Unique Identification Authority of India ((UIDAI)

STANDARD REQUEST FOR PROPOSALS

FOR PROVIDING APPLICATION SOFTWARE DEVELOPMENT, MAINTENANCE, & SUPPORT SERVICES TO UIDAI

VOLUME II: UID APPLICATION OVERVIEW AND REQUIREMENTS

January 25th, 2010

Contents

The UID System

Intent of UIDAI

The UIDAI has been setup by the Government of India with a mandate to issue Unique Identification numbers (UID Numbers) to all the residents in the country. UIDAI proposes to create a platform to enrol the residents of the country, issue UID Numbers. These numbers may then be used for authentication. This can be used by several government and private organizations for better delivery of services to residents.

The purpose of the UIDAI is to issue UID Numbers that are (a) robust enough to minimise / eliminate duplicate and fake identities, and (b) can be verified and authenticated in an easy, cost effective way. UIDAI will use common demographic and biometric data for establishing and verifying identity, therefore, it becomes essential to standardize these data fields and verification procedures across its registering partners (Registrars). This will aid interoperability across many systems that capture information and work with the residents.

UIDAI has selected biometrics feature set as the primary method to check for duplicate identity records. In order to ensure that an individual can establish their identity uniquely in an easy and cost-effective manner, it is essential that the captured biometric information is of a quality and standard that is capable of being de-duplicated. Further, for authentication of identity at the time of service delivery by government and private organisations, it is essential that the biometric information capture and transmission are standardized across all users of the UID Application.

In order to set these standards two committees were set up by the UIDAI. The Demographic Data Standards and Verification procedure Committee constituted under the Chairmanship of Shri N.Vittal and the Biometrics Committee chaired

by Dr. B.K.Gairola, Director General NIC, have submitted their final reports. These reports are available on the UIDAI website "uidai.gov.in".

Understanding UID System

India will be the first country to implement a biometric-based unique ID system on such a large scale. The UID will serve as a universal proof of identity, allowing residents to establish their credentials anywhere in the country. It will give the government a platform to monitor and track services and resource flows effectively, thereby achieving greater returns on social investments. Confirming 'you are who you say you are' remains the primary, often elusive goal of all identity systems.

The UIDAI approach – which will be online authentication, with biometric check – creates a very strong authentication system, and gives the UIDAI significant ability to confirm an individual's identity.

Goals of UID System

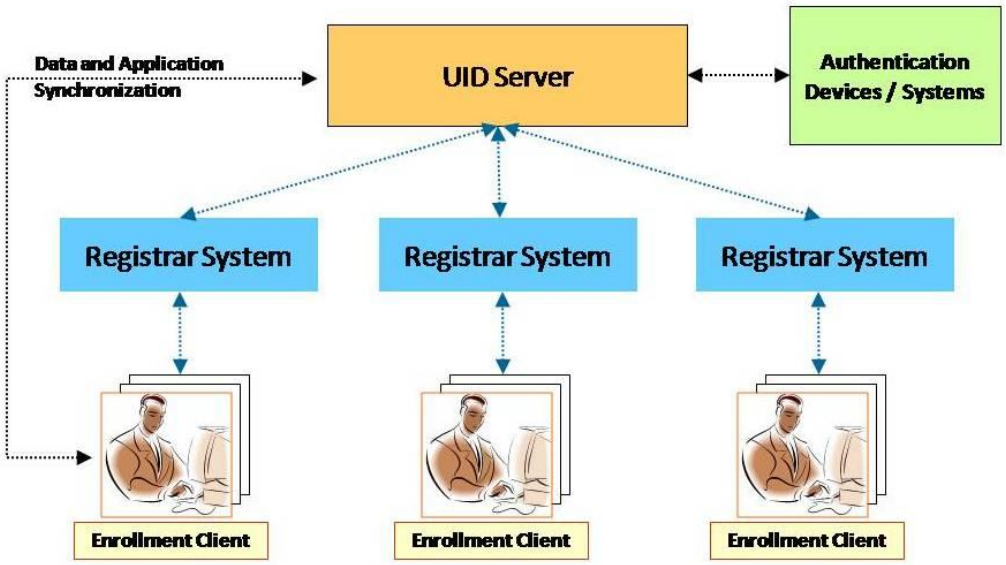
For details on the goal of UID system, refer to the document on UIDAI's website titled "Creating a unique identity for every resident in India - Draft approach" (http://uidai.gov.in/documents/Creating%20a%20unique%20identity%20for%20every%20resident%20in%20India.pdf).

Key Features of UID System

- **Identity** – every resident can have a lifelong ID that is common across systems.
- **Authentication** – Is the process of ascertaining a person's identity, supports answering the basic question "is a resident the person he/she claims to be".

- **Standardization** – Standardization of Know Your Resident (KYR) Data and Processes, and Biometric Standards in order to achieve interoperability across several users of the system.

High Level System Overview



- **UIDAI** – The Authority that will issue UID numbers and set standards for enrolment and authentication to be universally followed. UIDAI will among other things will design, develop, and deploy the UID Application with the help of service providers.
- **Registrar** – Any government, private or non-governmental agency that can enrol and use online authentication using the UID Application.
- **Enrolment Agency** – The agency that will actually enrol residents by capturing their demographic and biometric information in the field. They will be setup or employed on behalf of the Registrar.
- **UID Server** – The central server that responds to enrolment and authentication requests.
- **Registrar System** – The Registrars' IT systems and processes.
- **Enrolment Client** – Software provided by the UIDAI to Registrar/Enrolling Agencies in order to enrol residents into the UID system.

UID Data and Biometric Standards

Demographic Data Standards

In order to fulfil its purpose, the UIDAI should stay focused on its goals and ensure standardisation. Therefore, it is important that the KYR data is kept to a usable minimum so as to support purpose of UIDAI and to **avoid** other profiling and transactional fields.

Names and Addresses

Names in India can range from a single word to many (sometimes even 5 or more) words in length depending on the region, caste, religion, etc. A standardized structure for names needs to be created for common KYR and interoperability between various systems.

Additionally, the country does not have a standardized national address format or well documented geographic boundaries beyond the village level. This creates issues when trying to map addresses in a standard way. Various forms issued by existing Registrars vary greatly when it comes to capturing addresses.

The Demographic Data Standards and Verification procedure Committee looked into standardization of name and address structure to enable uniformity across the country, recommended the fields which the UIDAI should capture and also prescribed the verification process for the fields.

UID Number Format

The design of the UID number format is based on several principles and requirements:

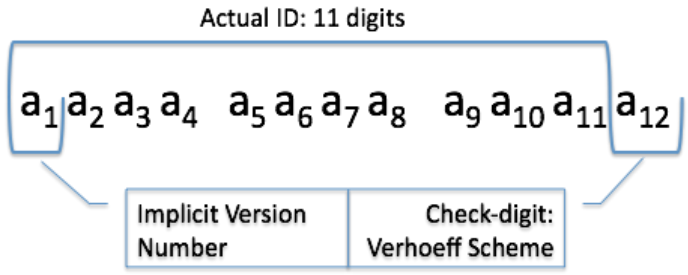
- The Unique Identifier should simply be a number and not include alphabets since a specific alphabet brings dependency to a specific script/language and literacy.
- The number should be semantics-free. Apart from reserving two special values for the first digit and the last digit (used as check digit), the remaining number value will be generated using a randomized process at the time one requests a new ID.

12 decimal digits will be sufficient to satisfy all the requirements, outlined below.

- The number should support 80 to 100 billion ID's at the outset. In other words, there should be at least 11 digits available for actual numbering.
- The number should be extensible with backwards compatibility to have more decimal digits, for example, 20 digits, if a need should arise in future. This can be accomplished by reserving a value of 0 for first digit of the number
- There should be well known, reserved numbers for purposes outlined below.
- The number should have an error detecting check digit that detects as many data entry errors as possible.
- To make it harder to guess a correct valid ID assigned to anybody we propose a much larger space (80 billion IDs) than the maximum number of IDs needed at anytime (estimated to be about no more than 6 billion IDs). This notion is captured by the density, which we define as a ratio of total number of ID's assigned to the total number of IDs available. Our target is that by design we keep this ratio below 0.05 at all times. The sparseness of the numbers will make it difficult to simply guess numbers. The check digit is another form of sparseness but, being a publicly disclosed algorithm, will not prevent guessing. The check digit enables error detection at data entry.
- There may be a need to assign UIDs to entities such as schools, companies and other institutions to facilitate symmetry in transactions between residents and entities. For example, financial transactions for NREGA scheme may deposit NREGA wages direct from a Gram Panchayat to a

particular resident. Such transactions could take the form: "TransferMoney(GramPanchayat_UID, Resident_UID, Amount)". While several other backend systems need to be in place for such transactions to take place, currently we are making a provision to assign up to ten billion entity UIDs. This requirement is met by reserving the value 1 for first digit (a1=1) to entity UID numbers.

Number Design



The format of 12-digit number is discussed below.

- The Version Number: Some digits may be reserved for specific applications. This is an implicit form of a version number embedded into the numbering scheme. We recommend the following reservations:

  0 - numbers (a1 = 0) could be used as an "escape" for future extensions to the length of the number. For example, in future if we need 16 digit numbers, then we could say that 0 means that the number is 16-digits. As of now we can simply declare all 0 - numbers as TBD (to be decided).

  1 - numbers (a1 = 1) could be reserved for entities rather than individuals. Alternatively, 11 could be reserved for entities (or 111) to match the size of the reserved space to the number of entities expected.

  We could use 2-9 numbers (a1 =2, 3… 9) right away to assign UIDs. That is 80 billion numbers -- plenty of space.

- Number Generation: The numbers are generated in a random, non-repeating sequence. There are several approaches to doing this in the computer science literature.

- Lifetime: Individual UID number is assigned once at inception and remains the same for the lifetime of the person, and for a specified number of years beyond. At this point there is no consideration of reusing numbers.

- Entity ID's: We expect that entity ID numbers (1- numbers) will have different rules for periods of validity and retirement.

UID for Infants and Children

All children will be assigned a UID number. It is very important for several service organizations such as education and health to be able identify children uniquely in order to deliver services effectively. Children's' fingerprints are not fully formed and hence cannot be used for de-duplication given the current state of technology.

Hence during enrolment, details of the parents are captured in order to link the child to established UID numbers so that either parent's information can be used to authenticate the child. When the child's biometrics are well-formed (as per biometric committee recommendations), biometric capture will take place and the child will be de-duplicated to ensure the uniqueness of the child. Until the child's biometrics can be used for de-duplication, their UID record will be flagged as "De-duplication not performed".

The best way to ensure that in the future all residents are correctly assigned UIDs is by enrolling infants at birth. This will require the birth registration systems be it manual or computerized get integrated into the UID enrolment process.

