www.pwc.com

L3: Overview of the Technical and Functional Solution

Strictly Private and Confidential

Implementation of National Population Register, Morocco

January 2018

pwc

31 January, 2018

Mr. Omar El Alami
Project Chief – RNP
Ministry of Interior
Administrative District
Av Mohamed V, Rabat

Dear Mr. Alalami,

Subject: *Deliverable L3 – Overview of the Technical and Functional Solution for Implementation of National Population Register (RNP), Morocco*.

In pursuance of our contract for the engagement dated 22 November 2017, with the Ministry of Interior, Rabat, Government of Morocco, we are pleased to submit our Report on the Overview of the Functional and Technical Solution as part of consultancy services for the Implementation of National Population Register (RNP), Morocco.

We wish to express our appreciation for the cooperation we have received from the Ministry of Interior, the RNP team and other stakeholders. We hope that we can continue to receive similar level of cooperation throughout the rest of the assignment.

Should you require any information or clarification on the report, please contact me on email: Nabil Kettani (nabil.kettani@pwc.com) or Bharat Nanawati on bharat.nanawati@pwc.com

Yours sincerely,

For: PricewaterhouseCoopers

Nabil Kettani

(Partner)

Acknowledgement

This report has been produced by the PwC based on discussions and meetings held at Morocco during November 2017 to January 2018. From the Ministry of Interior, Mr. Abdelhak Harrak (Governor Director of Information System), Mr. Omar El Alami, Ms. Amina Benomar, Mr. Achraf El Ouali Aboulaich, Ms. Wifak Tayeb and Mr. Youssef Arahou have been involved during the preparation of this deliverable. The PwC team led by Bharat Bhushan Nanawati, Sudhanshu Jain, Vikram Sharma and Mehdi Barrakad, supported by other team members prepared this report.

The team is grateful to the Ministry of Interior, Government of Morocco for providing the opportunity to interact with all key stakeholders and providing suggestions on the report. We would also like to acknowledge with much appreciation the significant support received from various organizations and agencies in Morocco.

Abbreviations

Abbreviation	Full Form
ABIS	Automated Biometric Identification System
ACD	Automatic Call Distributor
ADS	Active Directory System
AHT	Average Handling Time
API	Application Programming Interface
ARIMAX	Autoregressive Integrated Moving Average
BI	Business Intelligence
CNIE	La Carte Nationale d'Identité Électronique
COTS	Commercially Off the Shelf
CRM	Customer Relationship Management
CSC	Citizen Service Centre
CSV	Comma-Separated Values
CTI	Computer Telephony Integration
DB	Database
DC	Data Center
DFS	Distributed File System
DMS	Document Management System
DQ	Data Quality
DR	Disaster Recovery
DS	Data Store
DW	Data Warehouse
EDW	Enterprise Data Warehousing
ESB	Enterprise Service Bus
FTR	First Time Resolution
GIS	Geographic Information System
GPS	Global Positioning System
GUI	Graphical User Interface
HDFS	Hadoop Distributed File System
HRMS	Human Resource Management System

Abbreviation	*Full Form*
HSM	Hardware Security Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IDMS	Identity Management System
ISO	International Organization for Standardization
IVRS	Interactive Voice Response System
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
KS	Kolmogorov–Smirnov
KYC	Know Your Customer
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
KMS	Knowledge Management System
LPG	Liquefied Petroleum Gas
MIS	Management Information System
MPLS	Multiprotocol Label Switching
NOC	Network Operating Centre
ODS	Operational Data Store
OLAP	Online Analytical Processing
OLTP	Online Transaction Processing
OTP	One Time Pin
OTS	Off The Shelf
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RDBMS	Relational Database Management System
RFP	Request for Proposal
RNP	Register of National Population
ROC	Receiver Operating Characteristic
SDK	Software Development Kit
SEDA	Staged Event Driven Architecture
SFTP	Secure Shell File Transfer Protocol
SI	System Integrator

Abbreviation	*Full Form*
SOA	Service Oriented Architecture
SOC	Security Operations Centre
SSN	Social Safety Net
SSO	Single-sign On
TSP	Trusted Service Provider
UIN	Unique Identification Number
USSD	Unstructured Supplementary Service Data
UA	User Agencies

Table of Contents

Acknowledgement 3
Abbreviations 4
1. Introduction 12
1.1. National Register of Population Program 12
1.2. Background 12
1.3. Scope of Work 13
1.4. About this report 13
1.5. Design Considerations 13
2. High Level System Overview 17
2.1. Logical layout of RNP System 18
2.2. Key Services of RNP System 19
2.2.1. Pre-Enrolment 19
2.2.2. Enrolment 20
2.2.3. Authorization, UIN Generation and Issuance 20
2.2.4. Authentication and e-KYC Services 20
2.2.5. Lifecycle Update Services 20
2.3. Solution Architecture Principles 21
3. RNP Functional & Technical Solution 23
3.1. RNP Software System 23
3.1.1. Core Applications 23
3.1.2. Support Applications 24
3.2. RNP - Data Store (RNP-DS) 25
3.3. RNP-DS Operations 25
3.4. Software Development Lifecycle Management 25
4. RNP Software System 26
4.1. High Level System Overview 26
4.1.1. Functional Overview 26
4.1.2. RNP Stakholder Ecosystem overview 28
4.1.3. Integration Overview of RNP System 29
4.2. Core Software Application Components 31
4.2.1. Pre-Enrolment Application 31

4.2.2. Enrolment Software 34
4.2.3. Identity Management System (IDMS) 37
4.2.4. Authentication Services (Authentication and KYC) Application 43
4.2.5. Automated Biometric Identification System (ABIS) 44
4.3. Support Application Solution Components 46
4.3.1. RNP Portal and Mobile Application 46
4.3.2. Business Intelligence and Data Analytics 48
4.3.3. Partner and Device Management 50
4.3.4. Identity and Access Management 51
4.3.5. Customer Relationship Management (CRM) 52
4.3.6. Document Management System 52
4.3.7. Knowledge Management System 53
4.3.8. Fraud Management 53
5. RNP Data Store 55
5.1. RNP Data Store Reference Model 55
5.2. Software Components of RNP-Data Store 56
5.3. Design of Data Store using Cell Architecture 58
5.3.1. Components of Cell Architecture 58
5.4. Overview of Data Center Deployment Architecture 60
5.4.1. Militarized Zone (MZ) 60
5.4.2. De-Militarized Zone (DMZ) 61
5.4.3. Management and Security Zone (MSZ) 61
5.5. Server Components 62
5.5.1. Server Reference Model 62
5.5.2. Server Types 62
5.6. Database 64
5.7. Storage and Backup Components 65
5.7.1. Distributed File System 65
5.7.2. Storage Area Network (SAN) 66
5.7.3. Tape Library 66
5.8. Network Infrastructure 67
5.8.1. WAN and Internet connectivity 67
5.8.2. RNP Data Store Network 70
5.8.3. Network and Network Security Components 73

5.9. Security Components 74
5.9.1. Security and Privacy Framework Components 75
5.9.2. Enhancement in the security posture 77
6. RNP Data Store Operations 83
6.1. Design, Supply, Install, Commission & Acceptance 84
6.1.1. Servers 84
6.1.2. Storage 84
6.1.3. Backup Target (Virtual Tape Library) 85
6.1.4. Tape Library 85
6.1.5. SAN switches 86
6.1.6. Network Components 86
6.2. Operations, Maintenance and Administration 86
6.2.1. Core Services 86
6.2.2. Support Services 87
7. Software Lifecycle Management 94
7.1. SDLC Overview 94
7.2. SDLC Management 95
7.2.1. Requirment Analysis 95
7.2.2. Design 95
7.2.3. Solution Development 95
7.2.4. Testing 97
7.2.5. Release Management 98
7.3. Continuous Build 99
7.4. Container Architecture 100
8. Enterprise Reference Model for RNP Solution 101
9. Assumptions and Parameters for Sizing 102
9.1. General Statistics 102
9.2. Estimation of Enrolments 102
9.3. Estimation of Authentication and e-KYC requests 103
9.4. Sizing of Packets for Enrolment and Identification Services 103
9.5. Estimation of Users 104
9.6. Technical Parameters 105
10. Annexures 106

10.1. Annexure-I: Consent Procedure 106
10.2. Annexure-II: Whitelisting procedure of Enrolment Officers 107
10.3. Annexure-III: RTO and RPO 108
10.4. Annexure-IV: Manual Adjudication Process 110
10.5. Annexure-V: Structural Validations 111
10.6. Annexure-VI: Use of Virtual ID in Authentication Services 112

