കേരള സർക്കാർ

സംഗ്രഹം

പൊതുഭരണം - സംസ്ഥാനത്തെ എല്ലാ സർക്കാർ സ്ഥാപനങ്ങൾ, അർദ്ധ സർക്കാർ സ്ഥാപനങ്ങൾ, സ്വയംഭരണ സ്ഥാപനങ്ങൾ , ഗ്രാൻഡ് ഇൻ എയ്ഡ് സ്ഥാപനങ്ങൾ എന്നിവയിൽ സ്പാർക്ക് ബന്ധിത ബയോമെട്രിക്ക് പഞ്ചിംഗ് സംവിധാനം സ്ഥാപിക്കുന്നത് സംബന്ധിച്ച തുടർ നടപടികൾ നിശ്ചയിച്ച് - ഉത്തരവ് പുറപ്പെടുവിക്കുന്നു.

പൊതുഭരണ (ഏകോപനം) വകുപ്പ്

സ.ഉ.(സാധാ)നം.5090/2019/പൊഭവ. തീയതി, തിരുവനന്തപുരം, 30-08-2019.

പരാമർശം- 1) സ.ഉ(പി) നം. 26/2005/ഐ.റ്റി.ഡി, തീയതി, 24/10/2015
2) സ.ഉ(എം.എസ്) 108/18/പൊഭവ, തീയതി, 18/05/2018
3) സ.ഉ(സാധാ) 7637/18/പൊഭവ, തീയതി, 22/11/2018
4) സ.ഉ(സാധാ) 8153/18/പൊഭവ, തീയതി, 17/12/2018
5) സ.ഉ(സാധാ) 77/2019/പൊഭവ തീയതി, 06/05/2019

ഉത്തരവ്

കേരളത്തിലെ എല്ലാ സർക്കാർ ഓഫീസുകളിലും സ്പാർക്കുമായി ബന്ധിപ്പിച്ചുകൊണ്ട് ബയോമെട്രിക്ക് ഫിംഗർപ്രിന്റ് അറ്റൻഡൻസ് മാനേജ്മെന്റ് സിസ്റ്റം (പഞ്ചിംഗ് സിസ്റ്റം) നടപ്പിലാക്കുവാൻ നിർദ്ദേശിച്ചുകൊണ്ട് പരാമർശം 1 പ്രകാരവും ആയത് എപ്രകാരം നടപ്പിലാക്കണമെന്നത് സംബന്ധിച്ച മാർഗ്ഗരേഖ പരാമർശം 4 പ്രകാരവും പുറപ്പെടുവിക്കുകയുണ്ടായി. ഇതിനായി സ്വീകരിക്കേണ്ട തുടർ നടപടികൾ ചുവടെ പറയും പ്രകാരം നിശ്ചയിച്ച് ഉത്തരവ് പുറപ്പെടുവിക്കുന്നു.

1) AEBAS മാന്വലിലെ specification പ്രകാരമുള്ളതും UIDAI യുടെ അംഗീകാരമുള്ളതുമായ മെഷീനുകളുടെ ടെണ്ടർ നിർമ്മാതാക്കളിൽ നിന്ന് കെൽട്രോൺ ക്ഷണിക്കേണ്ടതാണ്.

2) മെഷീനുകൾ ടെണ്ടർ ചെയ്യുന്നതിനുള്ള ടെണ്ടർ ഡോക്യുമെന്റ് അന്തിമമാക്കുന്നതിനും, ഇതിന്റെ സാങ്കേതികവശങ്ങൾ പരിശോധിക്കുന്നതിനും ടെണ്ടർ തുക അന്തിമമാക്കുന്നതിനും പൊതുഭരണ വകുപ്പിന്റെ ടെക്നിക്കൽ കമ്മിറ്റി മുമ്പാകെ സമർപ്പിക്കേണ്ടതും ആയത് പരിശോധിച്ച് പൊതുഭരണ വകുപ്പ് അന്തിമ ഉത്തരവ് പുറപ്പെടുവിക്കുന്നതുമാണ്.

3) ടെണ്ടർ ക്ഷണിച്ച് വിവിധ വകുപ്പുകൾക്ക് മെഷീനുകൾ നൽകുന്നതിന് കെൽട്രോണിന് 5% റ്റി.എസ്.പി ചാർജ്ജായി അനുവദിക്കുന്നതാണ്.

4) മെഷീനുകളുടെ സ്ഥാപനവും, പരിപാലനവും കെൽട്രോണിന്റെ ചുമതലയാണ്

5) മെഷീനുകളുടെ വാർഷിക പരിപാലന കരാർ തുക പരാമർശം 1-ലെ സർക്കാർ ഉത്തരവ് പ്രകാരമായിരിക്കേണ്ടതാണ്.

6) AEBAS മാന്വലിൽ നിഷ്കർഷിക്കും പ്രകാരം ഉദ്യോഗസ്ഥരുടെ എണ്ണം കണക്കിലെടുത്ത് 50 ജീവനക്കാർക്ക് ഒരു wall mounted machine , കൂടാതെ 20-ൽ താഴെ ജീവനക്കാർ മാത്രമുള്ള ഓഫീസുകളിൽ കമ്പ്യൂട്ടറിൽ ഘടിപ്പിക്കാവുന്ന തരത്തിലുള്ള Finger print scanning device സ്ഥാപിക്കാവുന്നതാണ്.

7) ബയോമെട്രിക്ക് പഞ്ചിംഗ് സംവിധാനം സ്ഥാപിക്കുന്നതിന് എല്ലാ ജില്ലകളിലും സാങ്കേതിക സഹായത്തിനായി 2 പേരെ വീതം കെൽട്രോൺ നിയമിക്കേണ്ടതും ആയതിന്റെ ചെലവിന്റെ 50% പൊതുഭരണ വകുപ്പ് വഹിക്കുന്നതുമാണ് (TSP Charge-ന് പുറമേ).

8) സിവിൽ സ്റ്റേഷനുകളിൽ പ്രവർത്തിക്കുന്ന ഓരോ ഓഫീസിനെയും പ്രത്യേകം യൂണിറ്റായി കണക്കാക്കാതെ ഒരൊറ്റ യൂണിറ്റായി കണക്കാക്കേണ്ടതും ടി യൂണിറ്റിൽ പഞ്ചിംഗ് മെഷീനുകൾ സ്ഥാപിക്കുന്നതിനുള്ള ചെലവ് റവന്യൂ വകുപ്പ് വഹിക്കേണ്ടതുമാണ്. മിനി സിവിൽ സ്റ്റേഷൻ, വിവിധ ഓഫീസുകൾ സ്ഥിതി ചെയ്യുന്ന ഡയറക്ടറേറ്റുകൾ, വികാസ് ഭവൻ പോലുള്ള ഓഫീസ് സമുച്ചയങ്ങളിൽ പഞ്ചിംഗ് സ്ഥാപിക്കുന്നതിന്റെ ഏകോപനം പൊതുമരാമത്ത് വകുപ്പ് ഏറ്റെടുക്കേണ്ടതും, ആയതിനുള്ള ചെലവ് ടി ഓഫീസിലെ വകുപ്പുമേധാവികൾ ആനുപാതികമായി വഹിക്കേണ്ടതുമാണ്.