Data Fields Summary

Information	Fields	Mandatory / Optional	Data Type
Personal Details	Name	Mandatory	Varchar (99)
	Date of Birth##	Mandatory	Date
	Gender	Mandatory	Char (1) – M/F/T
Address Details	Residential Address	Mandatory	8 address lines and pin code
Parent / Guardian Details	Father's/Husband's /Guardian's Name*	Conditional	Varchar (99)
	Father's/Husband's /Guardian's UID*	Conditional	Number (12)
	Mother's/Wife's /Guardian's Name*	Conditional	Varchar (99)
	Mother's/Wife's /Guardian's UID*	Conditional	Number (12)
Introducer Details	Introducer Name**	Conditional	Varchar (99)
	Introducer's UID**	Conditional	Number (12)
Contact Details	Mobile Number	Optional	Varchar (18)
	Email Address	Optional	Varchar (254)
## *A flag is maintained to indicate if Date of Birth (DoB) is verified, declared, or approximate.*			
* *For infants, Father/Mother/Guardian's name (at least one) and UID is mandatory.* * *For children under a particular age, biometric de-duplication will not be done. Hence their UID will be flagged as such until they are biometrically de-duplicated at a later age (see section on UID for Children). Their UID will be linked to at least of the parent's UID.* * *For adults, Name of either Father/Husband/Guardian or Mother/Wife/Guardian is mandatory. But, an option will be provided to not specify in the case the adult is not in a position or does not want to disclose.*			
** *For residents with no document proof, an "introducer" should certify his/her identity. See later section on Introducer System.*			

Table 1: Data Fields Summary

Data Verification Process

It is essential that key demographic data is verified properly so that the data within UID system can be used for authentication of identity by various systems. There are 3 distinct methods of verification:

- Based on supporting documents
- Based on introducer system (see section 3.5 for details)
- Based on the NPR (National Population Register) process of public scrutiny

All the above forms of verification are acceptable for UID enrolment.

At a high level the 'Personal Details' and the 'Address Details' are mandatory, whereas the 'Parent/Guardian', 'Introducer' and 'Contact' details are optional or conditional.

In order to verify the correctness of certain mandatory fields, such as Name, date-of-birth and address, there is a concept of 'Proof of Identity' (PoI) and "Proof of Address" (PoA). PoI requires a document containing the resident's name and photograph, whereas the PoA contains the name and address.

Verification Summary

Information	Fields	Verification Required?	Verification Procedure
Personal Details	Name	Yes	○ Any of the PoI documents. ○ Introducer for people who have no documents.
	Date of Birth##	No	---
	Gender	No	---
Address Details	Residential Address (for UID letter delivery and other communications)	Yes	○ Any of the PoA documents. ○ Introducer for people who have no documents. ○ Address will be physically

			verified during UID letter delivery. But, resident's physical presence not required during letter delivery.
Parent / Guardian Details	Father's/Husband's /Guardian's Name*	Conditional	○ No verification of Father/Husband/Guardian in the case of adults.
	Father's/Husband's /Guardian's UID*		
	Mother's/Wife's /Guardian's Name*	Conditional	○ No verification of Mother/Wife/Guardian in the case of adults.
	Mother's/Wife's /Guardian's UID*		
Introducer Details	Introducer Name**	Yes	○ Introducer's Name, UID on the form. ○ Physical presence of the introducer at the time of enrolment may not be practical. UIDAI will therefore suggest alternate methods to overcome this practical difficulty.
	Introducer's UID**		
Contact Details	Mobile Number	No	---
	Email Address	No	---
## *A flag is maintained to indicate if Date of Birth (DoB) is verified, declared, or approximate.*			
* *For infants, Father/Mother/Guardian's name (at least one) and UID is mandatory.* *For adults, Name of either Father/Husband/Guardian or Mother/Wife/Guardian is mandatory.*			
** *For residents with no document proof, an "introducer" should certify his/her identity. See later section on Introducer System.*			

Table 2: Process Summary

For complete document, please refer to
http://uidai.gov.in/documents/UID_DDSVP_Committee_Report_v1.0.pdf

Biometric Data Standards

The UIDAI biometrics committee was constituted to provide the UIDAI with direction on the biometrics standards, suggest best practices and recommend biometric modalities for the UID system. These standards govern the biometric specifications required by the UID system.

Details of the committee's findings can be found at
http://uidai.gov.in/documents/Biometrics_Standards_Committee%20report.pdf

Application Architecture

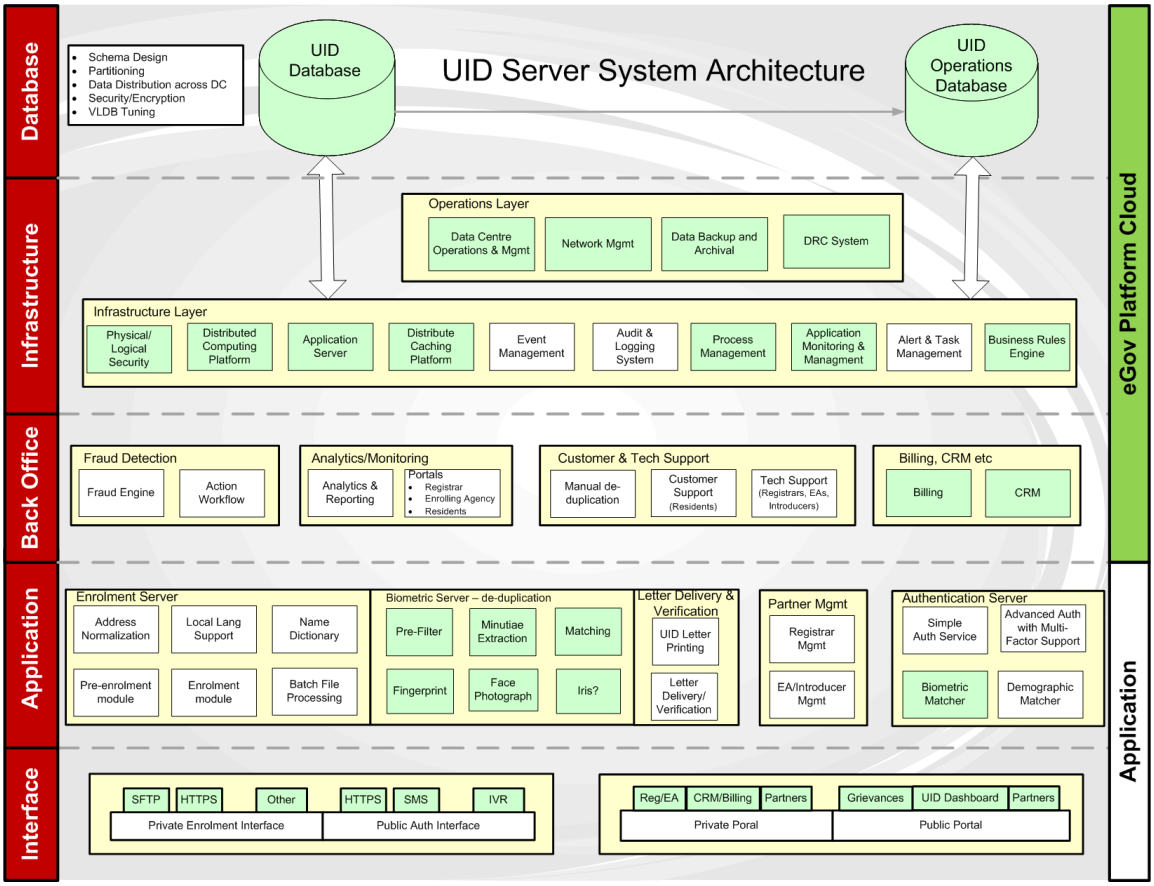
This chapter details out the architecture of the UID application and provide high level descriptions of the various modules within the system. In addition to high level system architecture, this chapter also describes the architecture principles and current choice of various technology frameworks that should be used to build the application.

Architecture Goals

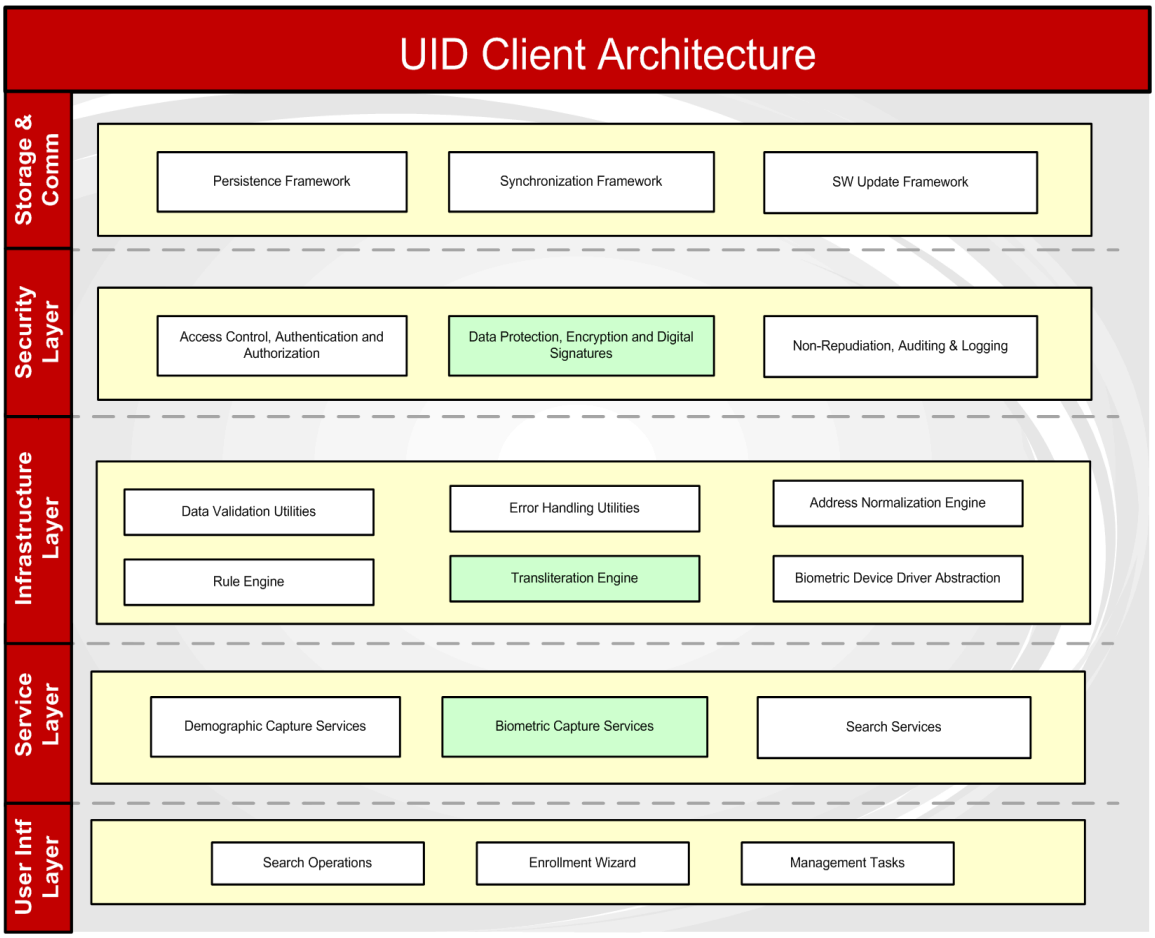
1. **Scalability**: Ability to scale the system within servers, across servers, and across Data Centers (DCs) without inherent bottlenecks and code changes.
2. **Performance**: Ability to perform enrolment and authentication services within the expected time under peak load.
3. **Security**: Ability to secure data from thefts, tampering, unwanted modifications, network attacks, and other security threats using physical and logical measures.
4. **Interoperability**: Ability to interoperate with other systems/services using open interfaces and ability to continually re-factor and/or replace specific components without affecting rest of the system. Note that UIDAI only provide enrolment and authentication APIs and does not provide open interfaces to directly access resident's data by any system.
5. **Manageability**: Ability to manage end-to-end system and its components to ensure system health and SLAs.
6. **Availability**: Ability of the system to be up and running over long periods of time and ensure continuous availability.
7. **Upgradeability**: Ability to seamlessly upgrade services, components, and modules without affecting services and open interfaces.
8. **Maintainability**: Ability to continuously maintain, enhance, re-factor system without breaking other parts.