Table of Figures

Figure 1: Level 0 (zero) diagram of the RNP System 17
Figure 2: Logical Layout of the RNP System 18
Figure 3: RNP Technology Solution 23
Figure 4: Functional Overview of RNP Solution 26
Figure 5: Overall RNP User Ecosystem 28
Figure 6: Integration Overview of R\NP 30
Figure 7: Pre-enrolment Process 33
Figure 8: Pre-Enrolment Application Technology Components 34
Figure 9: Proposed Enrolment Kit at the Enrolment Center 37
Figure 10: High level diagram depicting technical features of IDMS 39
Figure 11: Use Case of Enrolment 40
Figure 12: NIU Generator for EC and RNP Program 42
Figure 13: Identity services Technical components 44
Figure 14: Technical Overview of ABIS 46
Figure 15: Portal Components 48
Figure 16: BI and Analytics Components 50
Figure 17: RNP DS Reference Model 55
Figure 18: Components of Cell Architecture 58
Figure 19 - Server Reference Model - RNP Technology Platform 62
Figure 20: Network Architecture 69
Figure 21: DC Network Architecture 72
Figure 22 - Security & Privacy Framework Components 75
Figure 23 - Security Posture Enhancements 77
Figure 24 - Data Store Operations 83
Figure 25 - Software Development Lifecycle 94
Figure 26: Enterprise Reference Model for RNP System 101

1. Introduction

1.1. National Register of Population Program

The Government of Morocco aims to build an efficient and integrated system of delivery of social services and social spending. In 2011, the Government of Morocco adopted a new constitution, which in addition to governance procedures also aimed to promote equity and social inclusion in the country. In the context of new constitution, improving social service delivery and ensuring higher efficiency of social spending, constitute two key priorities.

Recently, the Government of Morocco has put in considerable efforts in Social Safety Net (SSN) programs and has implemented multiple initiatives. However, the collaboration between programs remain limited and fragmented due to which the required benefits do not get realized. One of the reasons for such fragmented approach and little coordination, as identified in the World Bank's report 'Identification for Development (ID4D), 2014', is due to the absence of established mechanisms for linking the same identity. Requirement for linking various repositories is imperative and can be achieved through creation of a Unique Identification Number (UIN) for all residents of Morocco.

The **National Register of Population (RNP)** will be a comprehensive database of all citizens and foreign residents of Morocco (in this report citizens and foreign residents of Morocco are being referred as 'Residents'). Each resident in the register will be unique and will be assigned an identification number. The objective is to create a system that successfully delivers services to residents under government programs using identity authentication mechanism. The RNP program does not envision to confer rights to an enrolled residents but shall only provide multi-purpose, verifiable and unique identity.

It is envisaged that the RNP program will have two main functions:

- Provisioning of unique foundational identity to all residents of Morocco
- Electronic authentication of the identity of each resident

With the RNP program, the government intends to improve targeting and data exchange with available SSN programs. The Government of Morocco envisions to extend the coverage of the population of Morocco with verifiable identity to better assess resident's eligibility for social benefits and to improve interoperability across different information systems of social assistance programs.

For effective and efficient implementation of the RNP program, the Ministry of Interior has engaged PwC as the consultants. The scope of work for PwC under this engagement has been detailed out in section 1.3 of this document.

1.2. Background

In the report titled '*L2: Implementation Roadmap & Strategy for the Implementation of the Project*', strategy of implementation of the various components of the project including enrolment, authentication, data centres, technology, procurement, etc., necessary for conceptualisation and preparing the implementation roadmap has been finalized. The present report has been conceptualised and prepared after consideration of the key decisions taken as part of the implementation strategy finalized in aforementioned report. A brief description of the issues covered in the implementation strategy and the decisions considered and taken in respect of the key aspects of implementation strategy is provided in Section 1.5 as a reference for the purpose of this report.

1.3. Scope of Work

The PwC's scope of work related to this deliverable as provided in the ToR is reproduced below for easy reference:

"The main objective of the Consultant in this activity is to formulate the detailed specifications of the technical and functional requirements for all components of the project, including application software and IT infrastructure. These specifications requirements as a basis for the preparation of the bidding documents for the design and development of RNP information system, acquisition and installation of the Datacenter and the acquisition and integration of the solution (hardware and software) handling of biometric data.

The consultant must prepare and document overview of the functional and technical solution of the system, and will provide input to the Detailed Project Report (DPR)."

1.4. About this report

This report titled *'L3 - Technical and Functional Solution Overview'* is intended to provide an overview of the complete RNP solution. In brief, this report covers the following:

- Functional and Technical Overview of RNP program,
- Functional and Technical features of the solution design,
- Overview of the RNP solution and its components,
- Enterprise reference model for the RNP solution,
- High level RNP Data Store operations, and
- Parameters used for sizing of the technology solution

The detailed technical specifications and functional requirements will be covered in a separate report titled *'L4 - Technical and Functional requirements specifications for the computer systems'*. In addition, report will also provide a detailed Bill of Material, Bill of Quantity and Specifications.

The estimated capital expenditure and operational expenditure of the RNP project will be provided as part of the report titled *'L5 – Detailed Project Report'*.

1.5. Design Considerations

The key implementation design principles that have been considered, as per decision taken (L2 report) for implementation of RNP program, to conceptualise the functional and technical solution design, are as enlisted below:

Pre-Enrolment	Before the enrolment stage, there shall be a pre-enrolment stage. In this stage, the resident will use online portal of RNP system to enter demographic details, upload supporting documents and take an appointment before going for physical enrolment at the Citizen Service Centre (CSC) of its choice

Enrolment	• A citizen who is 18 years and above coming for enrolment in the RNP system will produce CNIE card as a Proof-of-Identity. This will be mandatory before enrolment. Moreover, demographic information like Name, CNIE Number and Date of Birth will be verified with CNIE as part of enrolment validation process. • For enrolment of citizens below 18 years, the original birth certificate will be a mandatory document for Proof of Identity. • The enrolment under RNP program will be carried out in the designated centers. These centers will be known as 'Citizen Service Center (CSC)'. It has been decided that the current RAMED Centers would be designated as CSCs. In addition to the CSC of Ministry of Interior, the enrolment may also be outsourced to identified agencies (such as Banks) that could potentially undertake enrolment services. • There will be one or more enrolment officer in designated CSC for carrying out enrolment activities. These enrolment officers(s) will be deployed by the government. • The Ministry of Interior will provide network connectivity and will be responsible for provisioning and maintenance of connectivity at CSCs. • For undertaking enrolment, the enrolment software will be developed bespoke to ensure maintainability and flexibility to enable the use of different types of biometric capture devices. • The program will be implemented in two phases – in the first phase nearly 8 million population will be enrolled and in second phase, enrolment for the remaining population will be carried out. • Enrolment shall be multi-modal, i.e., photograph, fingerprints and iris biometric features will be collected from the residents during enrolment.
Design Principles	• The design principles to be considered for the RNP Solution are as follows: o Scalability & Mobility, o Security in Design, o Vendor Neutrality, o Interoperability, o Platform-based-Approach, o Manageability and Upgradability, o Flexibility, o Cost Effectiveness, and o Use of Automation • Overall IT design will ensure high availability, interoperability and compliance to the above mentioned design principles

System Design & Development	• Open source technologies and solutions will be utilized, wherever possible, for developing the complete RNP System to avoid vendor lock-in • A core application will be designed for the RNP System, which shall comprise all core functions of the system. Components other than those available in the core application will either be developed bespoke, or off-the-shelf products will be customized. • The core application components such as enrolment software, IDMS and authentication server will be developed bespoke to prevent vendor lock-in. • ABIS solution shall be procured from a single biometric solution vendor and multi-modal approach will be adopted. • For software lifecycle management, incremental Model of software development will be utilized.
Hardware Infrastructure	• Considering the evolving nature of the project the proposed IT infrastructure design shall be modular. Modularity is planned to be achieved through the concept of "Cell" and "Non-Cell". o Cell includes all IT infrastructure that needs to scale with growing enrolments and authentication o Non-Cell includes components that do not need to scale with growing enrolments and authentications
Data Centre	• There is a limited space at current data center facilities. Hence, MoI may engage a civil engineering firm to design and prepare the two data centers as per TIA 942 Tier III standards. • On basis of initial estimation, it seems 50 rack capacity at each data center may suffice the long term needs of Morocco Stack. However, the exact space requirements will emerge on the basis of infrastructure sizing which will be provided as part of report titled *'L4 - Technical and Functional requirements specifications for the computer systems'*. • A decision has been taken to use the existing data center at Ministry of Interior as Primary Data Center site and the existing data center at Hay Ryad as Disaster Recovery site. These current data centers would need augmentation of physical infrastructure like electrical, cooling, surveillance, LAN, etc.