(ഗവർണറുടെ ഉത്തരവിൻ പ്രകാരം)

ബിശ്വനാഥ് സിൻഹ

പ്രിൻസിപ്പൽ സെക്രട്ടറി

എല്ലാ അഡീഷണൽ ചീഫ് സെക്രട്ടറിമാർക്കും, പ്രിൻസിപ്പൽ സെക്രട്ടറിമാർക്കും, സെക്രട്ടറിമാർക്കും
എല്ലാ ജില്ലാ കളക്ടർമാർക്കും/എല്ലാ വകുപ്പ മേധാവികൾക്കും
പ്രിൻസിപ്പൽ അക്കൗണ്ടന്റ് ജനറൽ (എ &ഇ/ആഡിറ്റ്), കേരള, തിരുവനന്തപുരം
എല്ലാ പൊതുമേഖലാ/സ്വയംഭരണ സ്ഥാപനങ്ങളുടേയും മേധാവികൾക്കും
സീനിയർ ടെക്നിക്കൽ ഡയറക്ടർ, എൻ.ഐ.സി, കേരള സ്റ്റേറ്റ് സെന്റർ, CDAC ബിൽഡിംഗ്, വെള്ളയമ്പലം, തിരുവനന്തപുരം
സീനിയർ കൺസൾട്ടന്റ്, സ്റ്റേറ്റ് ഗവർണൻസ് മിഷൻ ടീം കേരള സ്റ്റേറ്റ് IT മിഷൻ, വെള്ളയമ്പലം
മാനേജർ, സ്പാർക്ക്, TC 25/3436/(37), ഉപ്പളം റോഡ്, തിരുവനന്തപുരം - 695 001
മാനേജിംഗ് ഡയറക്ടർ, കെൽട്രോൺ. സെക്യൂരിറ്റി & സർവൈലൻസ് ഗ്രൂപ്പ് , കരകുളം, തിരുവനന്തപുരം
സെക്രട്ടറി, നിയമസഭാ സെക്രട്ടേറിയറ്റ്, തിരുവനന്തപുരം (ആമുഖ കത്ത് സഹിതം)
സെക്രട്ടറി, കേരള പബ്ലിക് സർവ്വീസ് കമ്മീഷൻ, തിരുവനന്തപുരം (ആമുഖ കത്ത് സഹിതം)
രജിസ്ട്രാർ, കേരള അഡ്മിനിസ്ട്രേറ്റീവ് ട്രൈബ്യൂണൽ,തിരുവനന്തപുരം, (ആമുഖ കത്ത് സഹിതം)
രജിസ്ട്രാർ, കേരള ഹൈക്കോടതി, എറണാകുളം (ആമുഖ കത്ത് സഹിതം)
രജിസ്ട്രാർ, കേരള ലോകായുക്ത, തിരുവനന്തപുരം (ആമുഖ കത്ത് സഹിതം)
മെമ്പർ സെക്രട്ടറി, സംസ്ഥാന ആസൂത്രണ ബോർഡ്, പട്ടം, തിരുവനന്തപുരം, (ആമുഖ കത്ത് സഹിതം)
സെക്രട്ടറി, സംസ്ഥാന വിവരാവകാശ കമ്മീഷൻ, തിരുവനന്തപുരം
രജിസ്ട്രാർ, കേരള /കാലിക്കറ്റ്/ കുസാറ്റ് /കണ്ണൂർ/മഹാത്മാഗാന്ധി - സർവ്വകലാശാലകൾ
രജിസ്ട്രാർ, കേരള കാർഷിക സർവ്വകലാശാല, മണ്ണുത്തി, തൃശ്ശൂർ
രജിസ്ട്രാർ, ശ്രീ ശങ്കരാചാര്യ സംസ്കൃത സർവ്വകലാശാല, കാലടി. പി.ഒ, എറണാകുളം
രജിസ്ട്രാർ, കേരള യൂണിവേഴ്സിറ്റി ഓഫ് ഹെൽത്ത് & അലൈഡ് സയൻസസ്,തൃശ്ശൂർ- 680 596
രജിസ്ട്രാർ, കേരള വെറ്റിനറി & ആനിമൽ സയൻസസ് യൂണിവേഴ്സിറ്റി, ക്യാമ്പ് ഓഫീസ്, പൂക്കോട്, വയനാട്
കേരള കാർഷിക സർവ്വകലാശാലാ ക്യാമ്പസ്, മണ്ണുത്തി, തൃശ്ശൂർ
രജിസ്ട്രാർ, കേരള യൂണിവേഴ്സിറ്റി ഓഫ് ഫിഷറീസ് ആന്റ് ഓഷൻ സ്റ്റഡീസ്, പനങ്ങാട്, കൊച്ചി
പൊതുഭരണ (കമ്പ്യൂട്ടർ സെൽ), (പൊതുഭരണ വകുപ്പിന്റെ വെബ്സൈറ്റിൽ പ്രസിദ്ധീകരിക്കുന്നതിന്)
വെബ് & ന്യൂ മീഡിയ (സർക്കാർ വെബ്സൈറ്റിൽ ചേർക്കുന്നതിന്)
കരുതൽ ഫയൽ/ഓഫീസ് പകർപ്പ്

ഉത്തരവിൻ പ്രകാരം

സെക്ഷൻ ഓഫീസർ

On-boarding Manual for Organizations to Install Aadhaar-enabled Biometric Attendance System

National Informatics Centre (NIC)

Department of Electronics & Information Technology

Government of India

November 2014

Preface

As part of the "Digital India" program of Government of India, it has been decided to implement common Biometric Attendance System (BAS) in the Central Government Offices (Agencies) located in Delhi which may be extended to offices of the state and governments and other government institutions in future. The proposed system would enable an employee to register attendance by simply presenting his/her biometric (finger print/Iris). This event will be authenticated online after one to one match with the bio-metric attributes stored in the UIDAI data base against the employee's Aadhaar number.

For implementing this project, the Central Government Organizations need to follow a structured approach in coordinating with different stakeholders. The purpose of this document is to serve as handbook for the Central Government organizations that are implementing Bio-metric Attendance System for their employees.