9. **Open Standards Based**: Technology choices should be based on open standards and widely adopted frameworks as long as it meets the needs of the system.
10. **Cloud Enabled**: Ability to deploy and run the application within a private cloud platform to take advantage of next generation cloud features.

High Level System View



The UID Server System consists of the UID application that sits on top of the eGovernance Cloud Platform. UID Server System is deployed centrally on one or many data centres and exposes various services over a secure network. Main application modules are “Enrolment Module” and “Authentication Module”. In addition, various other modules for administration, analytics, reporting, fraud detection, portal user interface, etc. are also part of the UID Server System.



On the other hand, UID Enrolment Client is a rich client application that can be deployed to large number of computers on the field and works in offline disconnected mode. Enrolment agencies use the client software to enrol residents into the system on the field and upload data onto the server as a batch.

Following sections discuss these systems in detail and list out the functional and technical requirements of each of those systems and modules within them.

eGovernance Cloud Platform

Cloud computing is fast emerging as the next generation computing paradigm to build and deploy Internet applications targeting large sets of geographically dispersed users. Cloud computing facilitates these applications to be deployed and managed in distributed systems across data centres and provide clean abstraction from low level resource and application management. Typically these

deployments are highly virtualized and help businesses to use processors, memory, disks, and network in an optimal way.

Over the last few years several vendors have started offering these computing environments as "public" or "private" Internet cloud for the use of business. Next generation applications should be architected and deployed over such computing platforms to take advantage of scale and elasticity of the cloud. A private cloud deployment is very appropriate for eGovernance applications and Governments in various countries are rapidly adopting this platform.

UID Application will be architected for the cloud and will sit on an "eGovernance Cloud Platform" that will be assembled using open architecture and components. UIDAI will work with experts and platform providers to design and architect this platform. Specific procedures for building, sharing, and deploying this platform will be worked out in due course of time.

The eGovernance Platform will consist of mainly 3 layers:

- Back Office layer
- Infrastructure layer
- Operations layer
- Persistent Store (database) layer

Back Office Layer

The back office layer consists of administrative modules such as:

- Analytics and Monitoring
- Fraud Detection
- Billing & CRM
- Customer & Tech Support

Infrastructure Layer

The infrastructure layer contains system components such as:

- Distributed computing platform

- Application Server
- Distributed caching service
- Event Management
- Audit & Logging System
- Process Management
- Application Monitoring and Management
- Alert and Task management
- Business Workflow processor and Rule engine

Operations Layer

The operations layer contain components that help administer the data centre and servers of the UID system, they include

- Data centre operations & management modules
- Network Management
- Data backup and archival
- Disaster recovery system

UID Application

The UID application consists of the interface layer and the application layer as shown in the architecture diagram.

Interface Layer

The interface layer is the only way in which the UID system can be accessed by the outside world, it supports the key enrolment and authentication services as well as makes available portals and other analytics and monitoring reports to both end users the residents as well as the eco-system of UID partners.

Application Layer

The UID application layer mainly consists of 2 components with other supporting components:

1. Enrolment Server
2. Authentication Server

Enrolment server

The enrolment server which works in conjunction with the enrolment client, takes in a request for UID enrolment and after establishing the uniqueness of the resident using biometric de-duplication, assigns a UID number. The enrolment consists of several sub-components

- **Enrolment Module –** This module is the server counterpart to the enrolment client. It orchestrates the entire server side enrolment workflow to completion by calling various other sub-components like address-normalization, server side validation, biometric de-duplication etc.
- **Batch File Processing** – Due to the poor penetration of high bandwidth Internet services across large parts of the country, the UID enrolment needs to be designed for offline enrolment, where the enrolment client software continues to capture enrolment data at the local level and a batch file is submitted by the enrolling agency (through the Registrar) when connectivity is available. The creation, validation, uploading and tracking of these batch files is handled by the 'Batch file processing' sub-component.
- **Address Normalization** – Since 1.2 billion residents and their addresses will be captured in the process of creating the UID database, it is important that the address field is structured correctly and can be used for UID authentication as well as service delivery by several Registrars. This sub-component with the help of administration boundary codification (e.g. mapping Pincodes to administrative boundaries like state id, district id, and village id)

and physical address verification (during UID letter delivery) will help addresses to be well structured.

- **Local Language Support** – The UID system will support 2 languages (local language and English) during enrolment data capture. Though the UID client software will help transliterate from the source language (in which the form was typed, most likely the local language) to the other language, the server needs to validate the data being submitted in the 2 languages. There is also a need for the server to update the UID client with the latest language dictionaries and stemmers to keep the transliteration engine updated.
- **Name Dictionary** – Since the Name is likely to be used while authentication by several Registrars, it is important that a name dictionary be created and continually updated on the server side so that it ensures reliable authentication. These name dictionaries have to be maintained in all languages supported by the UID system.
- **Pre-enrolment** – Since the capture of biometrics using sophisticated biometric devices by highly trained professionals could be the bottle-neck in the entire enrolment processes, it is desirable to complete the other demographic data capture and verification ahead of the biometric capture. This step is called pre-enrolment. It is conceivable that through existing databases available to the Registrars (For example, state governments BPL, PDS, or NREGA databases) a pre-enrolment workflow can import data into the client module, and only call upon residents to capture biometric data so that it can be linked to the existing demographic record for that resident. The pre-enrolment server sub-component will need to support the above workflow – see UID enrolment diagram.

  Note that even with pre-enrolment, final verification is done at the time of enrolment during which biometric data will also be

captured.

- **Biometric Server** – The biometric server component will process the biometric information (fingerprints, photo of face and iris) to perform the minutiae extraction in the case of fingerprint and iris as well matching in order to de-duplicate the record before UID issue. During enrolment the biometric de-duplication requires a 1:N check against the entire database to ensure uniqueness. This is perhaps the most compute intensive operation that the UID server system will handle at peak loads of enrolment. Please see the section on Biometrics overview later in this document and the UID Biometric Standards report for a detailed review of the biometric capture, de-duplication and authentication.
- **Letter Delivery & Management** – The UIDAI will send a letter to the resident's address upon successful enrolment and issue of UID number. The printing, delivery and tracking of the letter is the purpose of this sub-component. This is likely to involve integration with the delivery partner in order to track the letter and its delivery in the UID's enrolment workflow. Exception processing in the case of undelivered letter, lost letter handling, etc. will be designed and be part of this workflow.

Authentication server

The UID authentication server will provide several ways in which a resident can authenticate themselves using the UID online system. At a high level a Registrar can perform 'Demographic Authentication' or 'Biometric Authentication' or a combination, but in all the above forms of authentication the UID number needs to be submitted so that this operation is reduced to a 1:1 match (the resident's record is first selected using the UID number and then the demographic/biometric inputs are matched against the database fields for authenticating the resident). Various combinations of demographic and biometric authentication APIs can be supported.

Note: All authentication services provide only a "yes/no" answer. No other data about the resident will be part of the response. There will not be any open APIs to access resident's data from the system.

Authentication server provides services for various UID authentication schemes. These include identity verification supporting verification of demographic fields and biometric signatures for residents. This is a 24x7x365 application providing anytime anywhere authentication over mobile and broadband networks. Authentication servers are high performance, massively distributed, and deployed across geographically distributed clustered system.

Authentication Channels: Authentication can be performed by accessing web services through an authentication client device (e.g. Mobile-phone/POS-device/Computer with a biometric scanner), can be performed by calling a phone number with operator assistance or IVR, by submitting a request via SMS. The UID interface layer will need to support multiple channels of authentication access.

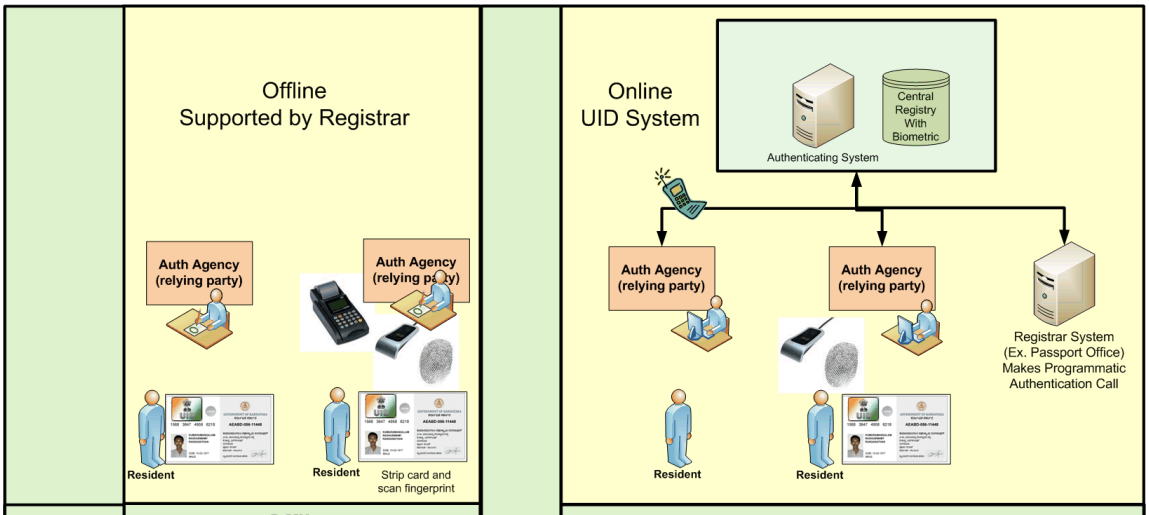
Assurance Levels: The level of assurance that a Registrar can get from the UID system depends on several factors. For instance a biometric authentication against the UID central server provides a high level of assurance, whereas a demographic authentication could provide a medium level of assurance.

