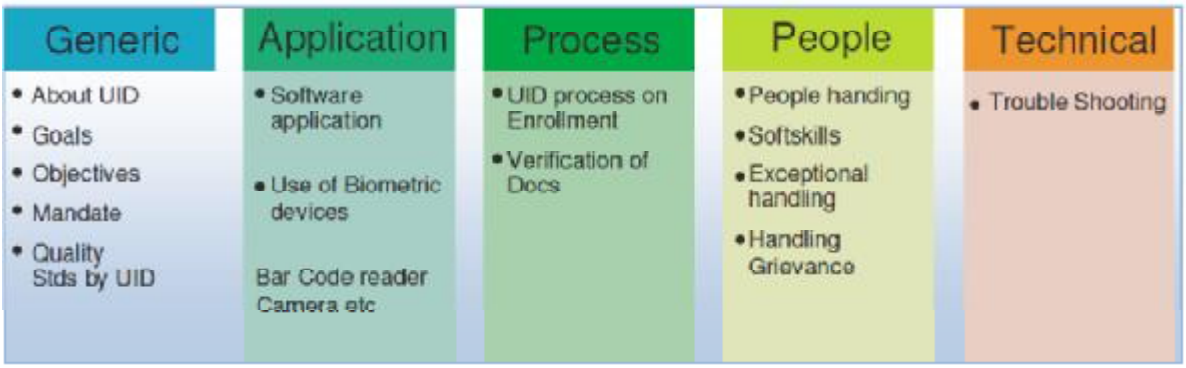
The enrolling agency is responsible for,

- Procuring biometric devices as per UIDAI specifications
- Setting up of enrolment stations and enrolment centres
- Hiring and Training manpower for enrolment
- Conduct enrolment operations as per standard processes specified by UIDAI
- Send enrolment data to registrar
- Ensure Security and Privacy of enrolment data
- Provide electronic reports on enrolment status daily

iii. Training Agencies

Persons involved in the enrolment process at the field level must be trained thoroughly to accomplish the job of enrolment. Similarly the supervisors of the enrolling agencies and the representatives of the Registrars who will be involved in the UID enrolment should also be sufficiently trained to ensure data-quality , especially of the biometric data which is the basis of de-duplication of biometric attributes of residents. As the number of enrolments is going to increase in the next few years, there will be a huge requirement of trained personnel.

A outline of the proposed modules and topics to be covered under the Training is given below.



The UIDAI proposes to create an eco-system of training agencies and capacities in the country so as to provide manpower needed for enrolment. Currently, the selection for training agencies is in progress.

Please refer to the detailed requirements for Training Agencies from UIDAI website.

f. Device Certification

The devices used for Enrolment, Authentication, Micro ATM and other UID functions should comply with the standards set by UIDAI. The Device Certification process includes,

- Devices used for enrolment and authentication are capable of delivering the outputs as specified by UIDAI
- Ensuring devices are robust enough to be used in different climatic conditions
- Check whether the device software has necessary application programming interfaces
- Ease of integration with demographic software used by UIDAI

The Standardization Testing and Quality Certification (STQC) have been selected as the Biometric Certification Agency for certifying biometric devices to comply with the standards set by UIDAI.

The device manufactures or suppliers who supply biometric devices for UID enrolment and authentication have to be certified by STQC.

- Enrolment Devices
- Authentication Devices
- Micro ATM
    - Financial Inclusion

g. Information Security

Protecting the Unique Identification Number (UID) and the supporting resources is of at most importance since the misuse of the system can render the system ineffective. Apart from protecting the UID number adequate security should also be extended for the technology and the processes surrounding them to provide a holistic view of security of the UID system.

The following diagram highlights the touch points of the UIDAI system with residents. At each of these points, the UID has the possibility of gathering data, and providing services to the residents. These touch points are also important from a security perspective, as these represent the points at which external security threats could emanate, and each of these becomes a threat zone.

Figure 12 UIDAI System touch points

h. Information Privacy and Data Security

The UIDAI is collecting, what is generally described as Personal Identifiable Information (PII). As a consequence, it is advisable that we clearly and publicly state how this data will be used, and how we will protect it from access. This section should guide the architecture, as well as be the basis for this external messaging. For the sake of clarity, this section contains information that is spread throughout this document.

Even as the UIDAI stores resident information and confirms identity to authenticating agencies, it will have to ensure the security and privacy of such information.

By linking an individual's personal, identifying information to a UID, the UIDAI will be creating a transaction identity for each resident that is both verified and reliable. This means that the resident's identity will possess value, and enable the transfer of money and resources.

The UIDAI envisions storing basic personal information, as well as certain biometrics. However, limiting its scope to this, and not linking this information to financial/other details does not make the resident records in the database non-sensitive. Biometric information for example, is often linked to banking, social security and passport records. Basic personal information such as date of birth is used to verify owners of credit card/bank accounts and online accounts. Such information will therefore, have to be protected. Loss of this information risks the resident's financial and other assets, as well as reputation, when the resident is a victim of identity theft. In the federated system that the UIDAI envisions, we must consequently have processes in place to ensure a fair level of data security.

The following security framework summarizes the set of measures required to protect the PII from theft.

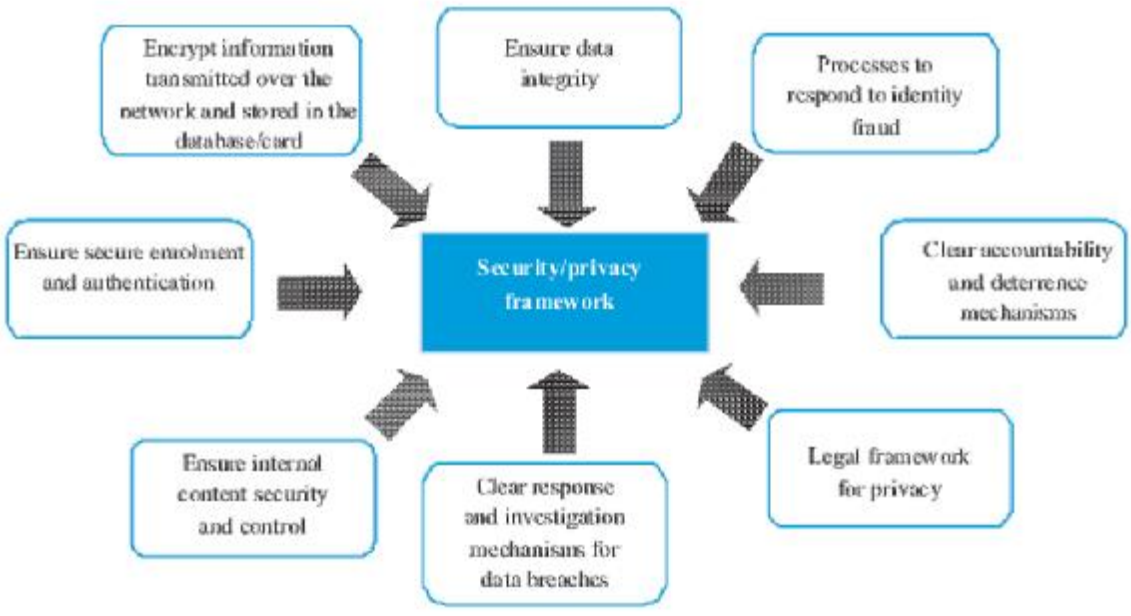


Figure 13 Security Framework

i. Collaborative Security Model

Working in a partnership model requires security to be met at each of the involved parties to provide an end to end security of the UID system. While security for the CIDR (Central ID Data Repository) will be the responsibility of the UIDAI, security of the UID connecting environment (application, networks, processes, etc) at each of the involved parties would be taken care of the respective agents. UIDAI would provide a governing model of security involving technology and processes to each of the partners participating in the UID system. All UID data deemed to be private and sensitive in nature would be provided adequate protection while in transit and storage both at UIDAI and at the agents involved with the system.

j. Defence in Depth

UIDAI would adopt a defense in depth strategy to provide multiple layers of defense to safeguard the UID system. This approach ensures relevant controls are implemented in the key areas including people, technology and process (operations) to secure the UID system and the accompanying environment.