Targeted Audience

This document is intended for the Central Government organizations that would like to implement Bio-metric Attendance System in their organization. The following are such envisaged Agencies;

- Ministries, Departments, Attached/Sub-ordinate organizations of Central Government
- Autonomous Central Government bodies, institutions and offices
- States, Districts and other Government/Semi Government bodies like municipalities
- Central Public Sector Units

Contents

1. Background

As part of the "Digital India" Programme of Government of India, it has been decided to implement common Biometric Attendance System (BAS) in the Central Government Offices (Agencies) located in Delhi to begin with. The proposed system would enable an employee to register attendance by presenting his/her biometric (finger print/Iris) which will be authenticated online by doing one to one match with the bio-metric stored in the UIDAI data base against the employee's Aadhaar number.

In the first phase of implementation, approximately 150 Central Government Organizations have on boarded about 50,000 employees on common attendance portal (attendnace.gov.in). 1000 wall mounted bio-metric attendance terminals, 5000 finger print scanning devices and 200 IRIS devices have been procured through an open tender process floated by NICSI. These client terminals have been installed in about 100 Government Bhawans/buildings.

During the 2nd phase of this program, it is proposed that Central Government organizations shall use the common biometric attendance portal, which is hosted at NIC data center and shall procure/maintain biometric attendance terminals and desktop fingerprint scanning devices/IRIS devices in a decentralized manner, through Open tenders, DGS&D rate contract & NICSI empanelled vendors. The Central Government Organizations shall also procure the required Wi-Fi Access points for enabling network connectivity in the biometric attendance terminals through DGS&D rate contract.

1.1. Need for BAS

Government of India employs several thousand officials working across Ministries, Departments and various organizations under itself. The management of attendance of the employees is a complex but necessary task, since the presence of officials in offices directly impacts productivity and efficiency. Traditionally, attendance has been managed through registers where officials mark their attendance upon arrival in office. However, supervision of this system is difficult and is also liable to incorrect information being entered into the system. Late arrival and early departure of employees is a common occurrence across organizations. This creates a situation where the sincere and punctual employees feel discouraged and dis-incentivized.

Several offices have implemented electronic attendance systems in recent times, where the manual entries into the registers have been replaced by electronic-attendance marked through smart-cards or biometric systems. These systems have allowed easy compilation and scrutiny of attendance data leading to better supervision and monitoring. However, such systems are often stand-alone systems and do not permit easy sharing of attendance data across various levels within the system, except with the officials authorized for monitoring the attendance information. Such systems are also often implemented independently by various offices leading to duplication of cost and effort.

Therefore, it would be more appropriate to develop and implement a centralized system for monitoring attendance in various government offices. Such system should leverage on existing identity infrastructure created by Aadhaar which will result in cost, efficiency and scalability advantages.

1.2. Challenges faced in currently implemented Attendance System

The currently implemented attendance monitoring systems face the following challenges:

- Largely manual – register based systems
- Electronic systems are implemented in silos, not easy to monitor/ share information across various levels
- Card-based systems are liable to misuse or wrong entries by handing over cards to colleagues
- Several officials work across more than one office-location, or attend meetings and other official duties in different government buildings. Standalone systems cannot collate information across different locations, therefore such officials may be marked absent even if they are attending to government duties in other locations
- Compilation and monitoring of attendance data in standalone systems is difficult
- Unavailability of attendance details in the public domain creates problems for citizens who need to meet them for official work. Unavailability of officials in office is often not known to citizens, who face substantial delays waiting for officials to arrive

1.3. Proposed Solution

It is proposed to implement a common biometric based attendance system across various government offices in New Delhi. This system is envisaged to have the following features:

- Cloud-based attendance software installed and operated from NIC National Data Centre.
- Dedicated secure connectivity will be provided between National Data Center and UIDAI Data Center by NIC for authentication
- All Ministries / Departments / subordinate organizations can access the system using the NIC network provided in the Bhawans
- Offices using the system will install biometric enabled terminals / devices to mark attendance; the number and location of required devices will be assessed by the offices; the offices concerned will be responsible for day-to-day maintenance of the devices
- Connectivity of terminals / devices will be established through Wi-Fi/GPRS
- Customized reporting formats for various levels of employees will be developed by UIDAI/NIC
- Facility for centralized compilation and publication of attendance data in public domain will be provided as per requirements

2. About Biometric Attendance System (BAS)

Government Organizations are operating across different locations. The major challenge is to enable and manage the attendance of the Government workforce across various locations keeping the Total Cost of Ownership (TCO) low.

Presently, various Government Organizations have deployed proprietary biometric attendance solutions, which lack uniformity in technical architecture due to which these solutions are difficult to scale up and integrate with each other.

Aadhaar based biometric Authentication for the purpose of attendance would ensure that the attendance of all the Government employees will be visible in real time on the common attendance portal ensuring transparency and accountability to bring efficiency.

2.1. Salient Features of cloud based BAS solution

Following features are envisaged for Common Bio-metric attendance System:

- This Biometric Attendance System is based on Aadhaar Authentication (Fingerprint and Iris Based Authentication).
- It is an attendance system with real time monitoring
- The system has comprehensive MIS
- This is a lightweight system which does not requires any special hardware or algorithm
- It is compatible with multiple platforms (Windows, Android, etc.) and form factors (Laptop, Desktop and Tablets, etc.)
- Robust System- Self sustained for small power cuts as it uses tablets at the front end.
- Time taken to Record Attendance is as low as 1-2 Seconds on Wi-Fi and 8-11 Seconds on GPRS (SIM)

- System is tightly integrated with the communication channel of SMS. A user gets SMS's from the systems at various levels like after registration, on non-marking of attendance and other conditions to empower the users of the system.
- The System has an in-built leave management system wherein an employee can be marked *"on leave"* so that the system recognizes him/her as on leave and does not send a late attendance SMS.
- The system maintenance is largely automated. Examples are: centralized monitoring of devices – through a dash-board, push-based updating of software on devices and PCs over the air, automatic fall back on SIM based connectivity once the Wi-Fi connectivity goes down and centralized scheduling of shut-down of devices during out of office hours. The efforts are on to make the system even smarter in future.

2.2. Why BAS? Merits of the System

Hardware: The system in simple to deploy due to no hardware lock in or vendor dependency. The hardware used for this system is neither specially manufactured nor is based on a technology patented by a particular company. This means that this system can be installed on any tablet working on android operating system or any desktop personnel computer or even a laptop working on windows platform .The system requires one STQC certified Fingerprint/Iris Scanner Device that follows the specifications of the UIDAI has to be attached to the host device.