Match Thresholds: The various demographic and biometric matchers work on match thresholds and not on absolute digital (MATCH/NON-MATCH) outputs, the interpretation of match scores to a MATCH or NON-MATCH needs to be tuneable using match thresholds. The match thresholds need to be configurable by the Registrar based on their clientele, service delivery and hence authentication needs.

- **Demographic Authentication** – Online services that match demographic details against the input using transliteration and fuzzy matching.

- **Biometric Authentication** – Online services that match biometric signature of the resident against the stored data.
- **Simple Authentication** – Online service that match just name against UID number. This service is also available over SMS.
- **Advanced Authentication** – Online service that match demographic and biometric inputs and support multi-factor authentication using PIN and DPIN.

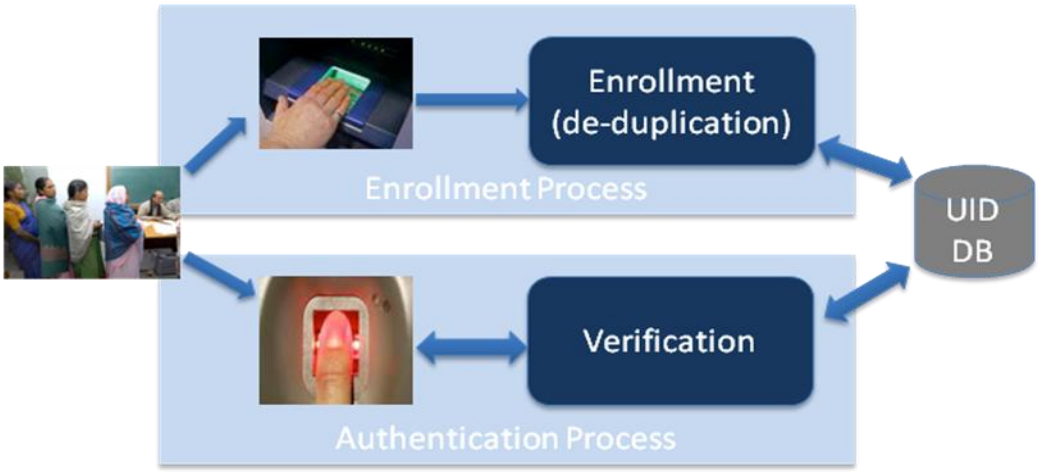
UID Application will support only online methods of authentication. Any offline authentication support needs to be provided by the Registrar's own system.



	Offline		Online		
Auth Types	Compare photo on card with card holder	Compare biometric on card with finger scan	Compare UID and demographic data online	Compare biometric on server against finger scan	Programmatic demo/bio Auth using APIs
Method	Photo Match	Biometric Auth	Demographic Auth	Biometric Auth	Demo/Bio Auth
Assurance	Low	Medium	Medium	High	Medium/High

Overview of Biometrics

The biometric functions are critical portions of the UID application. Given the unprecedented task of performing de-duplication of 1.2 billion records, the biometric components will be procured from biometric solution providers and will not be developed in house. Therefore the biometric requirements focus more on integration requirements. Certain biometric requirements such as de-duplication accuracy are provided for context only.



The biometric view of the overall system is divided into three sub modules:

1. Biometric enrolment client: The enrolment client captures biometric features of face image, ten fingerprints and dual iris images. It performs post-processing such as segmentation and image quality check. After the required criteria are met, biometric data is passed over to the enrolment client software.
2. Duplicate check: A core component of Enrolment Server is biometric duplicate check. The duplicate check sub-module receives incoming biometric data and performs duplicate check against its database. This software runs in "batch" mode and is not synchronized with the image capture process. If a duplicate enrolment is suspected, the enrollee's demographical and biometric information is sent over to a manual de-duplication workstation. Only on successful manual verification, the UID number is assigned.
3. Biometric verification: An API based function within Authentication Server accepts uncompressed or compressed image or feature set to compare against template stored in the database.

All of the three sub-modules will have a well defined interface with each other. The interface is based on well-accepted simple ISO standard, a relational database or well-insulated API. Any of the modules can be replaced without affecting the other sub-modules. This is a key requirement of the UID system.

The sub-modules fit inside more complete overall processes of Enrolment and Authentication.

Biometric System Selection Goals

Three system level goals drive the overall design of the biometric system design.

1. **Interoperability**: For foundation level system such as UID system, the design must allow for replacement of components without any impact on the remaining components. The components in this context should be as fine grained as possible. Use of open standards such as ISO are mandatory.
2. **Avoidance of vendor lock-in**: In the area of biometrics, proprietary algorithm and data representation are perhaps required to achieve performance and accuracy requirements of the UIDAI. The system is designed such that these algorithms and data representation form a part of the black box, and the entire box can be replaced without any impact on the other biometrics black boxes. For example, one can replace enrolment server biometric de-duplication solution without any impact on the authentication server biometric verification solution. All proprietary data formats needed within each solution are not exposed outside of the black box. Use of open source also aids in standardization.
3. **User Convenience**: The entire process of enrolment and authentication must be conducted with strict conformance to quality and precision. At the same time, the process will provide transparency, flexibility and convenience to the resident. For example, the collection of biometric features will have user interface that is consistent with these requirements.

Inter-module Interfaces

There are four important interfaces/data representation formats.

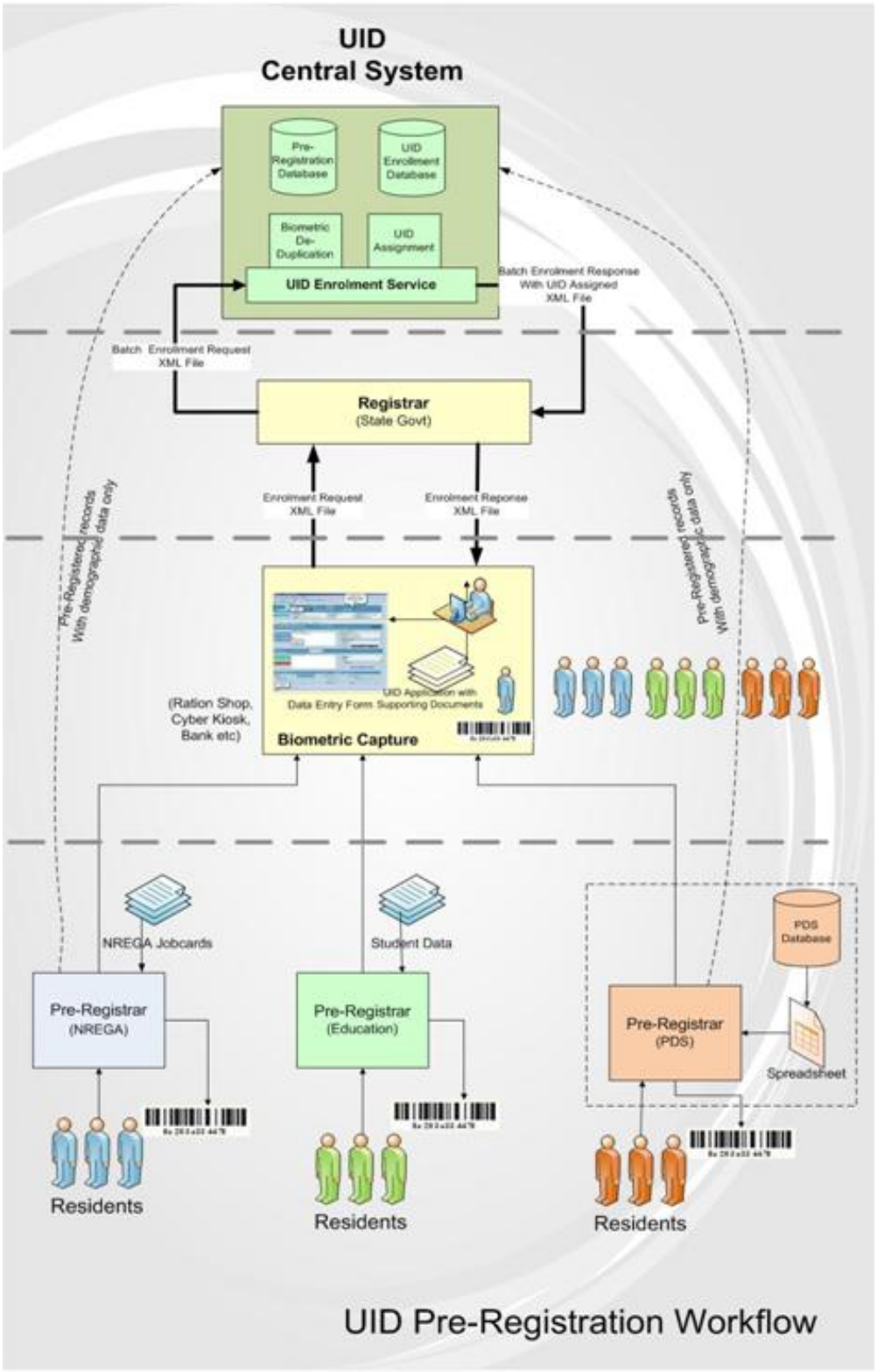
1. **Biometric Enrolment Client**: The captured biometric data is represented per UIDAI Biometrics Design Standards. The images are in uncompressed format. Security and encryption requirements are specified in their respective section. This data is sent to the Enrolment server.

2. **Biometric Enrolment Server**: Upon successful de-duplication and assignment of UID number, server stores biometric data in the Master UID DB. The biometric data format is per UIDAI Biometric Design. The data format and database used by the biometric de-duplication solution is within the "black box".
3. **Biometric Authentication Server**: The biometric authentication solution will generate the biometric template needed for verification from the Master UID DB. The templates are per UIDAI Biometric Design Standards. The storage and management of templates within the biometric solution is opaque to the rest of the system. It should be noted that templates created by Biometric Enrolment Server for de-duplication are distinct (and could be different) from the templates created in the authentication. Both templates are within the "black box" of respective biometric solutions.
4. **Authentication requests**: Incoming biometric verification request data format will comply with the UIDAI Biometric Standards.