<table>
<tr>
<td>Identification / Authentication</td>
<td>

A federated model of identity ecosystem will be built with two tiers. In the first tier, the Trusted Service Providers (TSP) will be able to access the RNP solution. In the second tier, the user agencies will send the identification service requests to RNP solution through Trusted Service Providers
Two major types of identity services will be provided as described below:

Authentication Service: The resident will provide a UIN and a factor of verification. In response, a ‘Yes’ or ‘No’ result will be provided by the RNP system. The authentication will be based on the factor of verification[1] (iris, fingerprint, photograph) captured at the time of resident enrolment and subsequent updates, if any.
Electronic Know Your Customer (e-KYC) Service: The resident will provide a UIN and a factor of verification. In response, the photograph and demographic details of resident will be provided by the RNP system. These details are ones captured during resident enrolment and subsequent updates, if any.

For privacy, a concept of limited e-KYC will be introduced wherein the response may be restricted to predefined fields depending upon the user agency from which the e-KYC request has been received
For availing the identity services, the following factors of verification will be permissible:
<table>
<tr><th>Factor</th><th>Authentication Service</th><th>Electronic Know Your Customer Service</th></tr>
<tr><td>Demographic Details</td><td>√</td><td></td></tr>
<tr><td>Fingerprint</td><td>√</td><td>√</td></tr>
<tr><td>Iris</td><td>√</td><td>√</td></tr>
<tr><td>One-Time Pin</td><td>√</td><td>√</td></tr>
<tr><td>Face</td><td>√</td><td>√</td></tr>
</table>
The biometric devices used for the purpose of identification services shall be registered with RNP solution

</td>
</tr>
</table>

[1] For OTP, the pin will be sent to mobile number registered in RNP system at the time of resident enrolment and subsequent update, if any

2. High Level System Overview

RNP is intended to provide online and verifiable identity to the citizens and residents of Morocco. This will lead to improved ability of residents to prove their identity on an anywhere anytime basis. This will also lead to the increased efficiency in service delivery and social inclusion. Thus, residents are at the heart of RNP program. With this consideration, the resident centric perspective of the RNP system is represented in the diagram given below:

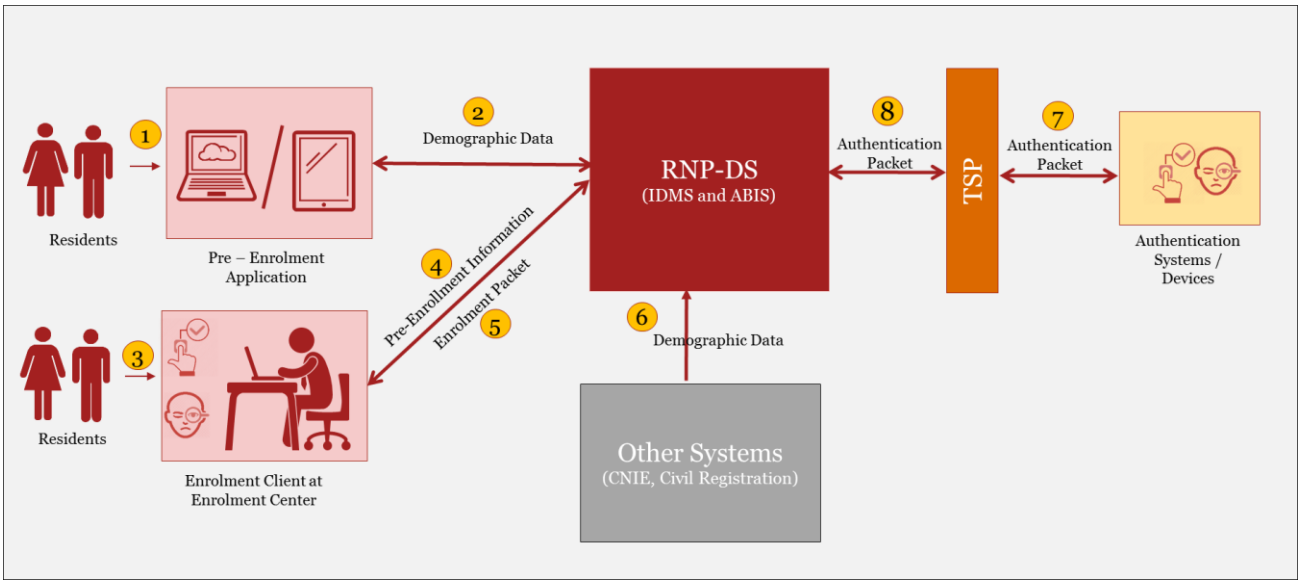


Figure 1: Level 0 (zero) diagram of the RNP System

The components of the system shown in the Figure 1 are described below:

- The pre-enrolment application will be used by the residents to enter their demographic information, upload their documents in support of the enrolment application, and obtain appointment at the enrolment center of their choice. The resident will be able to undertake pre-enrolment through their desktop, laptop or mobile.
- The resident will visit the enrolment center (referred to as 'Citizen Service Centre (CSC)') to register under the program. In the CSC, the enrolment officers will be able to enroll the resident using the enrolment software installed on the enrolment kit. During the enrolment, the resident's pre-enrolment information will be available at the CSC. After the enrolment, the resident's information will be bundled in a secure packet and sent to the RNP Data Store (RNP-DS). At the RNP-DS, the enrolment packet will be processed using a suite of software applications. As part of the processing, the enrolment information will also be verified against the other system as applicable. For example, for the citizens above 18 years of age, the information will be verified with the CNIE. Similarly, for new born the information will be verified with Civil Registration. In case the information is verified and approved as per the specified procedure of the CNIE / Civil Registration and RNP-DS is satisfied with the data quality and uniqueness of resident, the resident will be issued a Unique Identity Number (NIU).
- After getting the UIN, the resident will be able to utilize the same for obtaining the services of the government and private sector. The public and private sector entities interested in using the identity services of RNP will get registered with the RNP as Trusted Services Providers (TSPs) or User Agencies (UAs). At the time of service delivery, the resident will be able to prove their identities by giving UIN and their biometrics using the authentication devices. In the diagram above, the TSP can appoint User Agencies (UAs) for deployment of authentication devices. These authentication devices will have to be registered with RNP system before the identity services can be provided through these UAs.

- In addition to the citizen centric interface, there will be backend system which will be called as RNP Data Store (RNP-DS). This will be the technology system for delivering citizen centric services. The RNP-DS shall comprise two category of software applications – Core Applications and Support Applications. These applications will be hosted in the Primary Data Centre having a failover at Disaster Recovery Site.
- Core Applications will form the heart of the software solution. These will be critical to the delivery of citizen centric services and ensuing uniqueness and verifiability of the identities provided under the RNP program. Core applications category will comprise applications such as Pre-Enrolment, Enrolment Software, IDMS, Authentication Server, Integration Middleware, etc.
- Support Applications will augment the core applications for the provisioning, management and maintenance of services. This category would comprise applications such as Business Intelligence & Data Analytics, Customer Relationship Management (CRM), Portals, Knowledge Management System (KMS), Partner Management, Fraud Management, Identity and Access Management (IdAM), Document Management (DMS).
- RNP-DS would comprise the information technology infrastructure such as servers, storage, networks etc. and information technology platform such as Operating System (OS), Enterprise Service Bus (ESB), API Gateway Application, Web Containers, Domain Name Server (DNS), LDAP, Email, SMS Gateways, etc. to run the applications.

2.1. Logical layout of RNP System

The logical layout of the RNP system has been depicted in the diagram given below. The layout has been shown in a layered model.