Software: The client software for the biometric attendance system has been made in house by DEITY and is readily available. There are two separate versions of software available for desktop PCs running windows and android based tablets. All the supported biometric devices are integrated into the application. The software is a simple client application with no special algorithms. Modification and incorporation of additional features in the software is easy.

Connectivity: The system uses multiple internet connectivity channels and has an inbuilt fallback mechanism. The biometric device works on any available connectivity that is supported by the device on which the application is installed. The Tablet application uses Wi-Fi as well as GPRS with an auto switch mechanism to determine the best connectivity option. The desktop application can be used over Wi-Fi, Ethernet or Data Card connectivity option and Android tablet application can be used over Wi-Fi, GPRS/WCDMA options.

Accessibility for the employee: In order to make this system portable, it has been designed on a central architecture. Every client system is connected to the server in real time, the employee data resides on the central server and the changes are also made in the database of the central server for any transaction at any client at any location. This means that employees are not restricted to mark attendance from a designated client or a location. There is a strong client management and analysis system inbuilt which is capable of analyzing the transaction data of the clients for any anomalies.

Scalability: The system has been built with scalability in mind. Therefore any new office, employee or client can be on-boarded easily. The system can support practically unlimited number of clients.

Security: There is a proper mechanism of registration of any new client or any piece of hardware in the system before allowing it to be active to ensure safety of the system. Aadhaar authentication is highly secure system of biometric authentication, which adds to the security of the system. As the system uses this service, the sensitive biometric data resides in the secure Central Identities Data Repository of UIDAI. The biometric data captured locally by client is securely communicated to the UIDAI server for authentication and not stored in the system at any point of time.

Ease of Use: This is an extremely user friendly system where the employees can do online self-registration, update of their profile and details. The registered employees also get SMS Alerts on events of importance. This system can also monitor the health of attendance terminals centrally which makes is easier for the implementers to do maintenance work.

2.3. High level Architecture

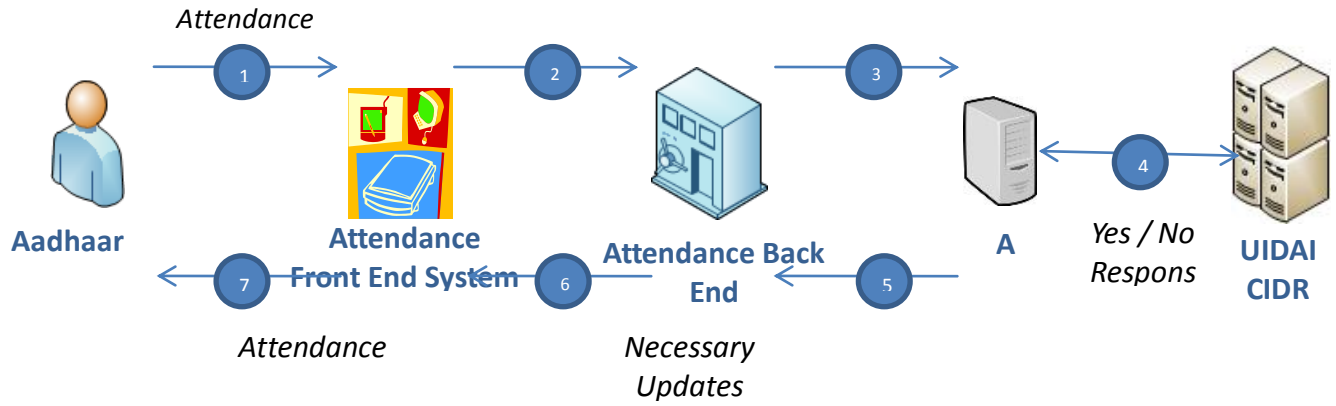
At a high level the overall solution would have two main components

A. Front End System

The Front End System (FES) or the attendance system would be a device having hardware and client attendance application. The client attendance module in the idle state would wait for user to enter his/her attendance id through touch screen in case of tablet based client or keyboard input in case of desktop based client. This attendance id would usually be first 6 digits or last 6 digits of the Aadhaar number of the employee. Once the attendance id is captured, the application would prompt user to provide the biometric data required for Aadhaar online authentication. It would then create the request in accordance with the Aadhaar Authentication API and send the request to the backend application at UIDAI Central Identity Data Repository (CIDR).

B. Back End System

The Back End System or attendance server would create Aadhaar Authentication request, submit the request and receive the response in accordance with Aadhaar Authentication API requirements. It will mark in/out attendance, attendance system activation/de-activation and generate reports for the same. The picture below represents a high level schematic diagram of the Biometric attendance system.