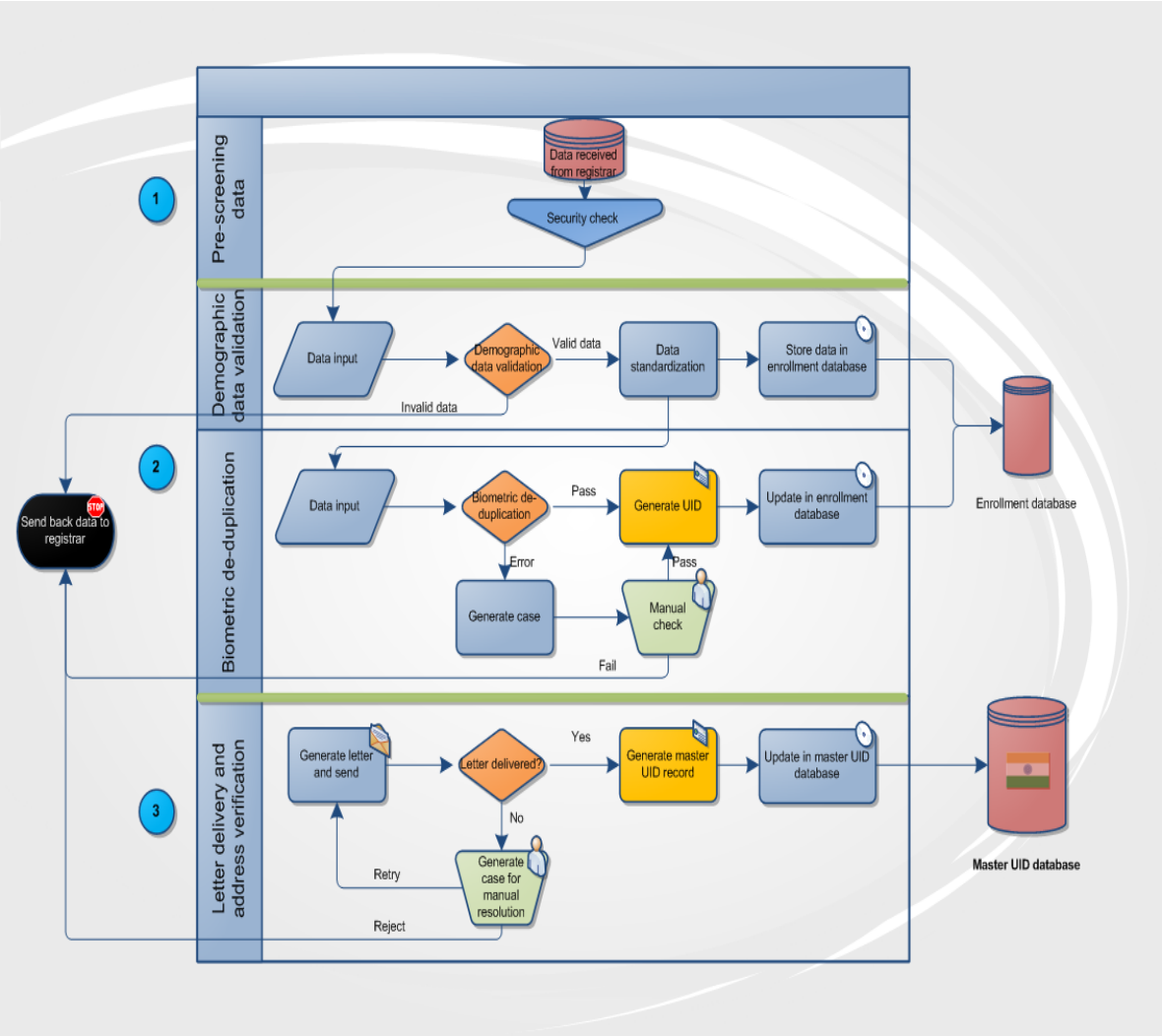
Note: Following sections describe main application modules in detail. At the end of each individual section, a list of requirements is provided in tabular format. Requirements are numbered using an internal requirement numbering scheme (e.g. REQ-EC-SYS-101-P1) for traceability throughout the software development lifecycle.

Enrolment Module

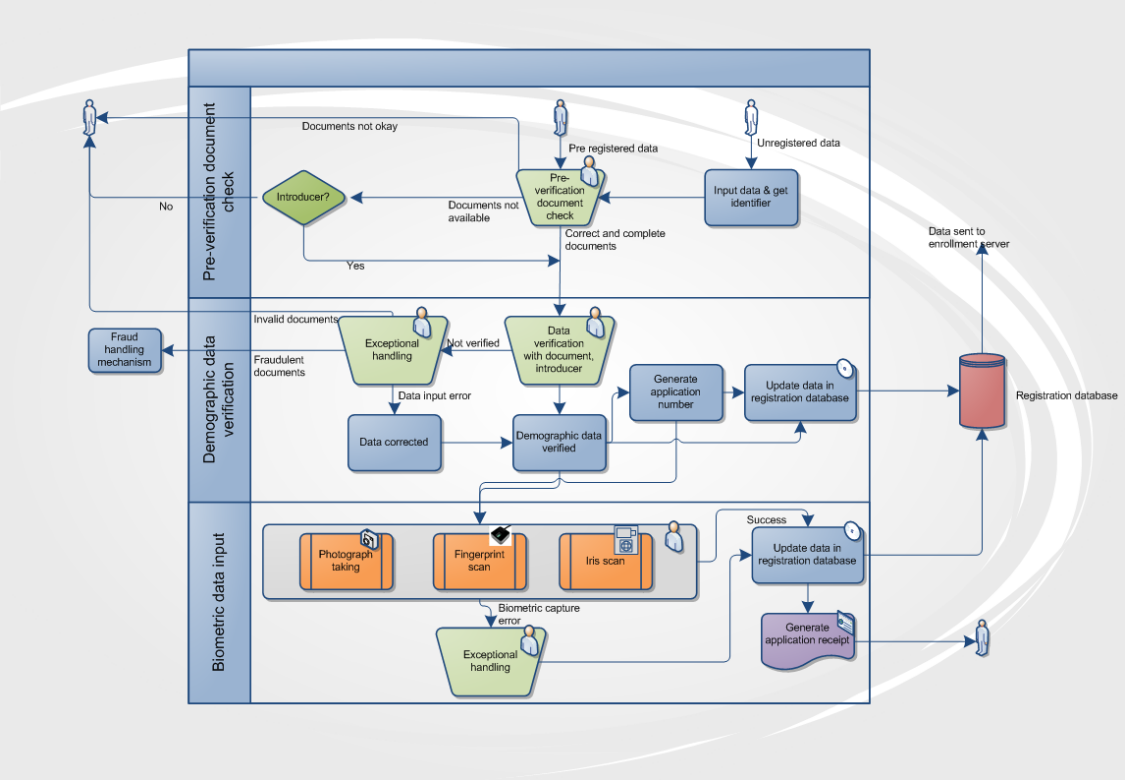
Introduction to UID Enrolment



Enrolment Server Flow



Enrolment Client Flow



Requirements at a Glance

Requirement ID	Requirement Title
REQ-EC-SYS-100	**General Client Features**
REQ-EC-SYS-101-P1	Capturing Usage Metadata
REQ-EC-SYS-102-P1	Supporting Local Storage for Master Data
REQ-EC-SYS-103-P1	Ability to Import Pre-enrolment Data
REQ-EC-SYS-104-P1	Ability to Pull up Resident Record Locally from Imported Pre-enrolment Data
REQ-EC-SYS-105-P1	Support for Multiple Pre-enrolment Data Sources
REQ-EC-SYS-106-P1	Ability to Print Enrolment Receipt
REQ-EC-SYS-107-P1	Ability to Capture Usage Metadata for Analysis
REQ-EC-SYS-108-P1	Support for Localization in Supported Indian Languages
REQ-EC-SYS-109-P5	Support for Audio Messaging (confirmations, instructions, etc.) in Indian Languages

REQ-EC-SYS-200	**Demographic Data Collection**
REQ-EC-SYS-201-P1	Capturing UID Data Fields as per Specification
REQ-EC-SYS-202-P1	Supporting Indian Language Transliteration
REQ-EC-SYS-203-P1	Supporting Local Data Validation
REQ-EC-SYS-204-P1	Supporting Pincode Validation
REQ-EC-SYS-205-P1	Mapping Pincode to Region Codes
REQ-EC-SYS-206-P1	Normalizing Address Structure
REQ-EC-SYS-207-P1	Capturing KYR Process Data
REQ-EC-SYS-208-P5	Ability to Auto Suggest Values Entered Before based on Fuzzy Comparisons and Dictionaries
REQ-EC-SYS-209-P1	System Verification of KYR Process
REQ-EC-BIO-300	**Biometric Data Collection**
REQ-EC-BIO-301-P1	Ability to Capture Finger Prints as per Specification
REQ-EC-BIO-302-P1	Ability to Capture Photo as per Specification
REQ-EC-BIO-303-P1	Ability to Capture Iris as per Specification
REQ-EC-BIO-304-P1	Ability for Supervisory Overrides
REQ-EC-BIO-305-P1	Ability to Check Biometrics Quality as per Standards
REQ-EC-BIO-306-P1	Ability Perform Segmentation
REQ-EC-BIO-307-P1	Ability to Retry Specific Number of Times
REQ-EC-BIO-308-P1	Automatic Audit of Forced Capture
REQ-EC-BIO-309-P5	Support for Local Duplicate Checks
REQ-EC-BIO-310-P1	Biometric Sample
REQ-EC-BIO-311-P1	Biometric Bundle
REQ-EC-SYS-400	**Client Manageability**
REQ-EC-SYS-401-P1	Ability to Easily Install the Client
REQ-EC-SYS-402-P1	Ability to Auto Update from a Central Server
REQ-EC-SYS-403-P1	Ability to Upgrade Easily with Small Patches
REQ-EC-SYS-404-P1	Ability to Export and Import Master Data
REQ-EC-SYS-405-P1	Ability to Export Enrolment Data

REQ-EC-SYS-406-P1	Retention of Data till Server Receipt Confirmation
REQ-EC-SYS-407-P1	Recovery of Data in case of Disk Failure
REQ-EC-SYS-500	**Client Security**
REQ-EC-SYS-501-P1	Support for Operator Authentication – Biometric, Multi-factor
REQ-EC-SYS-502-P1	ACL Based Authorization and Task Management
REQ-EC-SYS-503-P1	Support for Detailed Audit Trail
REQ-EC-SYS-504-P1	Ability to Secure Enrolment Data from Theft
REQ-EC-SYS-505-P1	Ability to Secure Enrolment Data from Tampering
REQ-EC-SYS-506-P1	Ability to Secure Enrolment Client from Tampering
REQ-EC-SYS-507-P1	Ability to Authorize Supervisory Overrides
REQ-EC-SYS-508-P5	Ability to Protect Data from Malware and Viruses
REQ-EC-SYS-509-P1	Ability to Protect Specific Master Data (such as ACLs) from Tampering
REG-EC-SYS-600	**Integration Features**
REQ-EC-SYS-601-P1	Ability to Plug-in Client UI into Registrar's Client
REQ-EC-SYS-602-P1	Ability for Registrar's Client SW to Fully Integrate at API level
REQ-EC-SYS-603-P1	Ability to Cleanly Provide KYR Data to Registrar's Client SW without Exposing Enrolment DB
REQ-EC-SYS-604-P1	Ability to Synchronize Master Data with UID Server
REQ-EC-SYS-605-P1	Ability to Upload Enrolment Data to UID Server through Secure Channel
REQ-EC-SYS-606-P1	Ability to Receive Processing Confirmations for Enrolment Requests
REQ-ES-SYS-100	**General Server Features**
REQ-ES-SYS-101-P1	Ability to Process Batch Enrolments Over a Long Duration
REQ-ES-SYS-102-P1	Ability to Validate Enrolment Request Data