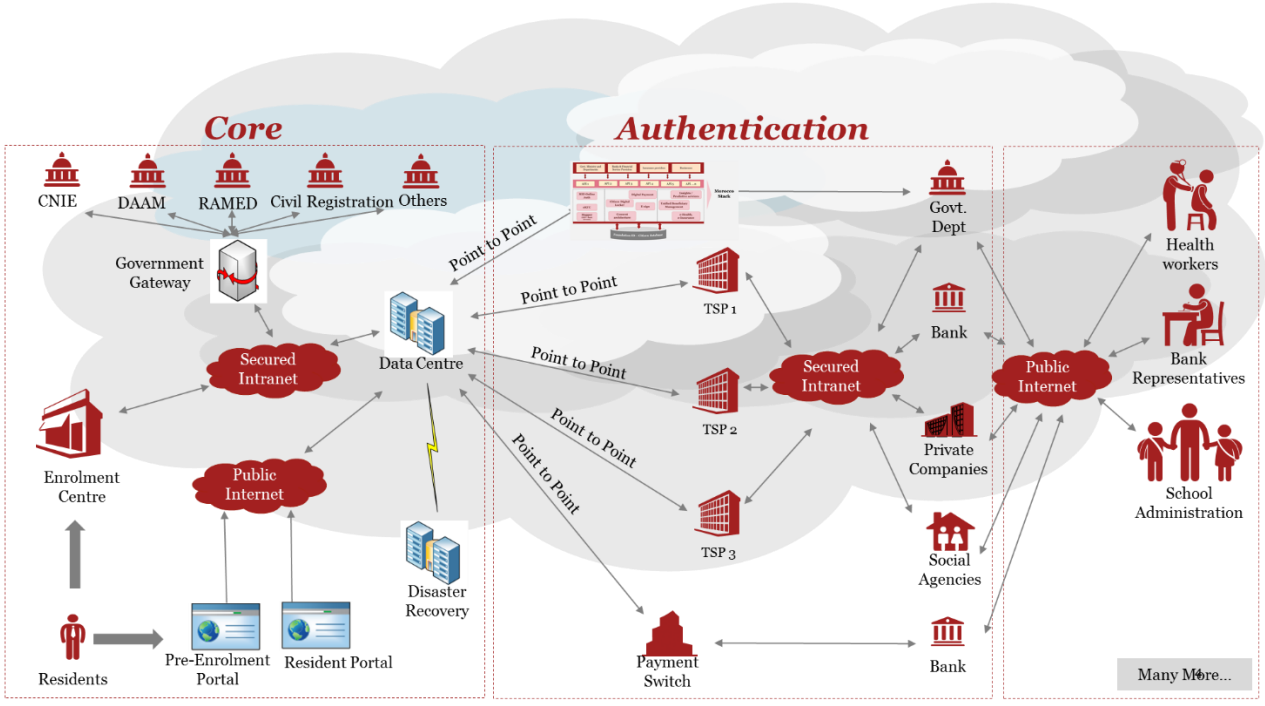


Figure 2: Logical Layout of the RNP System

The different layers of the RNP system are described below:

1. **Core Layer:** This layer shall consist of the RNP software applications, hosting sites, information technology infrastructure, enrolment centers, government gateway and network connectivity. The role of the software applications has been described briefly in the previous sub-section. The government gateway will act as the point for data exchange with the different stakeholders of the government and will result

in establishment of federal digital ecosystem. This federal digital ecosystem shall be built on top of the RNP Foundation Id System. The journey of the resident in this ecosystem is described below:

- The journey of a resident towards becoming a recipient of benefits and services from this digital ecosystem would begin with the resident pre-enrolling himself on a Pre-Enrolment portal available on the public internet.
- The resident would proceed for enrolment in a designated enrolment center to provide his demographic and biometric details. These details, once successfully encrypted and packed would be sent in a secure manner to the RNP backend applications to successfully allocate a UIN number and communicate the number to the resident through digital (SMS/Email) and physical means such as letter.
- The UIN number shall then be seeded through a Government gateway into various government database to provide direct benefit transfers, and removal of any ghost or duplicate entries, etc.
- Residents shall be provided with a facility to keep track of their enrolment requests, request for updates of their demographic information through a resident RNP Portal available on the public internet.

2. **Authentication Layer:** This layer shall be the interface to all the digital applications built for the Authentication and e-KYC functions. This layer has been modelled on a federated structure comprising Trusted Service Providers (TSPs) and User Agencies (UAs). The details of these two type of entities is provided below:
    - TSPs will be large entities (such as government departments, telecom companies, banks, etc.) which will directly and connected through a dedicated and secure connectivity. These TSPs would be required to invest in setup of infrastructure (e.g. Point to Point Dedicated Network to RNP-Data Store).
    - User Agencies (UA) wishing to utilize the identity services will route their requests through the TSP.
3. **Usage Layer:** This layer comprise end users who would access the RNP system to avail authentication and e-KYC services. The usage layer can be categorized into 2 types as described below:
    - **End User Applications**: These applications will be used for delivery of the public and private services to the residents. Some such services can be identified in the field of new mobile connections and bank accounts, healthcare services, school attendance, etc.
    - **Service Provider Applications**: These applications will use the authentication and e-KYC mode to deliver complex services to the end users. For example, the payment switch will be able to disburse the social benefits directly to the beneficiary's bank accounts. Other example is the layer of Morocco Stack, which will comprise new citizen centric services such as a digital locker, electronic signature, etc.

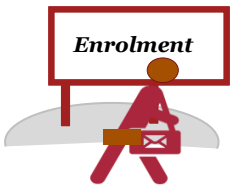
2.2. Key Services of RNP System

2.2.1. Pre-Enrolment

The Pre-Enrolment service shall provide the resident an option to pre-register the demographic details and obtain an appointment. For pre-enrolment the resident would fill in demographic details, upload identity documents, and schedule an appointment at the any enrolment centre within the province/prefecture whose Proof of Address is

submitted by the resident for enrolment As a confirmation of appointment, the resident will receive an acknowledgement that can be used during the enrolment process.

2.2.2. Enrolment



Enrolment service of RNP facilitates the resident to enrol into RNP for allotment of a UIN number. As part of this service, the resident has the option of visiting the enrolment centre with a pre-enrolment acknowledgement number/ receipt or directly walk-in without any such pre-enrolment. The Enrolment officer would collect the demographic details, biometrics profiles, verify/scan certificates as needed and provide acknowledgement receipt for making a successful application to the RNP. For remote areas, the mobile enrolment stations will be used for enrolment of residents.

2.2.3. Authorization, UIN Generation and Issuance

This service is related to the validation, de-duplication, quality-check, generation of UIN number, and communication of UIN Number to the resident. This is a sequential backend process carried out through a complex integration of IT and Biometric components.

2.2.4. Authentication and e-KYC Services

This service shall allow the resident to use the UIN generated by RNP for online real-time authentication at the point of service delivery of various agencies that subscribe to RNP services. For ensuring privacy, the resident would need to provide consent for using these services. For more details about consent, please refer Annexure-I: Consent Procedure. The authentication service can be Demographic, Biometric and OTP based and would provide only a YES or NO response. In case of KYC service, the RNP system would return the demographic details and the photograph of the resident.

2.2.5. Lifecycle Update Services

This service would allow residents to update their mobile number, address, email address either online or in assisted mode in the enrolment center. This will ensure that the demographic information in the RNP is up-to-date.

Once the child attains the age of 5 years, all biometric data should be provided by him/her by visiting the enrolment center. Using these biometrics, a deduplication exercise will be carried out while retaining the existing UIN allocated to the child. In case the child fails to update its biometrics within specified time, RNP may deactivate the UIN (in such case no authentication will be permitted). Similarly, the child on attaining age of 15 years has to again update his/her biometrics by visiting the enrolment center failing which UIN may be deactivated by RNP.

RNP may maintain a threshold for quality of biometrics and in case the quality of captured biometrics does not satisfy the threshold, the RNP may intimate the resident to update their biometrics. In addition, the resident may also choose to update their biometrics in cases when biometric their authentication requests are failing regularly.

In case of loss of UIN, this service can also be used to recover the same.