Some of the salient features of the UIDAI's security model include

- Connectivity to the UID application for UID enrolment and authentication (Private Portal) would be provided only for agencies that have been previously verified and authorized by UIDAI.
- All operations affecting the resident's UID data including enrolment and modification would be carried out only with the resident's biometric data.
- The technology stack at the CIDR (Central ID Data Repository) will be supplemented with appropriate security controls including firewalls, IPS (Intrusion Prevention Systems), etc. Additionally UID may mandate similar controls for the agencies involved with the UID system.
- UIDAI's process and technology at CIDR would be standardized as per international security standards e.g. IS027001
- The UID application and the client libraries developed at the agencies involve security controls to mitigate against all risks as specified in the OWASP (Open Web Application Security Project) Top 10 flaws
- UIDAI may conduct process audits of the information that comes in from the Registrars, to ensure data quality and that agencies are following guidelines recommended by the UIDAI.
- UIDAI may propose stronger security controls for agencies involved in collecting and storing resident's supporting documents for obtaining the UID. These include electronic documents of resident's passport, ration card, voter's card, etc
- Personnel handling the information systems of the UID system have prior experience and are trained to safeguard the IT assets against risks.

While Privacy is considered to be the key security attribute of the UID system the other factors (Availability, Integrity, Authentication and non-Repudiation) governing the security of the UID system have also have to be given par importance to ensure a safe and secure UID environment. The security model adopted by UIDAI ensures that all these elements are adequately met at all layers (People, Process and Technology)

2.7. Overview of Managed Services and Scope of Work

2.7.1. The scope of work for the vendor shall span across the CIDR data centres of UIDAI proposed to be located in the National Capital Region, New Delhi and Bengaluru. **The data centre located in Bengaluru shall act as the primary data centre and the data centre in New Delhi shall act as the business continuity centre.** However the Data Centre at NCR (New Delhi) is to be converted into an active-active site in due course.

2.7.2. The scope of work shall broadly include the following:

2.7.2.1. Transition and documentation of the processes, procedures, designs, configurations of the setup at Bengalure DC from UIDAI Tech Team, ASDMASP, BSP. Replication the Bengaluru DC setup at NCR DC.

2.7.2.2. **Installation, Integration, Build and Commissioning** of the materials supplied at the NCR-DC for creation of an **integrated infrastructure solution** for the CIDR. The vendor shall depute staff in adequate numbers and with necessary skills to perform these tasks.

2.7.2.3. Provision of **managed services** for management and maintenance of the integrated infrastructure solution at the NCR-DC on a 24 x 7 x 365 basis for duration of **12 months from the date of signing of this contract with the successful bidder.** Maintenance, upgrade, enhancement and additional supplies on a need basis to ensure that Service Levels are met. The vendor shall provide adequate staffing with necessary skill sets for provision of these services.

2.7.2.4. Transition of the managed Services to a Managed Service Provider who will come on board as decided by the UIDAI.

2.7.3. The tenderer is expected to work in close co-ordination with the entities involved in the project to ensure the success of the project. The tenderer is also expected to manage relationships with all the vendors to provide a single point of contact for UIDAI for resolution of issues and problems.

2.7.4. In addition to the above scope of work envisaged in the following sections, the tenderer is expected to co-operate with UIDAI in critical situations to provide services beyond the established scope of work.

2.7.5. The following sub-**sections de**tail the nature of work to be performed in each of the areas. These details are illustrative in nature and are intended as guidance to the DCSP.

2.7.6. The bidder should make use of the best practices and past experience for providing adequate quality of service to UIDAI.

2.7.7. As part of provision of managed services the DCSP shall setup a Network Operations Centre and a Security Operations Centre.

2.7.8. **Server installation, hardening and management**: The bidder shall perform the following.

2.7.8.1. Server monitoring and management shall involve supporting the purchaser with managing the equipment hosted in the data centre. The DCSP shall also provide helpdesk support to the customer and send periodic reports on the equipment performance.

2.7.8.2. Server installation and hardening: Install the server Operating System as per customer specifications, Configure common items like network, Web Server, FTP Server, databases etc., install common applications on the server, One time activity of server hardening at the time of installation that includes patching up of all reported vulnerabilities in the server, operating system and standard applications, implementation of proper access control on the files and the system resources as per the security policy of the customer, ensuring that the server runs only on required ports and services as per the application requirements and blocking unnecessary ports and services from the server.

2.7.8.3. Port monitoring: Monitor HTTP/HTTPS, DNS, SMTP, POP3, FTP, TCP ports are continuously to ensure network and applications are up and running.

2.7.8.4. Remote hands service: Execute instructions on hosted servers such as server restart, service restart, minor configuration changes in OS, executing a script on the server, installation of software etc. Activities shall include service restarts in Windows Servers / Killing and restarting of processes on Unix/Linux Servers, rebooting of servers and clearing of log files.

2.7.8.5. Manage Operating System: This shall include support of Operating System, format and reinstallation of OS as requested by the customer, creation and maintenance of User Accounts, Start / Stop service, application of upgrades and patches provided by the OS vendor and approved by the customer, OS debugging and recovery, maintenance of

server logs, management of server disk space, addition or removal of Hardware or Software.

2.7.8.6. Installation of Virtualization Software: This involves installation of virtualization software (e.g. kvm) on the host OS so that guest operating systems can be installed.

2.7.8.7. Installation of special utilities: Some special utilities such as a Distributed File System, Services such as Mail Server, Internet Services etc. will be required to be installed on the servers,

2.7.8.8. Manage database system: This shall include installation and configuration of database server, support of RDBMS as selected by UIDAI, re-installation of database system as requested by the customer, performance tuning and optimization, user access management by assigning access rights, startup and shutdown of database system as requested by the customer, backup & restore, access control, maintenance of server logs and trace files, monitoring of Critical Database parameters, performing Import/Export of data, management of database space and database fragmentation, addition or removal of Hardware or Software, configuration and maintenance of Client Connectivity like JDBC, SQL Net 8 etc., RDBMS version upgrades and migration. Ongoing support for the application vendors to deploy applications, application patches, trouble shooting, performance tuning etc.

2.7.8.9. Manage load balancing: This shall include management of the load balancer hardware device, regular Health Check of the Servers using TCP or ICMP connections, limiting the number of connections per server for optimum performance, seamlessly adding servers as and when existing servers are over-utilized without disrupting services.

2.7.8.10. Implement and maintain standard operating procedures for maintenance of the infrastructure based on the policies provided by the purchaser and based on the industry best practices / frameworks like **ITIL**. Create and maintain adequate documentation / checklists for the same.