Schematic diagram of BAS System

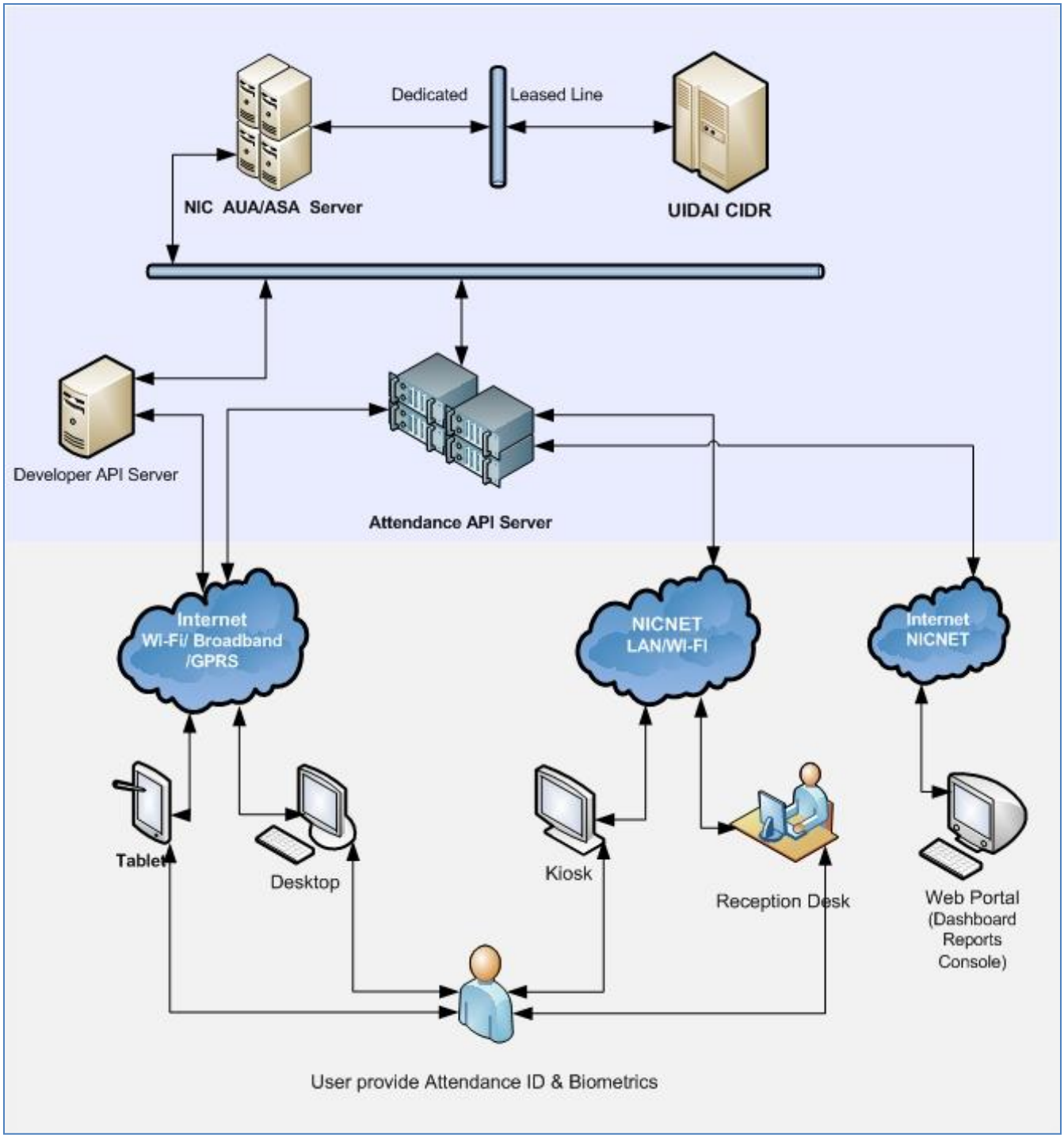


Figure 1: BAS Application Overview

2.4. Comparison with Traditional bio-metric attendance systems

Aadhaar based attendance system has an edge over the other traditional biometric attendance systems in many respects. The traditional biometric systems are not designed for scale as the machines generally store the biometric fingerprints locally. These systems have to be connected with LAN cables of the institutions network and cannot be monitored from global locations due to the dependency on the institutions connectivity ecosystems. The cost involved in these traditional biometric systems are also quite high and one terminal which can store 3000 to 10000 biometric fingerprints costs around Rs. 13000 to Rs. 25000.The traditional systems use terminals which authenticate biometric attributes locally and then push data to a server. Another challenge is to get registered in these systems as the user along with demographic details has to get all fingers enrolled as well which can happen on these terminals only.

Comparatively, this Aadhaar Enabled Biometric Attendance System needs only Aadhaar number, basic demographic details and a photograph of the user at the time of user registrations. This can be done by the employee himself/herself by on simple web based system. The biometric details are already available with the UIDAI which are then used for authentication. Moreover, this system ensures unique users as the user registration is stored on a central attendance server and Aadhaar ensures de-duplication through its 1: N check mechanism. In this system, the Management Information System is accessible from any global location to anyone which is very useful in bringing transparency and accountability to the entire system. This is a highly adaptable system with minimum cost requirements. Any agencies which work in the public sector can easily get incorporated in the system by setting up handheld devices which are nothing but a combination of an android tablet, a fingerprint scanner enclosed in a frame. This setup costs extremely less and the management information system does not require any resources or manual intervention. This makes it a highly cost effective system.

3. Current Status

Following activities have been completed during Phase I

- A common biometric attendance portal viz. attendance.gov.in has been developed. The attendance portal is hosted in NIC data center. These centralized back-end servers are common which will be used by all Central Government organizations for biometric attendance system.
- In the first phase of implementation, approximately 150 central Government organizations have registered more than 55,000 employees on common attendance portal i.e. attendnace.gov.in.
- UIDAI team has developed back-end portal software and client side attendance software.
- 1000 wall mounted biometric terminals and 5000 desktop STQC certified finger print devices have been installed in various Ministries/Departments located in about 100 Bhawans/Buildings in Delhi. For phase-I all the devices have been procured and installed by NIC by UIDAI funding.