2.3. Solution Architecture Principles

The design principles to be adopted for the RNP system are as follows:

- **Scalability & Modularity:** The system should be scalable in-line with the rollout plan for all IT Infrastructure. It should be modular for each business service, catered by a separate module thus ensuring separation of transactions. As the system would increase the coverage, new authentication agencies would start using the system. Therefore, the system should be designed in such a way that required hardware can be augmented into the Data Center in an incremental manner on a need basis. Data partitioning/sharding should be leveraged to ensure that system can scale with growth in data. Application scalability should be ensured using Open API's and asynchronous design in logic allowing each resource to do its job, loosely coupled through a messaging layer. Use of Open API's also provide a layer to integrate application components from different vendors addressing issues related to single vendor.
- **Security in Design:** The system should have the ability to secure data from thefts, tampering, unwanted modifications, network attacks, and other security threats. Use of Hardware Security Module (HSM) Technologies, Public Key Infrastructure (PKI) based encryption, hashing algorithms, strong physical security, access management, stringent audits, non-repudiation, 24x7 Network Operations Centre (NOC) and Security Operations Centre (SOC) monitoring, data encryption should be strongly enforced to make system robust and secure from any data thefts. Further, only necessary and minimal information would be shared after the consent by the resident for using the online authentication service of RNP. For more details about consent, please refer Annexure-I: Consent Procedure.
- **Vendor Neutrality:** The system should make use of open standards, open frameworks and open source software to avoid vendor locking, wherever possible. The open standards allow robustness, longevity and continuous adoption of best-in-class technology by different technology vendors. To ensure openness and vendor neutrality, system should use open standards such as ISO based biometric standards, data standards like JSON, XML, open security standards for PKI, LDAP, open protocols like https, etc.
- **Interoperability:** The system should have the ability to interoperate with other systems / services using open interfaces, open data standards and ability to continually re-factor and/or replace specific components without affecting the rest of the system. Use of vendor neutral layers like open API's based on open data standards such as XML, JSON would provide the necessary loose coupling between different components allowing technologies from different vendors to seamlessly integrate with each other and which can be changed easily.
- **Manageability & Upgradeability:** The system should have the ability for end-to-end management of the components to ensure health of the system and adherence to service levels. For complete lights out operation, all layers of the system such as application, infrastructure must be managed through automation and proactive alerts rather than manual management. The entire application must be architected in such a way that every component of the system is monitored in a non-intrusive fashion (without affecting the performance or functionality of that component) and business metrics are published in a near real-time fashion. This allows data center operators to be alerted proactively in the event of system issues at a granular level. Application architecture shall also allow specific components to be watched very closely through a component level debugging scheme. The system should have the ability to seamlessly upgrade services, components, and modules without affecting services.
- **Flexibility:** The system should be designed for extensibility for specific features using a Metadata based approach, Business Rules and/or SOA based open APIs. Open Architecture adopting open standards

followed by multiple vendors would mean that the system can work with hardware and software procured from different vendors at different times. Open API's would enable the applications to be developed in such a way that the applications can run from mobiles, smartphones, tablets, desktops and laptops. Further, open APIs create a layer that is vendor neutral allowing multiple vendor products and applications to co-exist also enabling change of vendors whenever technology or scalability issues are encountered.

- **Cost Effective:** Low cost technology would be used to maximize benefits, avoid vendor locking, etc. Use of scale out architecture through horizontal scaling capability of hardware and data, use of open API's allowing different vendors to co-exist together would ensure low Total Cost of Ownership (TCO).
- **Use of Automation:** Automation would be adopted to minimize the cost of ownership especially in areas of testing, application & infrastructure monitoring, provisioning of new environments using virtualization technology and run book automation.
- **Performance & Availability:** Infrastructure and networks should be designed to support performance as per the agreed Service Levels (SLAs). Each application should be tested to identify and mitigate performance issues. The potential performance bottlenecks need to be identified and cost-effective paths for performance improvements should be provided for these identified problem areas. The system infrastructure should be architected considering failover requirements and ensure, a single server or network link failure does not bring down the entire system. The platform solution should support effective disaster recovery.

3. RNP Functional & Technical Solution

The RNP Technology Solution can be broadly categorized into four solution components viz. RNP Software System, RNP Data Store, Software Development Lifecycle & Release Management, and RNP-Data Store Operations. This section provides an overview of the RNP Technology Solution, which is depicted in the diagram given below. The details about each of these components are covered in the subsequent sections.

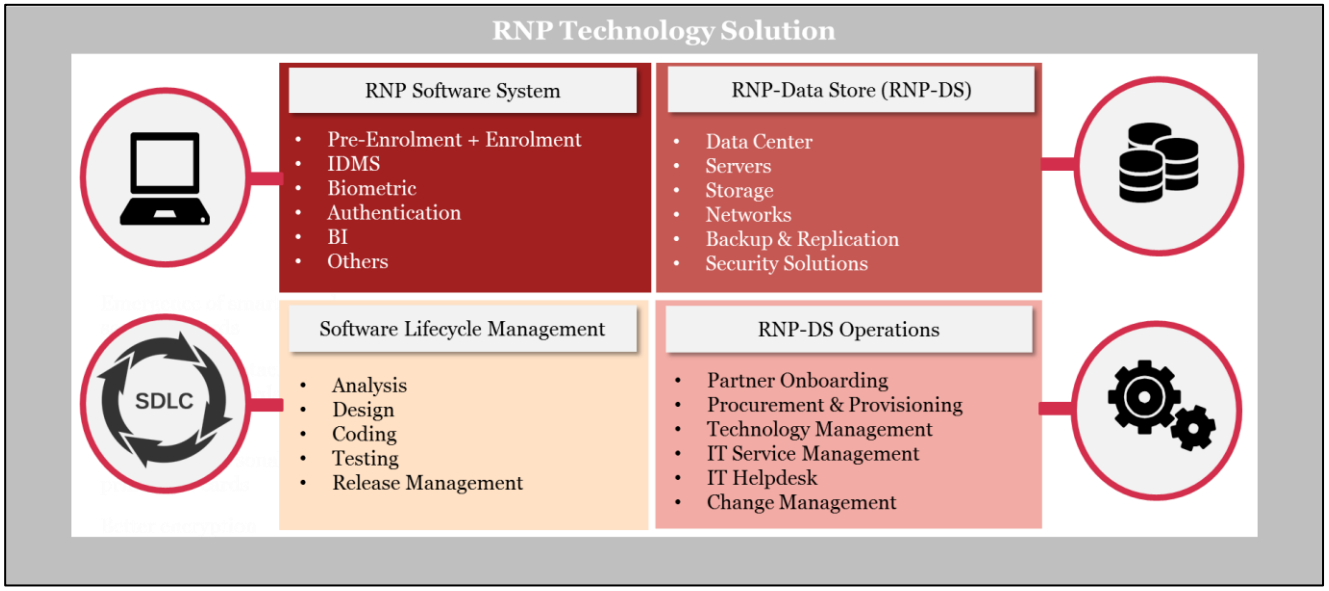


Figure 3: RNP Technology Solution

3.1. RNP Software System

RNP Software system shall contain the core application as well as support applications. The details about these applications is provided below:

3.1.1. Core Applications

The core applications category has multiple applications focused on a particular aspect of service delivery. These applications are described in brief below:

1. **Pre-Enrolment Application:** This application shall allow the residents to submit pre-enrolment information through a web based portal or mobile app interface and obtain appointment at any CSC within the province/prefecture whose Proof of Address is submitted by the resident for enrolment
2. **Enrolment Software:** This application shall be hosted on a Desktop/Laptop of the enrolment officer and will be used for enrolment of the resident. The enrolment officers would login using the UIN number and their own biometrics. Through this software, the Enrolment Office will fetch the pre-enrolment information (wherever applicable), enter remaining demographic information, scan supporting documents, capture biometrics (photograph, ten fingerprints and both iris). Resident information once captured would be stored in the desktop/laptop in an encrypted format for onward transmission to RNP-DS in a secured format.

3. **ID Management System:** This application shall receive in the enrolment packet and process it in a sequential staged manner from the validation of the packet to the generation of UIN number and intimation of the UIN to the resident. This application shall contain a management and a core layer. The management layer will orchestrate requests and the core layer will host the business logic. This system shall execute the following steps in a staged-wise manner through an orchestration middleware:
    - Ensuring structural integrity of the transmitted information along with other validations. For example, CNIE validation for resident of 18 years and above, and Civil Registration validation for new born
    - Perform a demographic de-duplication operation wherein any duplicates are identified based on demographic details
    - Coordinate a biometric deduplication operation with the Automated Biometric Information System (ABIS) to perform a biometric deduplication check for the enrolment packet
    - Generate UIN using a UIN Generator, which will be placed outside the IDMS and would be used for generating UIN for Civil Registration as well as RNP Program
    - Coordinate with SMS/Email system for sending the NIU number to the resident
    - Coordinate with printing agency in case the government decides to provide printed letters to the residents
4. **Authentication System:** This software application shall provide online authentication and e-KYC services. The core functions of authentication system shall include the following:
    - An extractor which extracts the biometric templates for newly enrolled residents and stores in a resident database. The resident database would be used for biometric based authentications.
    - The biometric matcher shall compare the biometric templates received as part of a biometric authentication request with the biometric template of resident stored in resident database after enrolment.
    - A set of open API's for different types of authentications (Demographic, Biometric and OTP).
    - A cached OTP retained and deemed valid for designated time period. Authentication requests would come to this application through an array of Trusted Service Providers (TSP) and User Agencies (UA).
5. **Automated Biometric Identity System:** This software application would perform the biometric de-duplication check for the resident. This software would contain a gallery of biometric templates against whom the de-duplication operation is carried and in case the 1: N de-duplication check passes successfully, the biometric template is added to the gallery with ABIS.