2.7.8.11. The bidder shall be responsible for managing the user names, roles and passwords of all the relevant subsystems, including, but not limited to servers, applications, devices, etc. The bidder shall be responsible for management of passwords for all relevant components and devices under his purview and implement a **password change mechanism** in accordance with the security policy of the purchaser.

2.7.8.12. The bidder shall be responsible for the installation and management of UIDIA application stack which includes the ASDMSA application and assocaited middleware and other software components

2.7.9. **Network management:** The bidder shall perform the following:

2.7.9.1. Network health check on daily basis

2.7.9.2. Monitoring and Management of Network equipments – routers, firewalls, switches, load balancers, SSL accelerators

2.7.9.3. Monitoring and Management of WAN/Internet links

2.7.9.4. Manage, backup and restore device configurations

2.7.9.5. Optimize performance of network devices

2.7.9.6. Ensure proper firmware patches and updates are applied

2.7.9.7. Review, updating and management of device policies

2.7.9.8. Regular reporting that includes real time report on network health status and trend analysis through customer portals.

2.7.9.9. The bidder should also co-ordinate with the VPN vendor for ensuring smooth routing of network traffic to the BCP site in case of disaster / drill.

2.7.9.10. The bidder should co-ordinate with the DC vendor in case of break fix maintenance of the LAN cabling.

2.7.10. **Security management**: The DCSP shall perform the following:

2.7.10.1. Setup a Security Operations Centre (“SOC”) for management of security related aspects of the CIDR IT infrastructure.

2.7.10.2. Implement the Information Security policies and procedures specified by UIDAI.

2.7.10.3. Monthly Vulnerability assessment: Assess server for vulnerabilities locally using automated scanning and manual assessment.

2.7.10.4. Implement system control, authentication and access policies and user practices to detect possibilities of an external and internal compromise due to flaws in system policies.

2.7.10.5. Identify and resolve weaknesses in configuration and settings that can lead to failure and weaknesses in implementation of access and sharing policy on server that can lead to disclosure of confidential information

2.7.10.6. Identify and fix unsafe practices and processes used for the administration of the server.

2.7.10.7. Quarterly Penetration testing: The DCSP shall perform quarterly penetration testing to ensure the following: Create a hacker's view of the server, in terms of the ways it can be hacked from outside. Identify security vulnerabilities and fix holes discovered. Implement emergency quick fix solutions and long term solutions against successful exploits.

2.7.10.8. Firewall management: Initial setup of the firewall, implementation of rule base on the firewall to enable customer specific applications and ports, implementation of security policies based on services (HTTP, FTP, Telnet), source address / name, destination address / name, online monitoring of firewall through a central console with 24x7 support, system administration for firewall, including updates & hot fixes that affect its performance, changes in firewall rule base with proper change management and backup of firewall configuration each time there is a configuration change.

2.7.10.9. Intrusion detection and prevention: Initial installation and setup; applying appropriate levels of risk assessment for specific needs which allows security policies to be an integral part of scanning process; tracking of resource usage for anomalies and logging any suspicious packets from the outside; log maintenance and management; automated network based security assessment and policy compliance evaluation.

2.7.10.10. Distributed Denial of Service defense: The DCSP shall deploy a suitably qualified team for detection, mitigation and prevention of attacks on target web sites, hosted applications or network infrastructures that leads to absorption of available bandwidth and disruption of access for legitimate customers and partners of UIDAI.

2.7.10.11. Testing and application of patches: The DCSP shall carry out testing and application of periodic patches released by software and OS vendors to plug vulnerabilities in the system.

2.7.11. **Storage and backup management**: The DCSP shall perform Tape and disk backup as per the guidelines issued by UIDAI. This will include installation of backup software, managing the tape library, regular backup and restore operations and assuring security of the media through appropriate access control. In addition, the DCSP shall also manage scheduled data replication. The activities shall include:

2.7.11.1. The tenderer should undertake study of the application environment in order to plan for an integrated storage infrastructure based on SAN. The zoning, LUN and volume creation should be decided based on the characteristics of the application.

2.7.11.2. Develop an implementation plan, installation and configuration of the storage infrastructure, including but not limited to configuration of disk arrays, switches, routers, fibre channel, tape library, disk library and other solution components to implement the overall solution.

2.7.11.3. It is expected that the tenderer will draw knowledge from industry best practices and his experiences to develop a storage architecture that is best suited for the purchaser and document the blueprint for a cohesive architecture, prior approval for which should be obtained from the purchaser before actual implementation.

2.7.11.4. The deployment of the disk storage shall consists of tasks, including, but not limited to, installation and configuration of SAN and NAS design, creation and configuration of volumes, LUN, RAID storage sets, assisting in migration of data and undertake tuning exercise to optimize performance of the solution.

2.7.11.5. Backup of operating system, database and application should be performed as per stipulated policies of the purchaser at the data centre premises. The bidder should use provision for appropriate tools for undertaking these activities.

2.7.11.6. Monitor and enhance the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies.

2.7.11.7. Ensure prompt execution of on-demand backups of volumes, files and database applications whenever required by the purchaser or in case of upgrades and configuration changes to the system.

2.7.11.8. Real-time monitoring, log maintenance and reporting of backup status on a regular basis. The administrators should ensure prompt problem resolution in case of failures in the backup processes.

2.7.11.9. The administrators should undertake media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets (onsite and offsite).

2.7.11.10. The bidder should ensure the physical security of the media stored in cabinets.

2.7.11.11. **The bidder should also ensure that a 24 x 7 support for file, database and volume restoration requests is available at the data centres.**

2.7.11.12. **The bidder shall also provide sufficient media (tape library) for daily, weekly and additional backups for the duration of the contract.**

2.7.11.13. **At least two copies of backup should be maintained in the media.**

2.7.12. Application Monitoring

2.7.12.1. The bidder should monitor the UIDIA application stack including the ASDMSA, ABIS application and associated components

2.7.12.2. The bidder should ensure high-availability and response times of the system as defined by UIDIA

2.7.12.3. The bidder shall support the ASDMSA and BSP vendors in troubleshooting the corresponding application stacks

2.7.13. Data Management

2.7.13.1. The bidder shall support UIDAI in Loading and scrubbing of data as per Operational documents and Work instructions

2.7.14. System Integration

2.7.14.1. The bidder shall integarate the hardware (servers, storage, network), system software and application software to ensure the end to end smooth functionality fo the CIDR system in terms of enrollments and verifications

2.7.14.2. The bidder shall assist the other vendors in the smooth integration of their application with the CIDR infrastructure

2.7.14.3. The bidder shall troubleshoot and identify faults if any in the system and co-ordinate with the corresponding vendor/provider of the component and resolve the issues as per UIDAI defined SLAs.

2.7.14.4. The bidder shall keep the NCR-DC infrastructure and system setup upto date in terms of configuration, patches in line with the Bengalure-DC setup.

2.7.15. **Support for data centre operations**

2.7.15.1. **The data centre operations should be provided onsite full-time at the data centres on a 24 x 7 basis.**

2.7.15.2. The operators present in the data centres should act as the guardian of the infrastructure setup by the purchaser.

2.7.15.3. The data centre operators should regularly monitor and log the state of environmental conditions and power conditions in the data centre.

2.7.15.4. The operators should coordinate with data centre vendor to resolve as per SLA with DC vendor any problems and issues related to the data centre including but, not limited to, environment conditions, power, air-conditioning, UPS, LAN, racks, fire, water seepage, dust, cleanliness, etc.