REQ-ES-SYS-103-P1	Integrate with Biometric Server for De-duplication
REQ-ES-SYS-104-P1	Publishing Events to Other Parts of the System
REQ-ES-SYS-105-P1	Ability to Audit Enrolment Processing
REQ-ES-SYS-106-P1	Ability to Store Intermediate Enrolment Data
REQ-ES-SYS-107-P1	Generating UID Number as per Specification
REQ-ES-SYS-108-P1	Interfacing with Letter Dispatch System
REQ-ES-SYS-109-P1	Tracking Statuses Based on Enrolment Workflow
REQ-ES-SYS-110-P1	Ability to Manually Take Decisions on Exceptions
REQ-ES-BIO-200	**Biometric De-duplication**
REQ-ES-BIO-201-P1	Ability to Perform Unbundle and Consistency Check
REQ-ES-BIO-202-P1	Ability to Perform Segmentation
REQ-ES-BIO-203-P1	Ability to Check Image Quality
REQ-ES-BIO-204-P1	Ability Perform Multi-modal De-duplication as per Accuracy Specifications
REQ-ES-BIO-205-P1	Ability to Perform Manual Check
REQ-ES-SYS-300	**Integration Features**
REQ-ES-SYS-301-P1	Supporting Integration with Enrolment Clients for Master Data Update
REQ-ES-SYS-302-P1	Supporting Enrolment Client Software Update
REQ-ES-SYS-303-P1	Supporting Integration with Enrolment Client for Enrolment Data Upload
REQ-ES-SYS-304-P1	Integration with Biometric Server
REQ-ES-SYS-305-P1	Integration with Authentication Server
REQ-ES-SYS-306-P1	Integration with Letter Delivery System
REQ-ES-SYS-307-P1	Responding to Enrolment Requests for Feedback to Registrar's System
REQ-ES-SYS-400	**Performance, Scalability, and Availability**
REQ-ES-SYS-401-P1	Ability to Distribute Enrolment Jobs Over the Compute Grid

REQ-ES-SYS-402-P1	Ability to Deploy Enrolment Server across Many Servers for Scalability
REQ-ES-SYS-403-P1	Ability to Deploy Enrolment Server across Partitioned Data
REQ-ES-SYS-404-P1	Ability to Load-balance Jobs Across Servers
REQ-ES-SYS-405-P1	Ability to Restart from Failures
REQ-ES-SYS-406-P1	Ability to Execute Multiple Sub-tasks (validation, de-dup, etc.) in Parallel
REQ-ES-SYS-407-P1	Ability to Add and Remove Nodes from Cluster without Affecting Jobs
REQ-ES-SYS-408-P1	Ability to Handle Peak Load and Maintain Expected Throughput
REQ-ES-SYS-500	**Data Storage**
REQ-ES-SYS-501-P1	Ability to Store Data Across Multiple Storage Schemes
REQ-ES-SYS-502-P1	Ability to Partition Data Horizontally and Vertically and Distribute Across Nodes
REQ-ES-SYS-503-P1	Ability to Secure Data Storage for All UID Data
REQ-ES-SYS-600	**Network, Deployment, and Manageability**
REQ-ES-SYS-601-P1	Ability to Deploy Enrolment Servers within Secure Network
REQ-ES-SYS-602-P1	Ability to Deploy Partitions Across Different Networks Secured from Each Other

Authentication Module

Understanding Authentication

There are multiple forms of authentication that the UIDAI can offer providing different levels of assurance ranging from high to low. Here we summarize the main forms of authentication, depending on the situation and equipment available.

Online Authentication

Online authentication is supported by the UID system. This can include:

- Online demographic authentication where the authenticating agency compares the UID number and demographic information of the UID holder to the information stored in the UID database. The assurance level here is medium.
- Online biometric authentication where the biometrics of the UID holder, his/her UID number and key demographic details are compared to the details on the server. The assurance level in this case is high.
- Online demographic/biometric authentication with API where the Registrar's backend system makes a programmatic call to the authentication APIs exposed by the UID system to perform authentication. The assurance level here may be medium-high depending on whether the check used demographic or biometric inputs.

Offline Authentication

Following offline authentication methods may be optionally supported by the Registrar, and does not use the authenticating service provided by the UIDAI.

- Photo match authentication where the photo on the Registrar-issued card is compared with the cardholder. This is the most basic form of authentication. The assurance level here is low.
- Offline biometric authentication compares the scanned fingerprint of the cardholder to the biometric stored on the Registrar-issued card. The assurance level here is medium.

Stateless Authentication Services

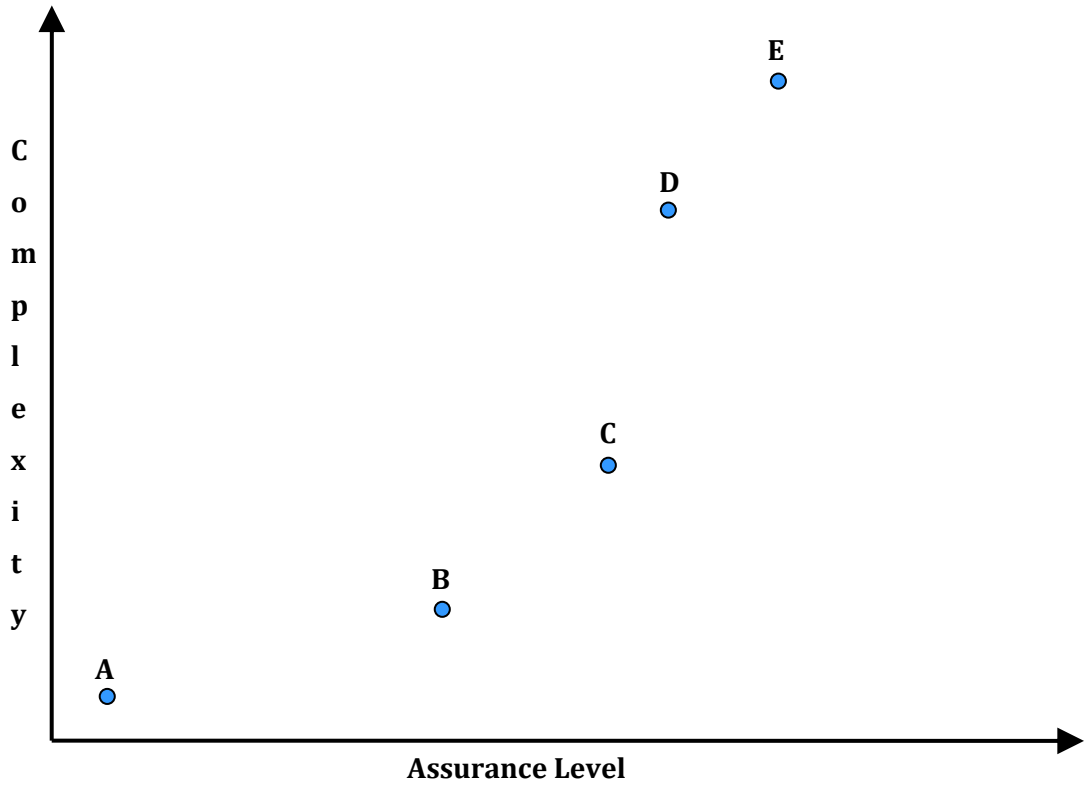
UIDAI expects extremely large volume of authentication requests a day once the UID number is widely adopted within various systems across the country. To cater to such large volumes, all authentication APIs should be stateless for high scalability and seamless load-balancing.

This means that "no" state should ever be maintained on the server and every request should be serviced as if it is a new request. Authentication clients should maintain necessary state during interaction with the resident to allow error handling, retries, and overall provide a friendly experience to residents.

Managing Assurance Levels

Authentication services should be made available under various assurance levels. Based on the functional need, applications should be able to choose an appropriate assurance level for its use. For example, banking or financial application may choose to use a higher level of assurance compared to NREGA or RSBY.

When choosing higher assurance levels, it is important to note that complexity (in terms of device and user knowledge point of view) also increases. Following chart indicates the relationship between assurance level and complexity.



A – Simple demographic authentication has lowest complexity

B – Using biometric (finger print or iris) input during authentication increases assurance. Complexity also increases due to the fact that resident need to provide his/her biometric and possibility of errors or usage issues increases.

C – Using DPIN (dynamically generated transaction level PIN) increases the assurance further. But requirement for a mobile device and obtaining and inputting DPIN adds complexity.

D – Using a secret PIN adds further assurance. But, most residents may not be able to remember PIN. In addition, communicating, resetting, etc. adds to process complexity.

E– Using a combination of biometric/DPIN/PIN (multi-factor) during authentication provides highest assurance, with most complexity.

Note: Above graph is for illustrative purposes only.

"Tolerance Level" for Fuzzy Matches

Authentication services will allow checking of demographic data such as name and address. In the context of Indian names and local language usages, (see a separate requirement on local language support during authentication) name and address matching can be tricky and can result in high non-matches. To avoid this issue, authentication services will support a concept called "Tolerance Level". This is the parameter which tells the authentication server how fuzzy the match can be. Requesting applications can provide their desired tolerance level as part of the input.

Tolerance level should only be supported for "Name" and "Address" matching. Requesting applications can supply an acceptable level as part of the input for authentication service. For example, when checking addresses, LPG delivery application may need "high" tolerance level where as NREGA may only need a "medium" level.

Typically, tolerance level is mapped to an internal "match score". For example, "High" tolerance level may be mapped to a match score greater than 95, "Medium" >80, and so on. Usage of match score or other techniques should be clarified as part of design.