3.1.2. Support Applications

The support applications category has multiple applications that focus on a particular aspect of service delivery. These applications are described in brief below:

- **RNP-Portal:** The web portal and mobile application would be available to all stakeholders (residents, internal users, Call Center agents, TSPs and Administrators) to perform various functions under the digital identity ecosystem. The residents will be able to use applications such as pre-enrolment, public dashboard, enrolment status, etc. The internal users will be able to access applications like manual quality check, adjudication. The call center will be able to use applications such as CRM, Partner Management. The TSPs will be able to use the applications such as Partner Management.

- **Business Intelligence:** The data generated at various touchpoints from pre-enrolment phase to UIN generation phase would be assessed for the performance and efficiency of system to form the basis for continuous improvements of the RNP Solution. In addition to the data, the logs and events will also be assessed by the BI application.
- **Fraud Management:** The function of the fraud detection application would be to detect/prevent different types of frauds at all levels.
- **Other Applications:** Some of the other applications would be CRM, Partner Management, Document Management System, Identity & Access Management, etc.

This component of the solution is described in detail in Section 4 RNP Software System.

3.2. RNP - Data Store (RNP-DS)

The RNP-DS would form the backend of the RNP-System and would consist of the following:

Component	Sub-Component
Data Center Infrastructure	Servers, Storage, Networking equipment
Security Products	Firewall, DLP, Malware Protection, IPS/IDS, etc.
Technology Platform	System Software and Application Software

This component of the solution is described in detail in Section 5 - RNP Data Store.

3.3. RNP-DS Operations

IT system once live would be managed by a RNP-Operations team using a sound management framework based on ITIL. Following would be some of the key areas for RNP-DS:

- Technology Management (DBA, Server, Virtualization ,Storage & Backup, Network, Middleware Administration)
- Incident Management
- Change Management
- Event Management & Correlation
- Problem Management
- Configuration & Asset Management
- Application Support
- Availability, Performance and Capacity Management
- IT Helpdesk
- Tools Management
- Release Management
- Partner onboarding
- Procurement and Provisioning

This component of the solution is described in detail in Section 6 - RNP Data Store Operations.

3.4. Software Development Lifecycle Management

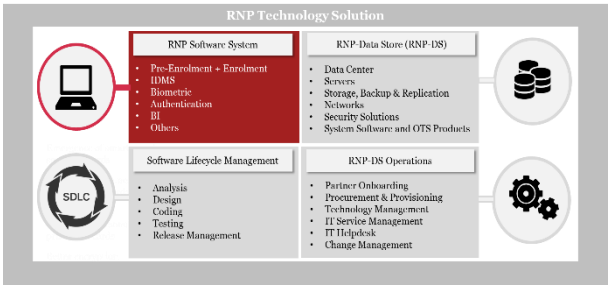
The Software development, enhancements and customization would be carried out using Software Development Lifecycle Services (SDLC) such as Iterative, Waterfall, etc., and would typically consist of Analysis, Design, Build, Test, and Deploy stages.

After release of version 1.0 of the RNP solution, it is recommended to move to iterative model for continuous integration, continuous testing and deployment in a phased manner.

This component of the solution is described in detail in Section 7 - Software Lifecycle Management.

4. RNP Software System

This section deals with the RNP software system component of the overall RNP Technology Solution as given in Figure 3. This section, inter alia, brings out the detailed functional and technical feature of the component. Following sub-sections are covered in this section:



1. High-Level System Overview (sub-section 4.1)
2. Functional Overview (sub-section 4.1.1)
3. RNP User Ecosystem Overview (sub-section 4.1.2)
4. Integration Overview of the RNP System (sub-section 4.1.3)

4.1. High Level System Overview

The high level system overview of the solution is provided in Section 2 - High Level System Overview where Level-0 (zero) details have been given. In this sub-subsection, the Level-1 details are provided, which show the internal building blocks of the RNP-Software System.

4.1.1. Functional Overview

The functional overview of the RNP software system is depicted in the diagram given below:

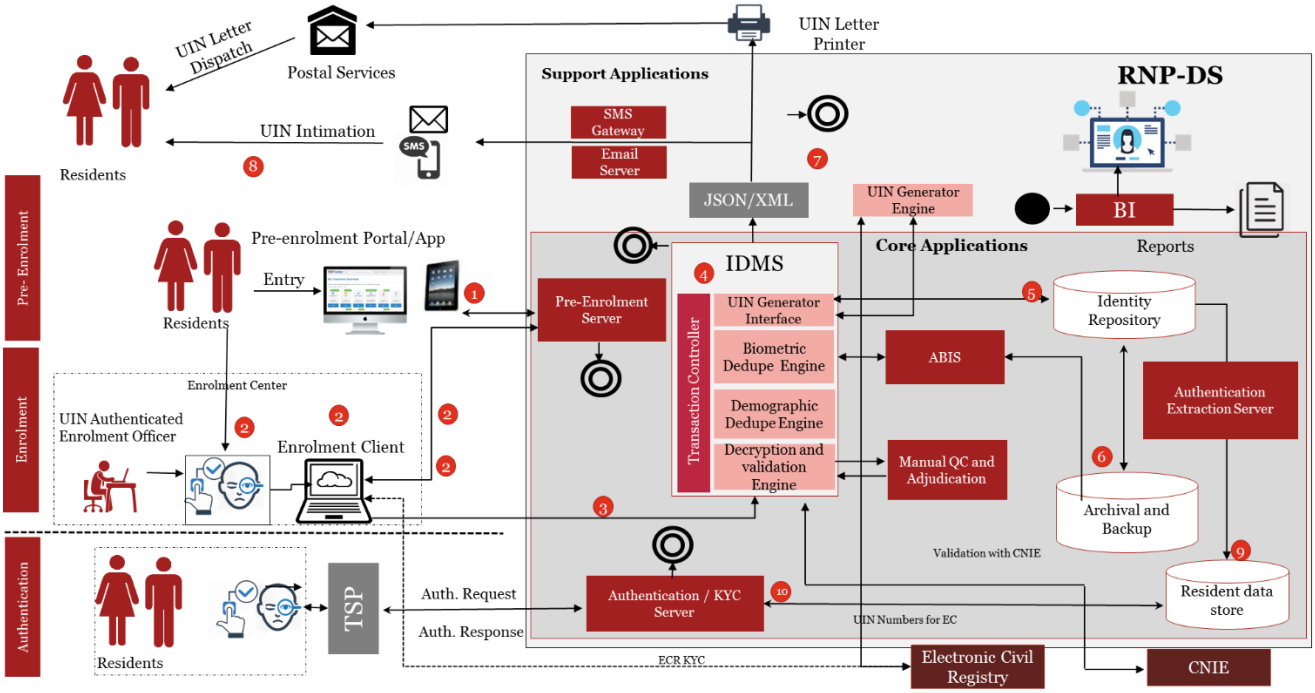


Figure 4: Functional Overview of RNP Solution

The diagram given above shows 10 steps of RNP solution, which are described below:

1. **Step-1**: The journey of the resident towards obtaining the UIN number starts with the pre-enrolment step, where the resident submits demographic details, upload scans of supporting document, choose a

convenient enrolment center and a time slot for appointment. Once the resident submits preferences and details, these are stored in the pre-enrolment server and resident is sent a pre-enrolment reference number as an acknowledgement with the date and time-slot for enrolment in the choice of center. The resident can take printout, SMS of the pre-enrolment acknowledgement number and visit the enrolment center on date and time of appointment. The residents who don't pre-enroll themselves in the system, can also visit the enrolment center during the working hours of enrolment center.

2. **Step-2:** At the enrolment center, an enrolment officer starts the enrolment process for the resident by logging into the enrolment software using his UIN number and biometric. Once logged in, enrolment officer can start capturing the biometric and demographic details of the resident. The complete session details shall be logged to ensure the officer is carrying out the process and storing the information in a legitimate fashion. At the start of day, the details of the pre-enrolment (except scanned documents[2]) of resident who have appointment on the given day will be automatically downloaded on the enrolment kit. The officer can retrieve the pre-enrolment information of the resident, wherever applicable, using the pre-enrollment reference number furnished by the resident. In case the resident has not pre-enrolled, the enrolment officer can enter the demographic data as per the physical enrolment application form filled by the resident at the enrollment center. The enrolment officer would check, scan and upload supporting documents, as applicable. Subsequently, the enrolment officer would collect the resident's biometrics, which would include a photograph, scan of 10 fingers, 2 iris scan. In case, the quality of captured biometrics are not of desired quality the enrolment officer would recapture the same. The enrolment officer would verify the captured information with the resident and make necessary corrections, if any. Once the resident and enrolment officer are satisfied, the enrolment officer will again provide its own biometric to complete the registration. At the end of enrolment, acknowledgement receipt bearing enrolment reference number and enrolment details would get generated. The enrolment officer will take printout of the acknowledgement receipt[3] and hand it over to the resident for reference. The enrolment officer will also take another print of the acknowledgement receipt for its reference. At the end of enrolment, the details captured would be sealed in an enrolment packet in an encrypted form. For cases involving handicapped individuals, resident without biometric exception processing[4] would be available in the enrolment software. For children, birth certificate carrying a UIN number allotted by Electronic Civil Registry (ECR) or manual birth certificate would be required. Similarly, for residents above 18 years, CNIE card will be required.