2.7.15.5. The bidder shall also be required to co-ordinate with the data centre vendor for implementing any changes that may be required towards the placement and layout of infrastructure within the data centre.

2.7.15.6. The operators shall also be required to act as the first level of support for any issues related to the network and communications equipment installed at the data centre. The operators should coordinate with VPN vendor to resolve at the earliest any problems and issues related to such equipment.

2.7.15.7. Physical Security related devices and their Management is within the scope of Data Centre Service Provider. However, since the Bidder is responsible for management & maintenance of the purchaser's equipment and as a guardian of purchaser's infrastructure at the Data Centre Sites, Bidder shall ensure vigilance, safety and prevention of unauthorised access at respective Data Centre Sites. The operators should ensure the physical security of the data centre by allowing only authorized personnel to enter the premises.

2.7.15.8. The bidder should prepare a list of equipment, software and configuration installed in the data centres and the same should be approved by purchaser. The bidder should maintain and modify the list in accordance to the modifications.

2.7.15.9. Any breach of security or non-compliance on part of the data centre vendor and/or data centre facilities shall be immediately brought to the notice of the purchaser with suggestions for improvements.

2.7.15.10. The bidder shall maintain at the data centre, a log of all personnel, including the bidder's personnel, entering or visiting the data centre. Such a log shall be provided to the purchaser whenever required.

2.7.15.11. Manage an inventory critical components and spares that are provisioned onsite and co-ordinate with the OEM to ensure replenishment of the same whenever required.

2.7.15.12. **The purchaser may undertake audits on a periodic basis and the same may be conducted by a third-party auditor. The bidder shall be required to provide necessary support for this and adequately address the audit findings in a timely manner. These audits may include:**

a. Information Security audits

b. SLA compliance audits

c. BCP readiness audit

d. IT Infrastructure audit

e. Policy compliance audit

2.7.16. **Management reporting**: The DCSP shall put in place a system for periodic management reporting of key performance indicators in line with the SLA framework proposed.

2.7.16.1. The bidder shall provide reports as listed in Annexure – 1 of this section.

2.7.16.2. The report shall include target and actual values of the key performance indicators. Suitable planning to overcome gaps between the two values shall also be part of the report.

2.7.16.3. Aadhar Related Reports: The bidder shall provider the following additional operational reports including but not limited to the following (upto 50). The detailed specifications of the report shall be provided by the UIDAI to the bidder.

a. UID Numbers Generated: Hourly, Daily, Weekly, Monthly, Quarterly (successful, unsuccessful, duplicates etc)

b. The reports shall be segregated by Enrollment Agency, Registrar, Geography and Enrollment Stations

2.7.17. **Technical support**

2.7.17.1. The bidder should provide comprehensive onsite support to the purchaser at the designated data centres on a 24 x 7 basis to meet the service levels in accordance with the SLA mentioned as part of this bid.

2.7.17.2. Ensure that the entire solution as a whole is operational and run according to stipulated performance standards.

2.7.17.3. The bidder along with all the associated OEMs should commit to provide all necessary resources and expertise to resolve any issues and carry out required changes, optimizations and modification so that complete system as a whole works according to the specified requirements and satisfaction of the purchaser.

2.7.17.4. The bidder should provide comprehensive technical support services for all the software proposed for the entire period of the contract. The technical support should include all the upgrades, updates and patches that are released by the respective OEMs during the period of contract.

2.7.18. **Change management**

2.7.18.1. The bidder shall be responsible for managing the changes that happen to the BCP setup on an ongoing basis, including but not limited to, changes in hard / soft configurations, changes to applications, changes to policies, applying of upgrades / updates / patches, etc.

2.7.18.2. The bidder should undertake planning required for changes, draw up a task list, decide on responsibilities, co-ordinate with all the affected parties, establish and maintain communication between parties to identify and mitigate risks, manage the schedule, execute the change, ensure and manage the port change tests and documentation.

2.7.19. **AMC tracking**

2.7.19.1. Track the Annual Maintenance Contracts for all the assets at the data centres and initiate procedure for renewal of the same at appropriate points in time. The bidder should provision for appropriate tools for managing the same.

2.7.20. **Documentation requirements**: The bidder shall be required to submit documentation in the format, media and number of copies as desired by UIDAI after each milestone as decided mutually with UIDAI and in accordance with the plan.

2.7.20.1. The documentation should be kept updated throughout the contract period with appropriate change management procedure and version control.

2.7.20.2. The bidder shall be responsible for creating and maintenance of all the documentation mentioned wherever in the scope of work including but not limited to configuration documents, network diagram, layout diagram, data center operation manual, system administration manual, database administration manual, security administration manual, password management manual, etc.

2.7.20.3. The maintenance manual shall, include but not limited to the sections on overall configuration of the system with layouts showing the location of every unit with block diagram with details for operation, detailed descriptions of component units with details for operation, block diagrams showing the flow and interaction, data and logic diagrams, detailed connectivity/cabling information, etc. The manual should also

include part list and wiring schedules, but care shall be taken to avoid obscuring of the operational description.

2.7.20.4. Maintenance procedures manual shall include but not limited to the sections on diagnosis of faults, testing and setting up adjustments, replacement of units, guidelines for preventive servicing, routine servicing, tuning guidelines and operation of test equipment.

2.7.20.5. The servicing manual should cover all the test and maintenance procedures and information necessary for the diagnosis and repair of faulty units or components of every type. It shall include circuits, board layouts, component schedules, test points and test parameters, and use of test equipment.

2.7.20.6. The bidder shall be also responsible for maintenance and update of all the policy documents including but not limited to security policy, backup policy, archival policy, messaging policy, ERM policy, backup policy, anti-virus policy, etc.

2.7.20.7. The bidder should make changes to the documents as and when there is change in the infrastructure or policies or as and when required by the purchaser.

2.7.20.8. The bidder should maintain a library of various artefacts including, but not limited to, documents, manuals, knowledge bases, CD / DVDs, etc. pertaining to all the components supplied by various OEMs. The bidder should keep a track of all the artefacts and manage the issue and return of the artefacts into the library.

2.7.20.9. All the documents would be solely owned by the purchaser.

2.7.20.10. The bidder should hand-over the processes, documentation and inventory to the Purchaser or any agency appointed by the Purchaser at the end of the contract period. The bidder shall ensure that a smooth transition takes place.

TECHNICAL SPECIFICATIONS

3. Technical Specifications

3.1. General Technical

The Data Center offered by the Date Center Service Provider (DCSP) should be of minimum Tier 3 standard (rated as per Uptime Institute Inc. guidelines). The DCSP is expected to provide sufficient network points, OFC links, telecom facilities, electrical connections, air conditioning, backup power through generator(s), access control, integrated fire detection and suppression, physical security and soft services etc as applicable for Data Center and as required for the proposed equipment on 24 x 7 basis in order to maintain uptime of all such facilities at as per SLA. DCSP to identify any Single Point of Failure in their infrastructure; reduce the same to absolute minimum and indicate any plan for future upgrade. DCSP shall submit necessary certificate and document to illustrate compliance in the aspects of building, electrical certification, fire certification, water treatment, safety and security.