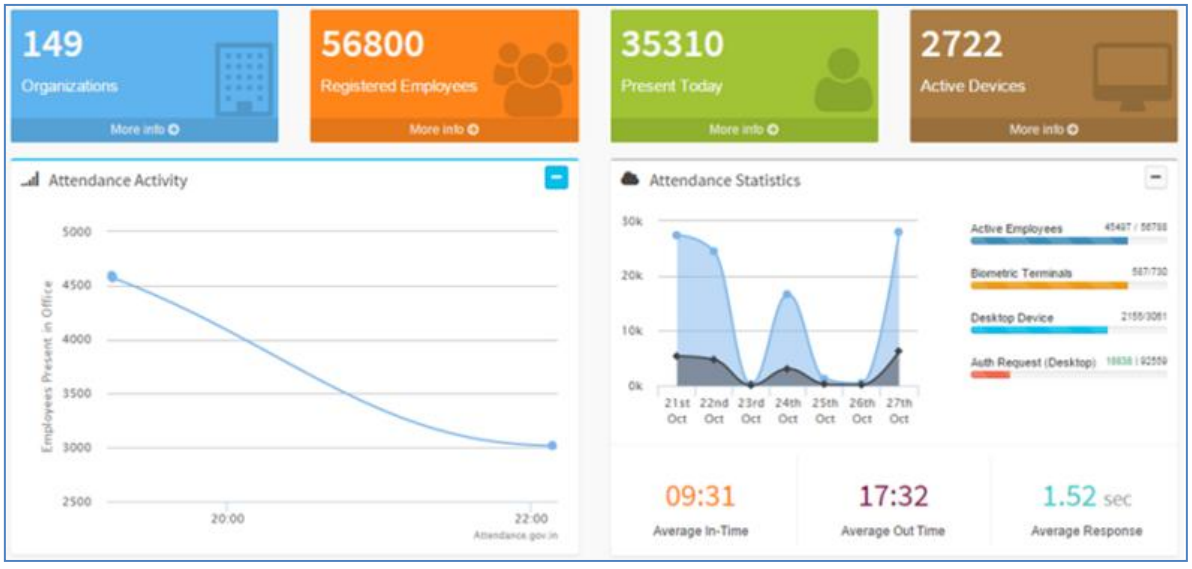


Figure 2: Phase I Metrics

4. Way forward: Proposed plan of Action

In **Phase-II**, it is proposed that

- Government organizations that could not register in phase-I shall register on attendance.gov.in portal for the implementation of biometric attendance system in phase II. All the central Government organizations shall use the common back-end infrastructure installed at NIC data centers.
- First step towards using bio-metric attendance system will be to appoint a nodal officer by each organization and register all their employees on-line at attendance.gov.in. This will undergo two steps of verification, first the Aadhaar verification by UIDAI and second verification by the appointed nodal officer. After that, the employee will be able to mark his/her attendance from biometric terminal to be installed at the user location.
- The Government organizations shall procure the wall mounted biometric attendance terminals and desktop finger print devices in a decentralized manner from the rate contract which will be finalized by DGS&D and alternatively, they could also procure these devices through NICSI or through open tender. The devices used in phase I have also been procured through NICSI.
- The Government agencies shall provide connectivity from various telecom service providers for connecting the bio-metric attendance terminals (GPRS/Wi-Fi using NICNET/Broadband/existing Internet) in a decentralized manner.
- Government organizations shall make suitable provision for getting Client 'API' installed on the software provided for wall mounted and desktop finger print devices.

The Government organizations shall be responsible for maintaining the devices installed in their premises and will be responsible for smooth day-to-day functioning of the Bio-metric Attendance terminals.

5. On-boarding guidelines

Organizations interested in using BAS are required to follow process guidelines for smooth switchover to the modern and futuristic BAS.

5.1. Identification of Nodal Officer

To facilitate the implementation and thereafter operate the Biometric attendance system, it is desired that the Ministry/Department shall nominate a Nodal Officer not below the rank of Joint Secretary for acting as a Single Point of Contact (SPoC) for driving the Bio-metric attendance initiative. The Nodal Officer shall be responsible for:

- Monitoring and co-coordinating with the stakeholders for smooth functioning of the Bio-metric attendance system
- Providing update facility for biometric updating in case of poor bio-metric capture during enrolment process and in cases where there are failures in detecting the fingerprints by organizing Aadhaar camps.
- Organizing special Aadhaar Enrolment Camps (AECs), if considerable numbers of employees are not able to register on the portal due to non-availability of Aadhaar numbers.
- Aadhaar number generation for the enrolments done in the AECs
- e-Aadhaar access
- Best Finger Detection and other Aadhaar related issues

The agencies may use the format placed at Appendix 'A' for capturing the details of the organization as well as Nodal Officer.

5.2. Registration of Organization

The Organizations are required to register online (once) on the portal for using attendance.gov.in by giving number of employees and their existing website name. Once the registration of the organization is complete, the organization will be listed in the portal for the enrolment of the employees and generation of various types of reports pertaining to the organization. The steps for on-boarding organization in the attendance portal can be found in Appendix 'B'.

5.3. Registration of Employees

Once the organization is registered with the attendance portal, employees of the organization are required to do online registration on attendance.gov.in portal for enabling them to mark attendance. The employees need to fill an online form using the link 'Employee Registration' on the attendance portal. Once the details are filled, the employee data goes to the quality check team of UIDAI/Nodal Officer of the organization for verification. After the approval from the nodal officer, the employee becomes active in the attendance portal and can mark its attendance through the devices installed. The details are required for on boarding of employees in the attendance portal can be found in Appendix 'C'.

5.4. Aadhaar Enrolment

One of the mandatory requirements for registering on the common bio-metric attendance system is a valid Aadhaar Number of the employees for enabling him/her to mark attendance. In order to facilitate the BAS implementation, UIDAI can organize Aadhaar Enrolment Camps (AECs) for all such employees, who do not possess Aadhaar numbers. UIDAI shall also extend its support for the employees who have already enrolled but have not yet received their Aadhaar, or have lost their Aadhaar, or for those who need to update their Aadhaar data.

5.5. E-Aadhaar access

To enable downloading of the Aadhaar for the employees who have enrolled but have not yet received their Aadhaar, or have lost their Aadhaar or did not received Aadhaar due to any reason whatsoever, UIDAI has provides access to e-Aadhaar facility to HoDs of the NIC deputed in various Ministries/Departments. The employees can get in touch with their respective HoDs of NIC to get their Aadhaar downloaded.

5.6. Best Finger Detection (BFD)

In order to increase the chances of the Aadhaar Authentication while marking attendance, UIDAI has also extended the facility of Best Finger Detection (BFD) to all the Head of Departments (HoDs) of NIC in the respective ministries or departments. Those employees, who are facing frequent authentication failures while marking attendance, can get their best finger identified from the device installed in the NIC cell in respective Ministry/Department. After identification of the Best Finger, the employee can use the identified best finger for marking attendance with an increased chance of success for Aadhaar Authentication.

5.7. Biometric Terminals (Devices)

As illustrated in the high level overview of the system it is mandatory to have devices aka biometric terminals installed for the purpose of attendance punching. These devices act as an interface for the end user to punch his attendance in the system, which in turn interacts with various API's to record the event in the central database.

The Biometric terminals may typically use the following components:
(Specification mentioned in Appendix 'D')

a. Tablet – machines with the capability to run the BAS client software.
b. Desktop – PC or laptops running Windows 7/8 can also be used to run the BAS software.
c. Fingerprint reader – these refer to the biometric fingerprint reader devices which capture the fingerprints of the user.
d. Iris scanner – these are used to capture the IRIS image of the user and do iris authentication

The biometric terminals can be setup using either of the above combinations, typical setup used in the Phase I of the project is:

i. **Tablet** setup - the wall mounted devices used in phase I are Android OS running tablets, with either finger print reader or iris scanner together housed in a cabinet to present an integrated device feel. The BAS software for android is readily available for download from the portal. Since network connectivity is mandatory for working these tablet devices are connected through Wi-Fi access points and are also equipped with a 2G sim card for GPRS connectivity for network failover support.

ii. **Desktop** setup - normal PCs on which the BAS windows version application can be run and the finger print or iris scanner are attached through usb ports are also being used to mark the attendance. The PCs are generally connected through the Office LAN network and alternatively dialup or broad band connections can be used for network connectivity. The fingerprint and iris scanners are readily available with drivers for windows platform, use of Office PCs can be the shortest route to get started with BAS as the requirement would be procurement of biometric scanner devices.

5.8. Procurement of Devices

The Organizations registering in phase-II or organizations who have registered during phase I but need additional devices, can procure the wall mounted bio-metric attendance terminals, desktop finger print and iris scanning devices through the following methods:

a. NICSI - devices are readily available for procurement through the empanelled vendors
b. Open Tenders – devices can also be procured through open tenders but device specification should adhere to Appendix 'D'
c. DGS&D - rate contracts are still being finalized, and will be available shortly

DGS&D has been requested to empanel vendors for supplying the devices required for installing bio-metric attendance system using common back-end infra-structure at NIC data centers.