3. **Step-3:** Enrolment packets would be transferred to the Identity Management System (IDMS), which is the backend system of the RNP technology solution, in a secure manner using Secure File Transfer Protocol (SFTP). IDMS is responsible for data processing from initial validation of packet, to coordinate for generation of the UIN number, and till onward communication in a sequential staged manner.

4. **Step-4:** The enrolment packet received would be first checked for any virus/malwares and structural integrity by the IDMS. Thereafter, it will be validated for information such as comparison with CNIE (for 18 years and above) or Civil Registration (for new born) data, ensuring the operator who sent the packet was active, checking if the packet was sent from a registered device, etc. Once the packet crosses the validation stage, it is then sent for de-duplication check using the demographic details in the packet, followed by a biometric data de-duplication. The IDMS is integrated with the ABIS which runs the biometric de-duplication activity and returns the status of de-duplication request to IDMS. In case the biometric de-duplication fails, a manual adjudication check is performed to ensure there are no False Rejections for any resident. A successful de-duplication means that a UIN number can be allotted to the resident and the same can be communicated by SMS/email/letter to the resident. The IDMS is integrated

[2] The scanned documents can be seen by the enrolment officer on need basis

[3] The acknowledgement receipt will contain details concerning the enrolment transaction (date, time, CSC code, etc.) and resident (name, photograph, listing of fingerprints captured, etc.). This refers to acknowledgement receipt, listing the fingers which have been captured. This is more relevant for biometric exception cases, where resident may not have all fingers. However, the exact format of the acknowledgement receipt has been to be finalized by MOI at the implementation.

[4] For handicap persons, the EO will be able to mark missing finger(s) and/or Iris on the EO and take photograph of the same as a proof. At the time of processing of such packets in IDMS, approval will be required during manual adjudication.

with the NIU Generator, which generates, allocates and returns a unique number on request to IDMS. The NIU generator would be a common engine, placed outside IDMS, that would generate UIN numbers for usage in RNP scheme as well as Electronic Civil Registry (ECR) for registration of birth for new born. This number would be available to ECR using a UIN fetch API.

5. **Step-5:** Once the UIN number is generated, UIN and enrolment information (demographic details, photograph of resident and biometric information) are stored in the identity repository.
6. **Step-6:** An archive of the enrolment packet is stored in filesystem for archival and backup.
7. **Step-7:** UIN number and other details will be sent for printing of UIN letter and dispatch to resident.
8. **Step-8:** UIN number allocated to the resident would be communicated to the resident using SMS/Email.
9. **Step-9:** The authentication module extracts the biometric and demographic details from the identity repository to create a resident data store which would be used for Authentications and e-KYC services.
10. **Step-10:** A resident who is required to get identified for service delivery by any authentication agency submits UIN number along with demographic/biometric details depending on the type of authentication. The authentication server receives the request and invokes the appropriate API (OTP/biometric/demographic) for authentication. Once the biometric authentication API is invoked, it would use the Biometric Matcher, wherever applicable, to return the response. The Biometric Matcher will be provided by the ABIS provider in form of a Software Development Kit (SDK). The consent[5] of the resident will have to be obtained by the User Agency for using the Authentication or e-KYC service.

4.1.2. RNP Stakholder Ecosystem overview

RNP system will have a wide ecosystem of stakeholders, which will be interacting with RNP system for various purposes. The diagram given below depicts some of the key stakeholders within the RNP ecosystem.

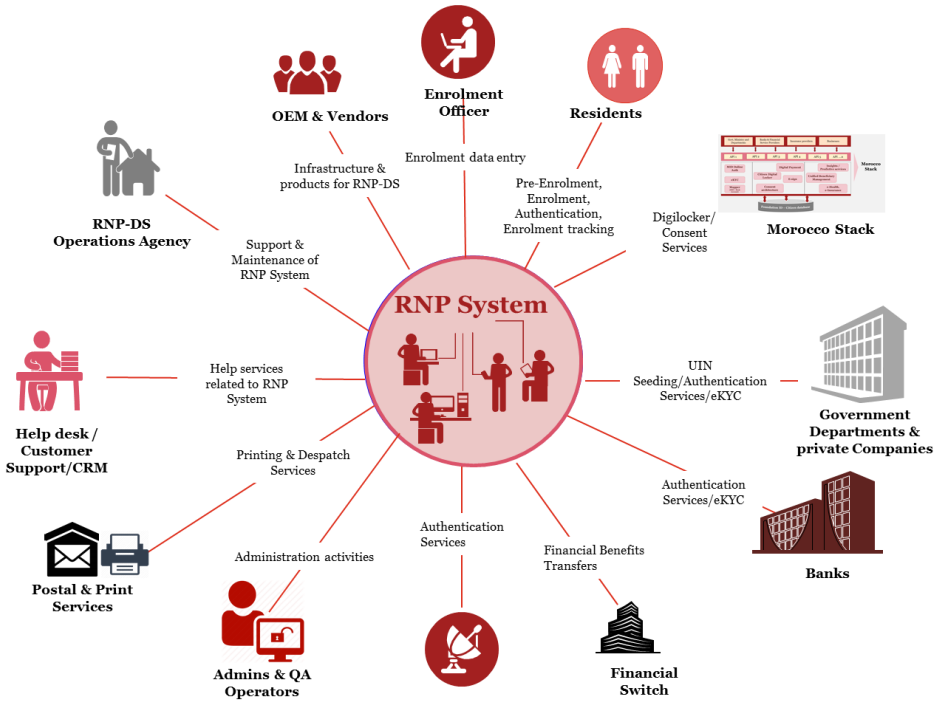


Figure 5: Overall RNP User Ecosystem

[5] For more details about consent, please refer Annexure-I: Consent Procedure.

A quick overview of all the potential stakeholders(s) is given below:

- **Enrolment Officers:** They shall be responsible for enrolment of the residents who present themselves at the enrolment centers. They would be interacting with the RNP system using an enrolment software that shall be available on desktops/laptops at the enrolment centers.
- **Residents:** The most important stakeholder in the system. Residents would be recipient of the UIN number and shall interact with the system in different ways – during pre-enrolment using the pre-enrolment application, during enrolment at the enrolment centers, during authentication as and when required by some User Agencies (UA). They would also be the users of the RNP Portal.
- **User Agencies (Government Departments, Private Companies, Banks, Health Agencies, and Social Sector Agencies):** These comprise the user agencies providing banking, telecom, healthcare or any other services, etc., and require to verify identity of residents who want to avail their services. The authentication requirement maybe a simple YES/NO answer or a KYC (complete demographic detail with the photograph).
- **Trusted Service Providers:** These TSPs shall be the gateway to the RNP system for user agencies, which want to avail the authentication services of the RNP system. The role of TSP would be to form a security fence around the RNP-DS. Only TSP would have any direct network connection with the RNP-DS. Thus, TSP will act as an additional layer of governance and control for the RNP Solution.
- **Financial Switch:** This would be a custodian of mapping information between financial institutions like bank account numbers, postal account numbers, etc., and the UIN numbers of residents who wish to avail direct transfer of government subsidies based on their UIN numbers. This switch would be useful for transfer of benefits to residents' bank account.
- **OEM and Vendor(s):** The manufacturers and suppliers of hardware, software, and services for the RNP solution and enrolment centers, etc.
- **RNP-DS Commissioning and Operations Agency:** The agency that would manage the RNP-Technology solution post go–live and rollout.
- **Call Center and IT Help Desk Operators:** The operators that would provide CRM services and grievance redressal support to the residents, enrolment officers, partner agencies including UAs and TSPs.
- **Administration and Quality Check Operators:** Internal users who would be responsible for administration of different applications in the RNP Software System. Quality Check operators would perform manual adjudications and decision making during demographic / biometric deduplication or validation with external systems like CNIE.
- **Morocco Stack:** This is a stack of APIs that would leverage the RNP Software System to modern citizen centric services such as a digital locker, electronic signature, electronic consent, etc. For more details about consent, please refer Annexure-I: Consent Procedure.