3.2. Architectural and Structural

3.2.1. **Location**

The proposed DC should be located:-

3.2.1.1. In Delhi / NCR Region.

3.2.1.2. Should be easily accessible by public transport.

3.2.1.3. Free from hazards like chemicals, radiation, industrial pollution, fumes, etc.

3.2.1.4. Safe from natural disasters like earthquake, floods, hurricane, volcano etc.

3.2.1.5. Isolated from neighbouring buildings with adequate setbacks.

3.2.1.6. Should have adequate access for entry of vehicles and personnel to carry out emergency activities like fire fighting, evacuation etc.

3.2.1.7. The building should not be located at the sites that are near the sources of continued or intermittent vibrations such as airports, mines, railway lines etc.

3.2.2. **Building**

The proposed DC building shall fulfill the following minimum criteria:-

3.2.2.1. The building structure should be complying to IS 1893, IS 4326 and respective revisions thereon.

3.2.2.2. Preferably it should be a standalone structure. If the DC is located in a multi storied building then the height of the building should not be more than 40 meters.

3.2.2.3. In any case, the Data Center should not be on the ground floor and the top most floor of the building.

3.2.2.4. Age of the building should be not older than 10 years on the stipulated date of opening of the bid. If the building is older, Structural Stability Certificate to be provided from a chartered structural Engineer issued within last 1 year.

3.2.2.5. Should be built to withstand seismic disturbances complying with Zone IV requirements.

3.2.2.6. DC true floor should have a load bearing capacity of 900-950kgs/Sqmt and more.

3.2.2.7. Should have a freight elevator to carry the IT equipment to DC located in upper floors.

3.2.2.8. Should have adequate fire exit staircase as per the statutory norms.

3.2.2.9. Should be provided with Fire fighting, public address and surveillance system.

3.2.2.10. The periphery where the building is located should be provided with fencing and possible surveillance deployed.

3.2.2.11. It should be a concrete structure with brick walls to resist forcible attacks.

3.2.2.12. Should be protected from Electro-Magnetic Interference and Radio-Frequency Interference.

3.2.2.13. Separate redundant ducts / trenches for entry of power cables and fiber cables.

3.2.3. Telco/ Communication Room

3.2.3.1. The Communication room should be of 100 sq.ft exclusive for UIDAI and strategically located with independent access control. Shared Communication Room with dedicated Cage for UIDAI should be acceptable.

3.2.3.2. The room should be provided with adequate cooling preferably through the plenum of false floor.

3.2.3.3. The room should be provided with fire alarm and fire suppression system.

3.2.3.4. The room should be provided with CCTV for monitoring the activities of the external agencies.

3.2.3.5. The fiber entering into the communication room should be from two different distinct paths.

3.2.4. **Staging Room**

3.2.4.1. The staging room should be having enough room for unpacking the equipments

3.2.4.2. Should be provided with minimum 32A power points two to four nos. to enable testing of servers and storage equipments.

3.2.4.3. At least one rack should be provided for testing the equipments.

3.2.4.4. Minimum of two seats with PC and LAN connectivity should be available for the personnel to upload applications and test the servers.

3.2.4.5. Fire alarm, fire suppression, air conditioning and access control should be provided in the room.

3.2.5. **Secure Storage Space (Store Room)**

3.2.5.1. The Secure Storage Space (store room) should be of 100sq.ft exclusive for UIDAI and conveniently located with independent access control. There should be adequate space for unloading the IT equipments / materials and storing should be available

3.2.5.2. The Secure Storage Space (store room) should be a secure place with proper locking arrangement.

3.2.5.3. The movement of equipments from the unloading dock to the store and from store room to the staging should be carried out using proper material movement trolleys.

3.2.5.4. The Secure Storage Space (store room) should have minimum of 400 – 500lux illumination.

3.2.6. **Server Hall**

3.2.6.1. The Server hall should be on the first floor and above and made of brick walls without windows.

3.2.6.2. There should be an emergency exit preferably diagonally opposite in the server hall with clearly marked fluorescent signs.

3.2.6.3. Ramp should be provided at the entry of the server hall to facilitate movement of IT equipments without any hindrance.

3.2.6.4. The hall including the doors should be two hours fire rated.

3.2.6.5. Access control and CCTV systems should be provided.

3.2.6.6. Fire alarm, fire suppression and early smoke detection system should be installed.

3.2.6.7. The hall should be provided with cementatious tile false flooring system.

3.2.6.8. The minimum distance between the true floor and the false floor should be 600mm.

3.2.6.9. The false floor tile should be 600mm x 600mm.

3.2.6.10. The false floor should be provided with anti-static laminate.

3.2.6.11. The false floor should have a load bearing capacity of minimum 900-950 kgs/Sqmt.

3.2.6.12. All openings in the hall should be sealed with fire rated material.

3.2.6.13. The hall should be treated for termite and rodent menace.

3.2.6.14. The walls and the slab should be treated appropriately for water ingress.

3.2.6.15. Partitions within the hall should be fire retardant preferably fire resistant.

3.2.6.16. The false ceiling (if provided) should be 2hrs fire rated and also possess acoustic property.

3.2.6.17. The clear height between the false floor and the bottom of ceiling (True ceiling or False Ceiling – which ever is applicable) should not be less than 2.7mtrs.

3.2.6.18. The hall should not be housing water sprinkler system.

3.2.6.19. Glass where ever provided in the hall should be fire rated.

3.2.6.20. Cages provided should be properly anchored to the civil structure.

3.2.7. **Services/ Utility Rooms**

3.2.7.1. The electrical room should be strategically located to receive power and distribute the same to the building and the server hall.

3.2.7.2. The electrical room should be provided with fire alarm and fire suppression system.

3.2.7.3. The room should be provided with access control to circumvent unauthorized entry.

3.2.7.4. Proper ventilation should be provided.

3.2.7.5. Chiller & AHU rooms should be provided with proper slope to drain water out of the building.

3.2.7.6. There should not be water stagnation in the chiller and AHU rooms

3.2.7.7. Cafeteria, Pantry or Rest rooms should not be above the server hall.

3.2.7.8. No food shall be cooked in the cafeteria or pantry.

3.2.7.9. A full sized Fire Retardant Filing Cabinet for media storage should be provided with all keys to be handed over to authorised personnel of the Purchaser.

3.3. Electrical Systems

3.3.1. ***Power***

3.3.1.1. The power from the electricity board should be a high tension supply

3.3.1.2. The power preferably should be from two different substations entering into the building / campus from two different distinct paths.

3.3.1.3. The power being received from the electricity board should be terminated in a HT breaker panel.

3.3.1.4. The HT panel should be properly earthed.

3.3.1.5. There should not be any joints employed in the HT cable from which the power is drawn.

3.3.1.6. The HT panel should be properly housed / protected against any damages.

3.3.2. ***Transformer***

3.3.2.1. The transformer employed should be as per the designed capacity.

3.3.2.2. If a dry type transformer is employed it should be properly protected against rodents

3.3.2.3. The dry type transformer should be provided with winding temperature indicator for monitoring.

3.3.2.4. In case of oil type transformer it is preferred to be installed out doors.

3.3.2.5. The oil type transformer should be properly fenced and protected.

3.3.2.6. Separate earthing for neutral and body should be provided.

3.3.2.7. Adequate fire suppression system to be provided especially if the oil type transformer is housed with in the building.

3.3.2.8. Adequate protection against surge in voltage and current should be incorporated.

3.3.3. ***Diesel Generator***

3.3.3.1. Backup diesel generator equal to the capacity of the transformer should be provided to supply power to the building in case of failure in main power from the Electricity board.