The organizations will have the option of selection of following devices for implementing BAS.

1. **Integrated Attendance Device (IAD) – Type 1:** These are Android Tablet based devices integrated with Single STQC certified Fingerprint (FP) scanner. Both the Tablet and FP device are then housed in rugged casing so that the Integrated Attendance Device could be suitably mounted on the wall as single unit. The specification of the Type-1 devices is mentioned at serial 1 of the table provided in appendix 'D'.

2. **Integrated Attendance Device (IAD) – Type 2:** These are the devices manufactured as a Single Unit with a capability of punching attendance number as well as scanning fingerprint for recording attendance. The specification of the Type-2 devices is mentioned at serial 2 of the table provided in appendix 'D'.

Note: the Bio-metric attendance system is to be implement using wall mounted devices for the employees at large. However, for senior level officers or in a section, there is provision of installing Bio-metric attendance system using USB based finger print scanning device/IRIS with a Windows 7/8 Desktop PC.

It is estimated that for every 50 employees, one wall mounted bio-metric attendance terminal would be sufficient and for every 20 employees one finger print scanning device on a desktop would be sufficient. Therefore, the total requirement of wall mounted biometric terminals as well as desktop devices could be estimated based on total number of employees in the department. However, depending upon the on-ground circumstances, the organizations can procure additional number of devices, if required, for smooth implementing BAS. The indicative specifications of the devices required for the installation of the BAS can be found in Appendix 'D'.

5.9. Procurement of Connectivity

Biometric attendance terminals installed at client locations would need Wi-Fi connectivity through Internet/NICNET for communicating with the back-end attendance servers, which are installed at NIC data centers. The organizations would need to procure connectivity (GPRS/Wi-Fi using NICNET/Broadband/Internet) from suitable service providers.

Looking the high traffic load during peak hours (8 am -11.00am and 4pm – 7pm), the minimum 1mbps of bandwidth connectivity would be required for proper functioning of Biometric attendance terminals.

The agencies may use the format placed at Appendix 'E' for capturing the connectivity requirements.

5.10. Site Identification and Preparation

The wall mounted biometric terminals arête be preferably placed at the entry/exit points with 24 hours security for enabling easy access to the employees for marking attendance. The organizations registering in phase – II shall ensure the locations identified for installing biometric attendance terminals should have the following: -

- 220V/5A Electrical points
- Suitable security within the premises
- Protection from environmental conditions like rain, sun, etc.
- LAN point for connecting Wi-Fi access devices
- Good data connectivity through GPRS/3G as a backup connectivity

The agencies may use the format placed at Appendix 'F' for capturing the site requirements.

5.11. Installation of Devices

The Organizations shall take up the installation, commissioning and maintenance of the Biometric attendance terminals in their premises with the help of vendors who are empanelled with DG S&D. UIDAI, NIC and DeitY shall extend all technical support for integrating back-end infrastructure.

5.12. Operations & Maintenance

The Organizations shall be responsible for maintenance of the devices installed in their premises. The agencies will also be responsible for taking suitable on-site warranty support for smooth functioning of BAS.

Appendix 'A' – Application format for Organization On-boarding

Organization Type	[ ] Ministry [ ] Department under Ministry [ ] Attached Office
Organization Name	
Address	
District	
State	
NIC Coordinator Mobile	
NIC Coordinator e-Mail	
Website	
No. Of Employees	
Office Timings	

Nodal Officer Name	
Aadhaar No	
Designation	
Mobile	
E-Mail	

Date:

Name & Designation
Head of the department with Signature & Seal

Appendix 'B' – Steps for on-boarding an Organization in the attendance portal

1. Select the 'Organization Registration' link in the attendance portal
2. Fill the downloaded form with the required information and get it signed by the Head of the organization/department, with the organization stamp/seal.
3. Scan the filled, signed & stamped form and save it in ".jpg" format of max file size 200 Kb. The scanned file has to be uploaded in the online form in the attendance portal.
4. Steps to fill the online form in the attendance portal
    - Select the name of your organization. If the organization name does not show than please get in touch with the Attendance help desk.
    - Enter the communication address of the organization
    - Select the state (as applicable)
    - Enter the Mobile number of NIC coordinator
    - Enter the email address of NIC coordinator
    - Enter the name of the nodal officer
    - Provide the Aadhaar number of the nodal officer
    - Enter the designation of the nodal officer
    - Enter the Mobile number of the nodal officer
    - Select the scanned file which you need to upload with the form
5. Review the form for any changes before submission.

Note:

a. After submitting the form, a One Time Password (OTP) will be sent to the nodal officer email and mobile, to verify the form data submitted.
b. After your request is processed, you will receive an email with your account details.
c. If your organization does not feature in the list, please get in touch with the Attendance helpdesk at **helpdesk-attendance@gov.in**.

Appendix 'C' – Details required for registration of employees in Attendance portal

1. Enter Full Name.
2. Enter Date of Birth (format DD-MM-YYYY)
3. Select Gender.
4. Please provide 12 digit Aadhaar number
5. Enter Email. And 10 digit Mobile Number.
6. Select the name of Organization. If the organization does not list, please get in touch with Organization's Nodal Officer to get your organization listed.
7. Select Employee Type
8. Enter the name of Division/Unit within the Organization (you can choose from suggestions)
9. Select Designation (only when Employee Type is Government)
10. Select office location.(e.g. your office building name)
11. Upload scanned/digital picture in ".jpg" format of max file size 150KB.
12. Please enter the captcha code.
13. Please review the form before submission.

Note:

a. If Organization does not feature in the Organization list, please get in touch with your Nodal officer for getting the Organization on-boarded in the Attendance system.

b. If any of the pre-requisite information is not available in the form (select options only), please get in touch with the concerned officer in your department to get the details updated.

For any other assistance please get in touch with the Attendance Helpdesk at helpdesk-attendance@gov.in.