Requirements at a Glance

Requirement ID	Requirement Title
REQ-AS-SYS-100	**Authentication Services**
REQ-AS-SYS-101-P1	Support for Tolerance Level for Fuzzy Matches
REQ-AS-SYS-102-P1	Online Demographic Data Check
REQ-AS-SYS-103-P1	Basic Name Check
REQ-AS-SYS-104-P1	Online Address Check
REQ-AS-SYS-105-P1	Test Automation for APIs
REQ-AS-SYS-106-P1	Statelessness of APIs

REQ-AS-SYS-200	**Managing Assurance Levels**
REQ-AS-SYS-201-P1	Using Biometric during Authentication
REQ-AS-SYS-202-P1	Using DPIN during Authentication
REQ-AS-SYS-203-P5	Using PIN during Authentication
REQ-AS-SYS-204-P5	Performing Multifactor Authentication
REQ-AS-SYS-300	**Local Language Support**
REQ-AS-SYS-301-P1	Local Language Support for Demographic Authentication
REQ-AS-SYS-302-P1	Local Language Support for Address Verification
REQ-AS-SYS-400	**Performance, Scalability, and Availability**
REQ-AS-SYS-401-P1	Simple Authentication Performance
REQ-AS-SYS-402-P1	Advanced Authentication Performance
REQ-AS-SYS-403-P1	Address Verification Performance
REQ-AS-SYS-404-P1	Horizontal Scalability
REQ-AS-SYS-405-P1	High Availability within a DC
REQ-AS-SYS-406-P1	High Availability Across Multiple DCs
REQ-AS-SYS-407-P1	Ability to Partition Data Across Servers and DCs
REQ-AS-SYS-408-P1	Ability to Load-balance Across Servers and DCs
REQ-AS-SYS-500	**Security and Auditing**
REQ-AS-SYS-501-P1	Protecting from Stealing Request Data
REQ-AS-SYS-502-P1	Protecting from Unauthorized Clients
REQ-AS-SYS-503-P1	Protecting from Request Tampering
REQ-AS-SYS-504-P1	Ability to Audit Authentication Requests
REQ-AS-SYS-505-P1	Ability to Retain Audit Trails for Prescribed Days
REQ-AS-SYS-506-P1	Ability to Optionally Notify Resident of Authentication Requests
REQ-AS-SYS-600	**Synchronization Requirements**
REQ-AS-SYS-601-P1	Ability to Synchronize changes from Enrollment DB

REQ-AS-SYS-602-P1	Ability to Synchronize across DCs
REQ-AS-SYS-603-P1	Ability to Guarantee Change Propagation
REQ-AN-SYS-100	**Authentication Network**
REQ-AN-SYS-101-P1	Basic Authentication over SMS
REQ-AN-SYS-102-P1	Advanced Authentication over Internet Connection
REQ-AC-SYS-100	**Authentication Client**
REQ-AC-SYS-101-P1	Cell Phone for SMS Authentication
REQ-AC-SYS-102-P1	Devices for use with Internet Connection (Mobile, POS, Computer, etc.)

Fraud Detection Module

Generally, fraud is defined as intentionally deceiving a person or organization to gain illegal access to resources and benefits. It is important for the UID system to create a fraud detection module that is able to detect and minimize identity fraud.

Following are some of the examples of fraud

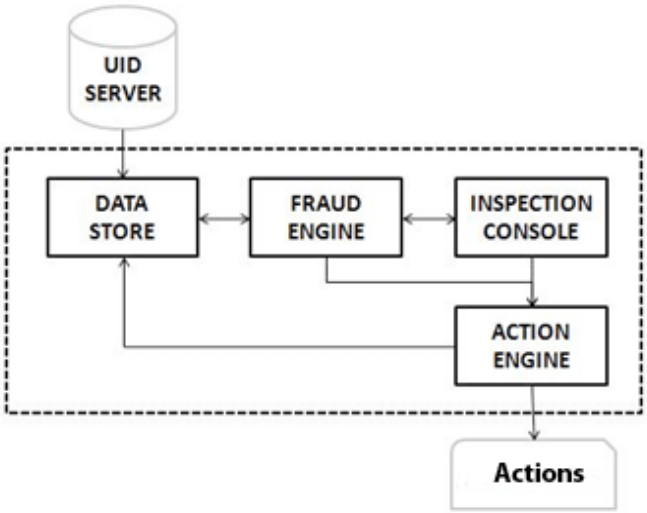
1. Misrepresenting information
2. Multiple registrations by the same resident
3. Creating invalid registrations of people who don't exist
4. Identity theft by authenticating as someone else
5. One or more of the above, without the knowledge or understanding by the resident

Given the heterogeneity of fraud detection, one cannot expect a single algorithm to address the situation. A layered Fraud Detection engine must be implemented as a part of the UID project which can detect/prevent various types of fraud. A

systems-based approach combined with manual inspection, investigation and learning is essential for a complete fraud detection system.

The fraud detection system should be designed to detect who committed the fraud at an individual or organizational level. Depending on the method used, it may also be able to detect the channel through which the fraud was committed.

Systems Overview



Above figure shows the components of the fraud detection system at a high level. The fraud detection system should be designed keeping modularity in mind, such that each functional block can be perceived as a black box with input and output interfaces to the rest of the system. The entire fraud detection system is a black box within the larger UID system, with a well-defined input and output interface.

1. **Data Store (DS)**: Sync audit trails and UID data from the UID data store
2. **Fraud engine (FE)**: Contains rules and algorithms for fraud detection
3. **Inspection console (IC)**: Anything requiring manual review is sent here
4. **Action engine (AE)**: All external actions (manual and automatic) are processed here

Both, FE and AE have extensible rule engines. The FE should also have a highly standardized and flexible interface that allows new algorithms from universities

and industry to be plugged in, without requiring detailed knowledge of other modules.

The fraud detection system must operate within the constraints of privacy and policies that are outlined in the UIDAI Act and other subordinate legislation (currently in draft stage).

Requirements at a Glance

Requirement ID	Requirement Title
REQ-IO-FRD-400	**Published Inputs and Outputs**
REQ-IO-FRD-411-P1	Supporting Black List Input
REQ-IO-FRD-412-P1	Supporting KYR Data as Input
REQ-IO-FRD-413-P1	Audit Trails as Input
REQ-IO-FRD-421-P1	Supporting Internal Feedback for Learning
REQ-IO-FRD-422-P1	Updating Blacklist based on Patterns
REQ-IO-FRD-423-P1	Supporting Manual Investigation
REQ-DS-FRD-500	**Fraud Data Store**
REQ-DS-FRD-510-P1	Creating Data Store
REQ-DS-FRD-511-P1	Supporting Storage of UID Fields for Optimal Analysis
REQ-DS-FRD-512-P1	Supporting Storage of Audit Trails for Optimal Analysis
REQ-DS-FRD-520-P1	Supporting Reputation scores
REQ-DS-FRD-530-P1	Supporting Extensible Metadata
REQ-DS-FRD-540-P1	Supporting Pluggable Engine based on Interfaces
REQ-DS-FRD-541-P1	Supporting Read/Write Interfaces to UID Server
REQ-DS-FRD-542-P1	Supporting Read/Write Interfaces to to Fraud Engine
REQ-DS-FRD-543-P1	Supporting Read/Write Interfaces to Action Engine
REQ-DS-FRD-550-P1	Process Session Data
REQ-DS-FRD-560-P1	Supporting Detailed Logging

REQ-DS-FRD-570-P1	Supporting ACLs
REQ-FE-FRD-600	**Fraud Engine**
REQ-FE-FRD-610-P1	Rules Interfaces
REQ-FE-FRD-620-P1	Supporting Job Scheduler
REQ-FE-FRD-630-P1	Methods for detecting fraud
REQ-FE-FRD-631-P1	Detecting Data Anomalies
REQ-FE-FRD-634-P1	Supporting State Driven Transitions
REQ-FE-FRD-635-P1	Supporting Setting Limits
REQ-FE-FRD-636-P1	Supporting Geographical analysis
REQ-FE-FRD-640-P1	Providing Rule engine
REQ-IC-FRD-700	**Inspection Console**
REQ-IC-FRD-701-P1	User Interface for Manual Inspections
REQ-IC-FRD-702-P1	User Interface for Configuration of Fraud Engine
REQ-AE-FRD-800	**Action Engine**
REQ-AE-FRD-810-P1	Supporting Configurable Action Engine Workflow
REQ-AE-FRD-811-P1	Keeping Track of Action Event Creator Identity
REQ-AE-FRD-812-P1	Keeping Track of Action Event Triggered
REQ-AE-FRD-813-P1	Configuring Action Event processing
REQ-AE-FRD-814-P1	Publishing Action Event Results
REQ-AE-FRD-820-P1	Integrated Workflow Management Tool

Administration Module

The UID system deals with a range of entities that access the system for specific administrative activities such as adding users, configuring access permissions, etc. The Administration module deals with the creation, management, and reporting of activities from these entities. The following entities are defined.

- **Registrars**: These entities are the primary contractual partners with which the UIDAI has agreements in place to enrol residents. A Registrar will have various users associated with it, who will be able to manage business processes that include the creation of Sub-Registrars, and enrolment agencies.
- **Sub-Registrars**: Various departments within a State are known as Sub-Registrars.
- **Enrolment Agencies**: A Registrar typically works through enrolment agencies for actual field implementation.
- **Field Agents**: These users are out in the field, typically part of an enrolment agency, collecting data from residents.
- **Introducers**: Registrars and/or UIDAI may enlist the support of introducers, who will vouch for the identity of individuals who lack sufficient documentation / proof of identity, and address. These introducers may belong to government or private enterprises including NGOs. Introducers must be added to the system before they can actually start introducing residents. For details, refer to section 3.5 of DDSVP Committee report.
- **Authentication Clients**: These are the business users of the UID system, who are allowed to verify the identity of various individuals.

In addition to external entities, certain internal groups (within the UIDAI) are also defined.

- **Administrators**: These users are responsible for managing the system. They have the ability to create other user types, setup groups, and assign access control parameters.
- **Customer Service Agents**: These respond to requests from residents – regarding various aspects of the UID system. Various use cases will be determined, which will allow the agent to answer user queries related to specific UIDs.
- **Biometric De-duplication Agents**: When the biometric system identifies certain enrolment records to be potentially duplicate, this is sent over to

de-duplication agents who use the demographic data, as well as the biometric data to identify duplicates (or otherwise).

- **Fraud Detection Agents**: These are part of the fraud unit, who are allowed to make certain queries to identify certain patterns of usage, and potential fraudulent activities.

The Administration module will allow the creation, modification, and deletion of these user records, and groups, as well as the setting up of appropriate access controls. In addition, it will provide an analytics / reporting module which will allow the UIDAI to track the performance and reliability of the system.

Administering Trust Network

The administration module is responsible for the creation, deletion, and modification of user records, groups, and permissions. Trust flows through this system from the UIDAI to the resident. The administration module should allow this trust network to be created, and managed.

Administering Various Cases

The main use cases are:

- **Administration**: Creation / User Management
- **Business Management**: Signing up Registrars, tracking documentation, and contracts.
- **Pre-Enrolment**: Collecting demographic data of residents prior to going out in the field and enrolling them.
- **Enrolment**: Issuing a UID number to a resident, after collecting the necessary demographic biometric data, and ensuring that no duplicate IDs are created.
- **Authentication**: Validating that a certain [Resident data, UID number] pair is present in the system.