3.3.3.2. The diesel generator should be provided with acoustic enclosure to reduce noise level as CPCB directives.

3.3.3.3. The exhaust of the generator should be installed at an appropriate height as per the directive of the pollution control board.

3.3.3.4. Neutral and Body earthing should be provided through separate earth pits.

3.3.3.5. The generator should be cranked and take the full load immediately in the event of failure of the main power through AMF feature.

3.3.3.6. The generator should be provided with fuel tank of 990Ltrs.

3.3.3.7. Local control near the generator should be provided.

3.3.3.8. The generator capacity should fulfill the power requirement of both IT and air conditioning load of the data center.

3.3.3.9. Separate storage tank should be installed within the campus to supply continuous diesel to the fuel tanks.

3.3.3.10. The fuel should be sufficient to run all the generators required for at least 48 hrs.

3.3.3.11. Should have a SLA with a vendor / fuel company for re-filling the fuel tanks.

3.3.4. Main LT Distribution Panel

3.3.4.1. The Main LT distribution panel should be housed in an electrical room.

3.3.4.2. The panel should have minimum two incomers one for the main power from the electricity board and the other for the diesel generator.

3.3.4.3. The incomer should be a breaker of equivalent capacity to the transformer and generator installed.

3.3.4.4. The breaker should have earth fault, overload and thermal protections.

3.3.4.5. The panel should have sufficient out going feeders to add any additional equipment required in future.

3.3.4.6. The panel should be provided with proper ventilation

3.3.4.7. Clearances from other equipments and walls from the panel should be as per the IEC guidelines.

3.3.5. Un-interrupted Power Supply (UPS)

3.3.5.1. The UPS should be of adequate capacity to cater to the IT load.

3.3.5.2. The UPS should be N+N redundant in two different rooms.

3.3.5.3. The UPS should have harmonic filters to limit the Total Harmonic Distortion to less than 10% and protection against surge.

3.3.5.4. It should provide clean power to the servers and storage equipments.

3.3.5.5. The battery back up for the UPS should be of 20minutes at full load the Generator should take over the supply within one minute

3.3.5.6. The battery room should be maintained at a temperature of less than 30 degrees.

3.3.5.7. Separate UPS should be employed for catering to the office equipment like PC's, fax, printers etc.

3.3.5.8. In an N+N scenario the UPS should be synchronized.

3.3.5.9. The bypass should preferably be connected though isolation transformer.

3.3.5.10. Static transfer switches should be provided at appropriate locations to enable seamless transfer in case of the UPS maintenance or breakdown.

3.3.5.11. Dedicated earth system has to be provided for the neutral of UPS.

3.3.5.12. The down stream from UPS should be double neutral.

3.3.5.13. The UPS System should preferably be dedicated to UIDAI.

3.3.5.14. The UPS should be of reputed make like Emerson, Chloride, Socomec, APC.

3.3.5.15. The UPS should be able to handle leading power factor without degradation

3.3.6. Distribution Panels

3.3.6.1. UPS power distribution panels should be separate from raw power distribution panels.

3.3.6.2. Emergency lighting panel should be separate and connected from the separate UPS designated for lighting and office area.

3.3.6.3. The power supply to the air conditioning equipments should be achieved through a separate distribution panel.

3.3.6.4. The panels should be properly named and tags to be provided for the cables.

3.3.6.5. Panels should be IP 45 as per IEC guidelines.

3.3.6.6. During maintenance of panels the regular operations should not be disturbed.

3.3.6.7. Capacitor panel of adequate capacity should be employed for correction of power factor.

3.3.6.8. Each rack should support a minimum load of 7 KVA.

3.3.6.9. The downstream of UPS shall have double neutral including the PDU.

3.3.6.10. The power distribution units (PDU) installed in the server hall for catering power to the racks should have double pole MCB's of minimum 32 Amps.

3.3.6.11. The PDU should also have provision for 3 phase circuits to cater to any specific equipment requirement being deployed.

3.3.6.12. Industrial sockets of 32A from two different UPS should be provided below false floor feeding to each rack that will be housed in the cage and in the communication area.

3.3.6.13. The rack should be powered up from the industrial sockets through vertical / horizontal PDU comprising female sockets.

*3.3.7. **Earthing***

3.3.7.1. Earthing shall be provided in accordance to IS 3043.

3.3.7.2. The cross sectional area of earthing conductor shall not be less than half that of the largest current carrying conductor

3.3.7.3. The resistance of the earthing system should be less than 1ohm.

3.3.7.4. All panels and equipments should be earthed to avoid accidents to the personnel.

3.3.7.5. Single reference grid should be laid below false floor.

3.3.7.6. The pedestals of the false floor should also be earthed.

3.3.7.7. Methods to control Electro static discharge should be adopted by employing hand straps, mats, etc.

*3.3.8. **Lighting***

3.3.8.1. Lighting in the server hall should be of 350-400lux.

3.3.8.2. Regular lighting and emergency lighting should be provided in all locations of the building

3.3.8.3. Lighting fixtures used in the office area should be of low glare.

3.3.8.4. Wiring for lighting should be laid in MS conduits (if exposed).

3.3.8.5. Lightening arrestor should be provided for the building.

3.3.8.6. Minimum 10% of the lights should be on emergency inverter.

3.4. Heat Ventilation and Air Conditioning

3.4.1. ***Comfort HVAC***

3.4.1.1. Comfort AC should be employed in the office area as well as Storage Room.

3.4.1.2. Fresh air should be routed to the AHU.

3.4.1.3. Grills for supply and return should be strategically located to provide a good environment for working.

3.4.1.4. The ducts should be properly insulated.

3.4.1.5. The ducts should be provided with fire dampers.

3.4.2. ***Precision Air Conditioning***

3.4.2.1. PAC should be employed in the Server Hall.

3.4.2.2. The PAC should have a redundancy of N+1.

3.4.2.3. The PAC should be intelligent micro-processor based system.

3.4.2.4. The temperature of the hall should be in the range 22 degree centigrade +/- 2 degrees centigrade.

3.4.2.5. The relative humidity should be 50% +/-5%.

3.4.2.6. The PAC should have water leak detection to communicate any leak in the chilled water pipeline, humidifier pipe or drain pipe.

3.4.2.7. The refrigerant in the HVAC system should be CFC Free.

3.4.2.8. The air throw shall be bottom charged feeding through plenum. Floor grills wherever required should be installed.

3.4.2.9. Minimum of 600CFM should be available in front of the rack without booster fan.

3.4.2.10. In case of additional requirement of CFM provision for adding booster fans should be available.

3.4.2.11. Cable trays blocking the path of the air flow should be re-routed to provide proper cooling to the server racks.

3.4.2.12. The rack layout should be designed to achieve hot and cold aisle.

3.4.2.13. The PAC units should have High Efficiency Particle Filters for Air Filtration to 5 microns. The HVAC should be designed such that the air should not contain more than 5, 00,000 particles per cubic foot of air of size 5 micron or higher.

3.4.2.14. Temperature and humidity sensing and monitoring should be done on a continuous basis and should be fed to the BMS System.

3.5. Fire Alarm & Fire Suppression System

3.5.1. Fire Alarm

3.5.1.1. The Data Center should be protected from Fire using State-of-the-art Automatic Smoke/ Heat Detection Alarms & Fire Control mechanism as per National Fire Protection Association (NFPA) standards.