Appendix 'D' – Indicative specifications of the Devices to be used in BAS

S.NO.	ITEM	SPECIFICATIONS
1.	**Integrated Attendance Device Type 1 - Integrated Android Tablet and Single Fingerprint Scanner Device Housed in Rugged Casing**	• Specifications of Android Tablet same as those given for Item No. 3 • Specifications for Single Fingerprint Scanner Device same as those given for Item No. 4 (STQC Certificate for the integrated bio-metric device must be submitted) • Android Tablet and Single Fingerprint Scanner should be integrated in a rugged casing. **The Rugged Casing should comply with the following:** • The casing should be made of inflexible, solid material and can be of polycarbonate / thick plastic / acrylic / other tough material. • It should be of black color and should have a glossy / matte finish • Acrylic casings must have a thickness of at least 5 mm. • Casing should be durable and should be able to withstand rough daily operational usage. • The casing should not suffer any damage or disfiguration on being dropped from a height of up to 2 meters • Tablet should be vertically oriented in the casing. This is important because the attendance application to be deployed is designed to run in vertical mode only. • The casing should be designed to cover/hide the android task bar of the tablet. This is required to prevent misuse of any other functionality of the tablet. • The casing should have provision to access the power/reset button of the tablet. The access should be easy but controlled. The vendor thus should make arrangements to provide an external tool to perform the power on/off and/or reset function of the tablet through the casing. • The fingerprint scanner should be ergonomically placed to support ease of usage for biometric attendance in standing posture of the users.
2.	**Integrated Attendance Device Type 2 - Integrated Attendance Device**	An integrated device for recoding biometric attendance with STQC certified fingerprint sensor meeting following configurations / requirements • Display – At least 4 inch display with a minimum of 800x480 pixel resolution, 16 M Colors • Processor- 1.0 GHz or above

S.NO.	ITEM	SPECIFICATIONS
	Manufactured as a Single Unit	• RAM- 512 MB or above • Hard Key / Soft Key Numeric key pad • Internal Storage- 4GB or above • Expandable storage through micro SD, minimum 8 GB • USB Port- Minimum one available USB host port to support application loading / configurations / full functional keyboard • Device must come with connector cables to allow connection of the device to Micro USB and Standard USB ports • Internal Speakers • GSM SIM card slot • Inbuilt replaceable battery with min. battery backup of up to 120 minutes • Charging / operation on AC 100 -240 volt range with inbuilt surge protection **Biometric sensor/extractor** • STQC certified fingerprint sensor/extractor for Aadhaar authentication (STQC Certificate for the integrated bio-metric device must be submitted) • SDK for fingerprint device • The fingerprint scanner should be ergonomically placed to support ease of usage for biometric attendance in standing posture of the users **Connectivity Requirements** • Mandatory Edge / 3G mobile data support • Wi-Fi IEEE 802.11b/g/n OR LAN (Ethernet) interface OR Both • Strength, safety and operating environment • Should be able to withstand 1 m drop test • Operating temp: 0°C to 50°C • Storage not including battery: 0°C to 55°C • CE certification/ RoHS certification • SAR values within acceptable range **Operating system / software requirements** • Android 4.0 Operating System or above • Sample application to test fingerprint sensor/extractor • Vendor has to provide all necessary technical support for integration of their device drivers with the attendance software and associated UIDAI applications.
3.	**Android Tablet with 7 inch**	• Processor- 1.0 GHz or above • RAM- 512 MB or above

S.NO.	ITEM	SPECIFICATIONS
	screen	• Internal Storage- 4GB or above • Expandable storage through micro SD, minimum 8 GB • USB Port- Minimum one Micro USB port and an optional additional USB Port • USB port should provide power supply to biometric device and support USB OTG. • Front facing Camera with VGA resolution • Internal Speakers • 7''Capacitive touch screen and minimum 800x480 pixel resolution or above, 16 M Colors • GSM SIM card slot • Min. Battery backup up to 120 minutes • SAR values within acceptable range • Separate charging non-usb port with AC adapter 200-240 volt range • Micro USB host cable • Connectivity Requirements • Mandatory Edge / 3G mobile data support • Wi-Fi IEEE 802.11b/g/n OR LAN (Ethernet) interface OR Both • Software Requirements • Android 4.0 Operating System or Above • Safety and other standards compliance – CE certification/ RoHS certification • Full featured Web Browser • Application to be deployed on android tablet will require rooted Android OS • Vendor has to provide all necessary technical support for integration of their device drivers with the attendance software and associated UIDAI attendance applications.
4.	**Single Fingerprint Scanner Device for use with Android Tablet**	• STQC certified Single Finger-print biometric device for Aadhaar Authentication with driver, in-built template extractor software/SDK (mandatorily with license, if required) (STQC Certificate for the device must be submitted) • API/SDK for Android (4.0 and above) platform. • Device should be plug and play with any android (4.0 and above) tablet without need of any additional license to be deployed. • The device should have integrated micro USB or standard USB type connector. • Device must come with connector cables to allow connection of the device to Micro USB and Standard USB ports

S.NO.	ITEM	SPECIFICATIONS
		• Vendor has to provide all necessary technical support for integration of their device drivers with the attendance software and associated UIDAI applications.
5.	**Fingerprint Scanner Device for use with Desktop**	• STQC certified single finger-print biometric device for Aadhaar Authentication and extractor software/SDK (STQC Certificate must be submitted) • API/SDK for Windows (7.0 and above) platform. • Device should be plug and play with any Windows (7.0 and above) without need of any additional license to be deployed. • The device should have integrated USB 2.0 type connector. • Device must come with connector cables to allow connection of the device to Micro USB and Standard USB ports • Vendor has to provide all necessary technical support for integration of their device drivers with the attendance software and associated UIDAI applications.
6.	**Iris Authentication Device for use with Desktop**	• STQC certified Iris authentication device for Aadhaar Authentication and extractor software/SDK (STQC Certificate must be submitted) • API/SDK for Windows (7.0 and above) platform and Android (4.0 or above) Operating System • Device should be plug and play with any Windows (7.0 and above) and Android (4.0 and above) without need of any additional license to be deployed • The device should have integrated USB 2.0 type connector. • Device must come with connector cables to allow connection of the device to Micro USB and Standard USB ports • Sample application for Windows and Android platform to test Iris sensor/extractor • Vendor has to provide all necessary technical support for integration of their device drivers with the attendance software and associated UIDAI applications.

Appendix 'E' – Format for Connectivity Requirement

S. No	Organization / Location Name	Address or the location identifier (such as entry /exit number/floor etc.) where the device would be installed	Is LAN point available at the point where device is to be installed (Yes / No)	If (3) is No then Can Wi-Fi be placed using nearby LAN point in the location (Yes / No)	If (4) is 'No' then a LAN I/O point is required to be installed (Yes/No)
	(1)	(2)	(3)	(4)	(5)
1					
2					
3					

Appendix 'F' – Format for Site Requirements

S. No	Organization / Location Name	Address or the location identifier (such as entry /exit number /floor etc.) where the device would be installed	Do electrical power point available at the point where device is to be installed (Yes / No)	If (4) is 'No' then an electrical point (220V/5A)point is required to be installed (Yes/No)
	(1)	(2)	(3)	(5)
1				
2				
3				