The administration module will allow administrators, and other users to see the status of these use cases, trace specific use cases, and measure the performance of individual users, and subsystems. The system will have built-in escalation mechanisms, to handle failure / delays. In the event of certain performance measurements going out of bounds, alerts can be sent by email / other escalation mechanisms.

Requirements at a Glance

Requirement ID	Requirement Title
REQ-AD-SYS-100	**General Features**
REQ-AD-SYS-101-P1	User Management
REQ-AD-SYS-102-P1	Roles, and Access Control list management
REQ-AD-SYS-103-P1	Business Process instrumentation
REQ-AD-SYS-104-P1	Status Reports

Analytics and Reporting Module

The progress of UID enrolments and the subsequent authentication requests needs to be provided for public view as well as Registrar monitoring. It would be desirable to be able to track these progress indicators by administrative boundary (State, District etc) as well as by Registrar (PAN, NREGA, PDS, Banks, Telecoms etc). The analytics and reporting module will publish these aggregate numbers for public consumption. A visual reporting system that includes GIS, graphs and pie-charts is envisioned in order to make the information user-friendly and accessible.

The Analytics and Reporting module will provide reports on the use cases, as well as the subsystems, and users involved in the handling of these cases. Aggregate statistics, by region, will be presented visually with the help of a map where appropriate, which will allow users to drill down on regions, and get statistics.

Requirements at a Glance

Requirement ID	Requirement Title
REQ-AR-SYS-100	**General Features**
REQ-AR-SYS-101-P1	Business Process Aggregate Metrics Reports
REQ-AR-SYS-102-P1	Interactive, Map based Aggregation / Drilldown
REQ-AR-SYS-103-P1	Sub-system Reports as Needed

Information Portal

The information portal will provide an overall dashboard to track the performance of the UID system. This is divided into the following portals.

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.

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.

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. REST style

URLs should expose this data and should encourage the ecosystem to build applications to take advantage of this data.

Requirements at a Glance

Requirement ID	Requirement Title
REQ-IP-SYS-100	**Partner Portal**
REQ-IP-SYS-101-P1	Provide Partner Level Statistics
REQ-IP-SYS-102-P1	Provide Partner Level Metrics
REQ-IP-SYS-103-P1	Supporting Drill Down within Various Reports
REQ-IP-SYS-104-P1	Track Individual Support Cases
REQ-IP-SYS-200	**Public Information Portal**
REQ-IP-SYS-201-P1	Provide Aggregate Metrics Visibility
REQ-IP-SYS-202-P1	Support Grievance Requests, and Handling
REQ-IP-SYS-300	**Data Portal**
REQ-IP-SYS-301-P1	Expose Public API for all Portal Data Access
REQ-IP-SYS-302-P1	Implement Public APIs
REQ-IP-SYS-303-P5	Provide an Application Development Platform

Implementation Frameworks

This section provides a high level overview of development frameworks to be used for the application development. The principles behind the choice of the implementation frameworks:

1) Need to scale to large number of enrolments and authentications.
2) No vendor lock-in.
3) Use of open-source technologies wherever available and prudent.
4) Use of open standards to ensure interoperability.
5) Ensure wide device driver support for biometric devices (important factor in the choice of the client implementation frameworks).
6) Use of technology platforms and tools that have large pool of qualified and trained technology personnel.

UID Server Frameworks

UID Server includes application modules that processes enrolment requests coming from the Registrars, validates data, does biometric de-duplication, generates UID number, and communicates with the resident as well as the Registrar. In addition to providing enrolment services, it also offers various online authentication services including biometric authentication to verify the claim of a resident.

Following are the technology framework choices for the UID Server modules:

- Machine architecture – 8086 32-bit / 64-bit Server
- Operating System – Linux
- Database – Industry Strength RDBMS
- Distributed computing platform, message queue, web server, distributed caching platform, biometric matching algorithm, etc. – Provided by vendors / 3rd party providers / libraries
- Application – APIs, web services, user interfaces, etc. built on Java using available 3rd party libraries and frameworks

UID Client Frameworks

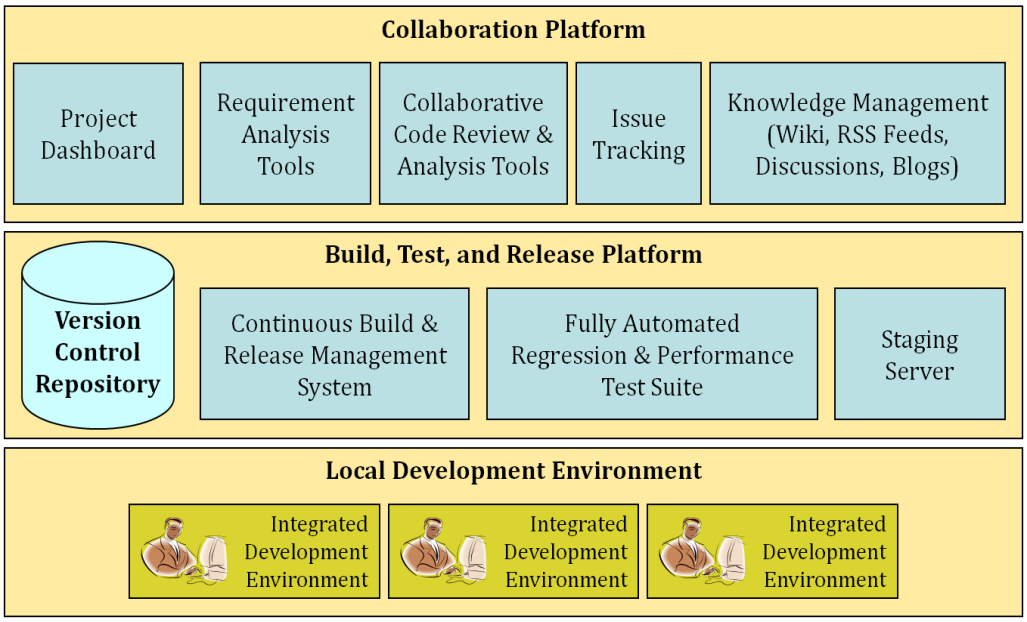
Enrolment Client is a rich client application that needs to work offline (without connectivity to any server) and fully support features such as demographic data collection, data transliteration, address normalization, biometric data capture, secure data storage, etc.

Following are the technology framework choices for the UID Enrolment Client:

- Machine architecture – 8086 32-bit Desktop / Laptop
- Operating System – Multiple (Windows, Linux, Mac)
- Device Drivers (biometric), Transliteration Engine, and other external components – Provided by vendors / 3rd party providers
- Application (API and User Interface) - Built on rich client technologies on supported the operating systems

Note: In the future, UIDAI may decide to choose alternate technology frameworks if found necessary to meet the technology needs of the system.

Engineering Environment Overview



Planned Roadmap of UID Application

UIDAI plans to use a rapid development and continuous build-test-release cycle for its application development. Continuous builds, highly automated test environment, and monthly integrated internal release cycles are critical for the success of this project.

Release 1

An integrated and fully tested initial release "Release 1" is planned in July, 2010. This release1 consists of 2 sub-releases

1) Cloud based eGovernance platform release1
2) The UID application release1

   The UID application release primarily consists of Enrolment Client, Enrolment Server with multiple biometric de-duplication engines, Authentication Server, and simple Administration Server. This release should handle up to the capacity of 1 million (10 lakhs) UID being enrolled into the system.

Release 2

Next main release "Release 2" is planned in November, 2010. This release consists of 2 sub-releases:

1) Cloud based eGovernance platform release2
2) The UID application release2

the UID application "Release 2" consists of "Release 1" features as well as additional fully functioning modules such as Administration, Analytics & Reporting, Partner & Public Portals, Fraud Detection, and enhancements to few other supporting frameworks. This release also is designed towards much higher scalability and should handle capacity up to 100 million (10 crores).

Features and Releases

Enrollment Client – Features	1.0	2.0	Future Versions
Pre-enrolment data support for pilot registrars	☑		
Advanced pre-enrolment data support		☑	
Self pre-enrollment portal		☑	
Demographic Data Capture	☑		
Basic Transliteration	☑		
Advanced Transliteration (local language keyboard, name dictionary)	☑		
Address Capture and region code normalization	☑		
Address Normalization (basic code mapping)	☑		
Address Normalization (street and landmark smart matching)		☑	
Biometric Capture	☑		
Biometric Verification, Quality checks	☑		
Local De-duplication		☑	
Data storage (encrypted and digitally signed)	☑		
Secure Data Upload	☑		
Secure Data Sync	☑		
Software Auto-update		☑	
Pluggability of Client into other application	☑		

Operator Auth (biometric & password)	☑		
Advanced Security Features (mal-ware checks, system validation checks, etc.)			☑

Enrollment & Auth Server – Features	**1.0**	**2.0**	**Future Versions**
Enrollment Data Interface	☑		
Biometric De-duplication	☑		
Advanced Biometric De-duplication (for medium scale)		☑	
Manual De-duplication Interface	☑		
Letter Printing and Delivery	☑		
Advanced Biometric (multi-modal) De-duplication and Scaling		☑	
Data Validation and UID Generation	☑		
Distributed Computing Platform		☑	
Distributed Caching Framework		☑	
Data Encryption	☑		
Data Partitioning		☑	
Simple Authentication Service	☑		
Advanced Authentication Service (Biometric, Address check, language support)	☑		
Multi-factor Authentication (PIN, DPIN)		☑	

High Availability Deployment	☑		
Manual User management (operator, admin, introducer, etc.)	☑		
Advanced UI for Configuration Data Management		☑	

Other Server Modules – Features	**1.0**	**2.0**	**Future Versions**
Fraud Detection Engine		☑	
Rules Engine		☑	
Basic CRM Features		☑	
Advanced CRM			☑
Billing			☑
Basic 3rd Party Application Development Infrastructure		☑	
Advanced 3rd Party Application Development Platform			☑
Portal Interface	☑		
IVR and Call Center Interface		☑	
Mobile Interface	☑		
Administration UI		☑	
Pub/Sub Event Framework		☑	
Alert & Task Management	☑		
Process/Workflow Management	☑		
Advanced Process/Workflow Management		☑	

Advanced Data Security, Partitioning		☑	
Multi-DC Deployment			☑
Basic DC Operations (Server Admin, Backup, NW Admin)		☑	
Advanced Multi-DC Operations			☑
Test Automation, Continuous Builds, Automated Deployment	☑		

Overview of workload

UID Application Release 1 should be built to scale up to 1 million (10 lakhs) UID numbers and subsequent version - Release 2 - should have the capacity to scale up to 100 million (10 crores) UID numbers.

Note: These are only system capacity numbers and not the actual UID number roll out plan. A detailed field rollout plan will be prepared by UIDAI and published later.