3.5.1.2. The fire detection system should be Analogue Addressable type.

3.5.1.3. The fire panel indicating the alarms shall to be monitored on a 24 x 7 basis & logged for providing reports.

3.5.1.4. Along with the fire alarm system the High Sensitivity Smoke Detectors (HSSD) or Very Early Smoke Detection Appliance (VESDA) should be deployed to allow swift detection of smoke or change in air quality.

3.5.1.5. The system should comprise a high sensitive smoke detector, aspirator, and filter.

3.5.1.6. The alarm system should be integrated to the building fire alarm system.

3.5.2. Fire Suppression System

3.5.2.1. Fire suppression system employed should be state-of the art and in accordance with NFPA.

3.5.2.2. The suppression should employ non toxic FM 200 gas based system.

3.5.2.3. The fire suppression agent shall not contain Ozone Depleting substances.

3.5.2.4. The smoke detector / heat detectors along with the fire panel should be programmed in a manner that they activate the suppression system.

3.5.2.5. Portable fire extinguishers should be provided in the building including office area, electrical room, utility areas etc.

3.5.2.6. The fire alarm system should be integrated with the PA system of the building.

3.6. Security Systems

3.6.1. ***Access Control System***

3.6.1.1. Entry to all critical locations in the building should be through the Access Control system employing proximity cards.

3.6.1.2. The Server Hall should be provided with biometric access to enable entry of only authorized personnel.

3.6.1.3. A panic bar should be installed to the emergency exit and integrated with the alarm system.

3.6.1.4. Access control software has to be installed on a stand alone computer and the logs of movements have to be recorded.

3.6.1.5. Periodic reports of the logs have to be recorded and sent to UIDAI.

3.6.1.6. Minimum 4 level of physical and electronic scrutiny should be incorporated before a person can enter the Data Center.

3.6.2. ***Closed Circuit Tele Vision System (CCTV)***

3.6.2.1. CCTV should be installed in strategic locations to monitor the movement of personnel in and out of all critical areas.

3.6.2.2. The CCTV should be fixed doom type with or without vary-focal lens.

3.6.2.3. PTZ cameras may be installed as required.

3.6.2.4. The CCTV should not only cover the movements within the building but also the periphery.

3.6.2.5. The DG area and the storage area should be covered through the CCTV.

3.6.2.6. The Digital Video Recorder should be IP based to allow accessibility for UIDAI to monitor remotely.

3.6.2.7. Camera recordings should be retained for a period of 90 days and should be available for UIDAI review as and when required.

3.6.3. ***Physical Security***

3.6.3.1. The building should have physical security deployed 24x7.

3.6.3.2. The security personnel should be trained to scrutinize the personnel entering the premises and also to carry out combat activities.

3.6.3.3. The security should monitor all the entrances.

3.6.3.4. Patrolling of the total campus should be done round the clock.

3.7. BMS System

3.7.1. The Building Management System should be implemented to monitor the various systems installed.

3.7.2. The BMS software should be installed which can communicate with all the equipments at site.

3.7.3. The system should be capable of generating reports of power consumption from the PDU.

3.7.4. The BMS should be monitored 24x7.

3.7.5. The system should be integrated with all the other systems including fire alarm system and water leak detection systems.

3.7.6. Monthly reports should be submitted for access logs, CCTV recordings, alarms of critical equipments and power consumption.

3.8. Network Setup, Racks & Cage

3.8.1. The network system should be properly routed such that the cable laying can be carried out in short period of time

3.8.2. The network cable tray should be laid with a clearance of 300mm from the power cable trays to overcome interference.

3.8.3. The cable trays should be such that they can accommodate both fiber and copper cables.

3.8.4. The cables should be properly laid and terminated as per TIA 942.

3.8.5. The network cables shall be laid between the server racks and between the network rack and server racks as per requirement as per the design submitted by UIDAI as and when required.

3.8.6. Supply and laying of cables shall be the responsibility of the Service Provider.

3.8.7. The server racks should be of 600 x 1200mm and the network racks should be of 800 x 1000mm.

3.8.8. Only 42U racks should be deployed as and when required by UIDAI.

3.8.9. The racks should have base frame and firmly rest on the false floor.

3.8.10. The racks should have at least 55% of perforation to facilitate sufficient flow of air to the servers.

3.8.11. The racks should have cable managers and ties for dressing of the cables.

3.8.12. Service Provider shall be responsible for supply and installation of racks in position

3.8.13. Cage made of MS should be provided for the space allotted to UIDAI.

3.8.14. The cage shall be properly anchored to the civil structure.

3.8.15. The cage shall not have mesh more than 1 inch spacing.

3.8.16. The caged area shall be provided with CCTV for surveillance.

3.8.17. The cage shall be provided with bio-metric access control.

3.8.18. Every Rack should be equipped with dual power strips with 24 sockets.

3.9. Office Space

3.9.1. The Office space should have a seating capacity of 15 scalable to 30 persons.

3.9.2. The office space provided should comprise of work stations, ergonomically designed chairs, storage space, lighting and access control.

3.9.3. The office space should be secure so as to allow only the UIDAI authorized personnel to enter.

3.9.4. Each work station shall be of 2feet x 4feet minimum along with keyboard tray and personal pedestal.

3.9.5. The office area should be provided with UPS power and DG backup.

3.9.6. The each work stations should have minimum 3 UPS and 1Raw power point.

3.9.7. Connectivity should be provided between the work stations and server hall including internet.

3.9.8. The office area should be provided with comfort air conditioning.

3.9.9. Each workstation should be provided with phones.

3.9.10. Cafeteria / pantry facility should be provided for having lunch/dinner.

3.9.11. Desktop / laptops shall be provided by the DCSP.

3.10. Operational Requirements

3.10.1. All operation procedures for the MEP Systems should be documented and available for review.

3.10.2. Security policy and procedures for movement of materials & men, within the building and the data center should be made available to UIDAI.

3.10.3. The Sample Operating Process (SOP) and Emergency Operation Process (EOP) for the fire alarm and fire suppression system should be demonstrated to UIDAI to ensure that during an incident, there should be no untoward damage to human resources and equipment.

3.10.4. Maintenance schedules of all equipments should be made available to UIDAI to ensure that all equipments are maintained as per the specifications mentioned by the respective OEMs and that all equipment is in healthy condition.

3.10.5. Maintenance procedures, Risk Assessment and Work method statements should be shared with UIDAI and the documents to be made available for review.

3.10.6. Operation procedures for critical situations like power failure, water leak, damage of fuel line, short circuit, etc should be available for review.

3.10.7. There should be a robust emergency response plan backed up with trained team members, escalation and communication system.

3.10.8. The earth resistance should be measured periodically and monitored.

3.10.9. The access logs should be available for at least 180 days.

3.10.10. The power consumption logs should be updated every 15 days and intimated to UIDAI.

3.10.11. The Managed Service Logs to be provided on a weekly basis and the Change Request Summary/ approvals to be taken from the Purchaser before any activity. Incident ticket Numbers to be generated, shared and escalated on an immediate basis and their resolution and closure should be at the earliest.

3.10.12. Shared Helpdesk is acceptable for the Data center Facilities catering to the Data Center Infrastructure.

3.10.13. The NOC should be provided with a secured facility.

3.10.14. The NOC should preferably be UIDAI dedicated.

3.10.15. The NOC should have a centralized monitoring console/ LCD/ Projector Screen (Video Wall).

3.10.16. The NOC should have a redundant and robust infrastructure with reference to UPS and Network links.

3.10.17. The type of physical/ electronic security should be Access Controlled with electronic and physical Surveillance provided in the NOC.

3.10.18. The Network security (Firewall/ IDS, etc.) should be provided in the NOC.

3.10.19. The following type of communication nodes are to provided in the NOC:

(a) Toll free numbers

(b) PSTN from multiple providers

(c) Email/ messaging

(d) Alerting via Email / SMS

(e) Conferencing

3.10.20. From the Network perspective, the following to be provided:

(a) Internet bandwidth:

1. The bidder shall provide 100 Mbps internet bandwidth.

2. The bidder shall provide internet bandwidth from two network providers.

3. It is recommended that the ISP's connecting Bangalore and Delhi Sites (for BCP/DR) should be same so that there is direct connectivity between the sites and provide low latency connectivity without going through the external networks.

4. UIDAI shall procure bandwidth in increments of 100 Mbits/Sec on a need basis subsequently. The bidder shall make suitable provisions for the same for scalability.

(b) MPLS connection between Data Centre in Bengaluru and Data Centre in NCR Delhi

1. The bidder shall procure dedicated MPLS connectivity between the two data centres. This connectivity shall be procured from two separate MPLS connectivity providers.

2. The bidder shall be responsible for establishing the connectivity with the Bangalore and Delhi data centers.

3. Minimum committed bandwidth of 100 Mbps should be provided between the 2 locations. Additional bandwidth shall be procured by UIDAI on a need basis from the bidder.

4. The bidder is required to provide bandwidth cost for the connectivity in C2 of Annexe 4.2.3c: DETAILED COST SHEET – Variable Recurring Cost.

5. The bidder shall provide the necessary services and equipment required for connectivity between the MPLS cloud of the two selected bandwidth providers as referred in clause (2) above.

(c) Network monitoring and management:

a. The bidder shall perform the following services:

   i. Develop the network architecture and layout diagram for the data centre. This will include physical layout of all network components. The same shall be submitted to UIDAI for approval and subsequent implementation.

   ii. Interconnect all network (LAN and WAN) and security devices as per design and network architecture approved.

b. The bidder shall:

   i. Interact with telecom service providers for integration of network connections in consultation with UIDAI. This will include Internet, Registrars/partners, UIDAI Intranet, and Disaster Recovery connection between UID Data Centres.

   ii. Integrate the perimeter security services with network.

   iii. Performing Move/Add/Changes including Network ports, Cable verifications and connect, Network devices, network other elements including but not limited to Firewalls, Load Balancers, IPS, VPN and Dual Authentication system.

c. From a monitoring perspective, the bidder shall perform the following:

   i. Network monitoring of Devices, Link Up/Down status, Wide Area Network (LAN), Local Area Network (WAN)

   ii. Interface with local Telcos and other service providers and other technical teams supporting UIDAI infrastructure

   iii. Engage and provide assistance to onsite personnel in performing break/fix activities

   iv. Make recommendation for improvements after analysis of operational data

   v. Network upgrades as requested for both device and network connectivity

   vi. Escalating the Service Level issues to the appropriate members as required for quick resolution of network or security problems

   vii. Perform the network availability monitoring

viii. Perform the availability monitoring of security infrastructure Firewalls, IDS/IPS, Event Correlation services, SSL and SSL VPN, etc (as per BOM)

ix. Perform the network alert monitoring

x. Perform the configuration change and log monitoring

xi. Monitor the network access and network ports to ensure the continuous CIDR operation

xii. Monitor the performance of Network, Security devices and highly available systems

xiii. Monitor the utilization of network resource and network connectivity

xiv. Monitor the network capacity and load distribution as required

xv. Proactively identify security vulnerabilities and potential threats and take necessary remedial action

(d) Local Area Network

3.11. MIS Reports

The DCSP should provide

3.11.1. Visitor details for Data Center including name, time of entry and exit, entry authorized by purpose of visit, etc as applicable.

3.11.2. Material movement for all material entering / exiting from the Data Center

3.11.3. Uptime Report for Input AC Power supply (AC input from Transformer / DG set)

3.11.4. Uptime Report for UPS system including load variations on an intraday basis.

3.11.5. Uptime Report for Air-conditioning system

3.11.6. Uptime and availability of CCTV Surveillance system

3.11.7. Uptime and availability of Access Control (Biometric & Proximity readers)

3.11.8. Uptime Report for Fire Management System

3.11.9. Incident reports leading to disruption, downtime, security violations or any such reports.

3.11.10. Helpdesk report including details of each call, time of call, defect reported, time of call resolution, action taken, etc,

3.11.11. SLA compliance reports

3.12. Bidder Company Experience

3.12.1. The Bidding Company should be having at least 5 years experience in the Data Center Business.

3.12.2. The total Data Center Raised floor area owned and managed by the Bidder should be at least 20,000 sq. feet aggregate Pan India.

3.12.3. The total Data Center Raised floor area owned and managed by the Bidder in Delhi should be at least 20,000 sq. feet.

3.12.4. All the Data Centers of the Bidder should be of Tier III rating or higher.

3.12.5. The Total Uptime recorded for the past 3 years should preferably be 99.99%.

3.12.6. The retention percentage of the clients for the past three years should be above 95%.

3.12.7. The average PUE obtained in the Bidders Data Centers across the country should be substantially below 2.00.

3.12.8. All the Incidents witnessed should have Root cause analysis done and the Incidents to be classified as Preventable and non – Preventable.

3.13. Personnel Details

3.13.1. The qualifications and commensurate experience of the staff in the Managed Services of Data Center should be at par with the market standards.

3.13.2. The qualifications and commensurate experience of the staff in the Facility Management and Operational Services of the Data Center should be at par with the market standards.

3.13.3. The qualifications and commensurate experience of the staff in the Projects Planning and Execution of the Data Center.

3.13.4. Profile and experience levels of your Top Management.

3.13.5. The Employees should be trained and skill sets of the employees should be upgraded and they should be encouraged to imbibe the latest technologies and improvements.

3.14. Experience of Managed Services Work Demonstrated in Past by Bidder or Consortium Member

3.14.1. Provide copy of work order(s) / contract/ purchase order(s)/ client certificate(s) in the Technical Bid for verification with clear reference to value of the contract. In addition to the above, detail should be given in a prescribed format set under **Annexe 4.1.13 of Corrigendum III – Annexure VIII.**

4. Rejection Criteria

The Bidder would be disqualified during the technical Bid if he does not qualify for the following requirements:

4.1.1. The Data Center flooring should have a minimum structural strength of 900 Kgs/ sq. meters.

4.1.2. The DG set/s should not be housed inside the Data Center building.

4.1.3. The fuel stored for the DG set/s should be more than 12 hours on full load with an SLA formalized with Fuel supplier for continuous replenishment within an agreed time period in hours.

4.1.4. Each rack should support a load of minimum 7 KVA.

Proposed Time Schedule

5. Proposed Time Schedule

Activity	Timelines in days
Commencement of activities for Data Center facilities	T+5
Supply and Installation of racks in Communications Room	T+7
Preparation and handing over of secure storage space (store room)	T+10
Installation and Commissioning of Office Space	T+15
Installation Testing and Commissioning of ISP connection	T+25
Supply and Commissioning of Racks, Trays, Structured Cabling, Cage and Access control for Data Center	T+30

***T = Date of issue of Letter of Intent/ Purchase Order**