4.1.3. Integration Overview of RNP System

RNP Software System will need to integrate with external systems such as CNIE, NIU Generator and Trust Service Providers. Within the RNP Software System, there will also be a need to integrate different components. The high level understanding of how the RNP system will get integrated with external systems as well as with internal components is provided in the diagram given below:

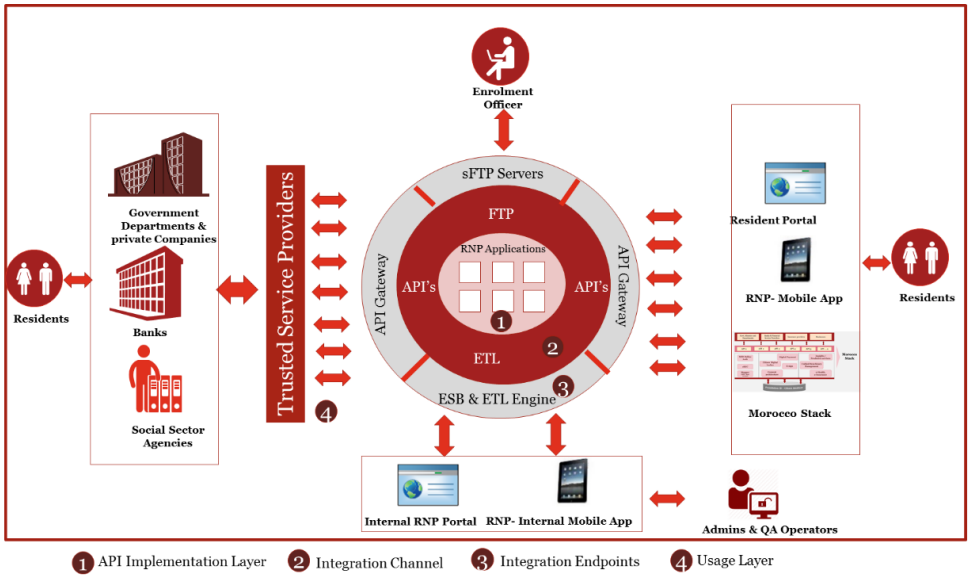


Figure 6: Integration Overview of R\NP

There are three major channels of integrations namely Open API's, ETLs and SFTP. These are described below in detail:

1. **Open API's** would be the major integration channel for integration with external applications and also for integration of internal applications. These API's would be exposed to external systems (TSP/UA/Residents) on biometric devices, web applications, mobile Applications & portals using API Gateways. For internal consumption of services within RNP-DS applications, these API's shall also be exposed using an internal Enterprise Service Bus (ESB) or an API Gateway. Advantages of using API based integration are provided below:

    - **Choice/Flexibility**: Users across the RNP ecosystem gets the choice and flexibility of using their preferred application and user interface without having to depend on a single portal.
    - **Innovation**: Application ecosystem can innovate in terms of providing all kinds of features such as offline capabilities, alerting capabilities, mobile/tablet interfaces, and so on as device and user interface technologies evolve without RNP system to build all possible features into a single portal.
    - **Agility**: When entire system is loosely coupled via components exposing APIs, it allows individual API implementations to change without having to affect the rest of the system. Building the entire system as a monolithic application completely takes away the agility of RNP to adapt to the changing policy decisions and rules. API driven approach allows encapsulation of components and data models without every other part of system knowing the details. API based design also allows automated testing of the entire system to ensure changes are quickly tested in a completely automated way to avoid regression.
    - **Manageability**: API based systems allow easy manageability in terms of monitoring, auditing, and performance analysis. In addition, individual APIs can be version controlled and deployed/upgraded/rolled-back instead of entire application being released, tested, and deployed.
    - **Scale**: For a national system like RNP to scale, load has to be distributed across various systems. This is key for responsive user experience as well as core system scaling. Instead of entire application being monolithic and access via web portal, if should be built with stateless APIs that can be scaled horizontally. Most critically, user interface load is distributed to external

applications making RNP System truly a lean platform that can be scaled to country's need. Providing stateless APIs allow load balancing across data centers for scale and distributing user interface load to 3rd party applications.

- **Data consistency**: Providing APIs to access all data models and functionality ensures data is not duplicated unnecessarily. This offers a single source of truth of data to be managed via common APIs. In addition, providing centralized data validation, digital signature, etc. ensures data is consistent and accurate across the system.
- **Security**: Data security is paramount to RNP system. Accessing data only via APIs ensure centralized management of security controls. Encapsulating access control, auditing, confidentiality (via encryption), and integrity (via signatures) is only possible via common APIs.
- **Cost effective**: Most importantly, RNP system can be kept simple, scalable, API driven, 3rd party application driven, and agile to meet the changing needs of residents, ecosystem partners, and policy makers which ensures that the cost of entire system is kept minimal while providing all core features and functionalities.

2. **ETL** would be used for integration of all application data with the Data Warehouse, Business Intelligence, Analytics, Fraud application, etc.
3. **SFTP** would be used for secured transfer of enrolment packets from enrolment centers to IDMS.

4.2. Core Software Application Components

These applications are defined in Section 3.1 as Core Application. While a brief definition of Core Applications has been provided in the previous section, this section details out the functionalities and technical features. This section comprise the following:

1. Pre-Enrolment Application (sub-section 4.2.1)
2. Enrolment Software (sub-section 4.2.2)
3. Identity Management System (sub-section 4.2.3)
4. Identification Services (Authentication and e-KYC) Application (sub-section 4.2.4)
5. Automated Biometric Identification System (sub-section 4.2.5)

4.2.1. Pre-Enrolment Application

The objective of the pre-enrolment software would be to improve the quality of demographic data capture and reduce the enrolment time at enrolment centre. This will also help in increasing throughput of enrolment centre and reduction of overall enrolment cost. The pre-enrolment service will be offered through the citizen portal and citizen mobile application. This pre-enrolment Application is an optional facility for the residents where the resident would have the facility to go for enrolment with a prior appointment. In case the residents who do not avail this facility, can still go for enrolment to any of the enrolment centres of choice within the province/prefecture whose Proof of Address is submitted by the resident for enrolment.

4.2.1.1. Key Functionalities of the Pre-enrolment Application

The key functionalities of the application are provided below:

- **Timeslot availability:** The Pre-enrolment application would maintain a list of available timeslots for appointment at each of the enrolment centers and would make this available as a real time service via open API's / web services enabling residents to check and make appointments for the enrolment services at enrolment centers.

- **Appointment bookings:** The pre-enrolment application would provide the facility of making appointment bookings from a set of available slots returned by the timeslot availability feature of the application.
- **Location dictionary:** A location dictionary would be available in the pre-enrolment database and would be mapped to the enrolment centers in the chosen geographical location. Depending on the address of the resident, a list of locations where enrolment can be done would be available for choice. The location dictionary would also contain latitude-longitude details for the pre-enrolment centers for display on the pre-enrolment web page using public geographical API's from Google, Bing or other GPS/Map services providers.
- **Demographic data capture:** The application would allow demographic data capture by the resident. Some of the key fields to be entered would be Name, Date of Birth, Gender, Address, Email, Mobile number, and CNIE number. The address field would be divided into multiple entry fields where certain information such as Province, Region, etc., would be available in drop box menu.
- **Document upload:** The application would allow the resident to upload scans of documents to provide Proof of Identity and Proof of Address.
- **Acknowledgement receipt:** The application would allow the resident to submit details. Once details are successfully submitted, an acknowledgement containing the pre-enrolment number, chosen enrolment center and date/time of appointment would be available for printing. In case the resident has provided a mobile/email, the receipt would be emailed and/or send as a SMS message to the resident.
- **Available on public internet:** The pre-enrolment application would be available and accessible as part of the RNP Mobile app and RNP portal on the web for residents of Morocco. The pre-enrolment facility will also be available to citizens of Morocco living abroad. These citizens will be able to submit a request which will get approved subject to verification from CNIE.
- **GPS APIs & Location Services:** The pre-enrolment web pages would be integrated with location based services like google maps or any other map service provider allowing residents to find the location of the enrolment center on the Web. A pre-requisite for this functionality would be that the enrolment centers be geo-tagged in the pre-enrolment database.

A diagram showing the key steps in pre-enrolment is shown below:

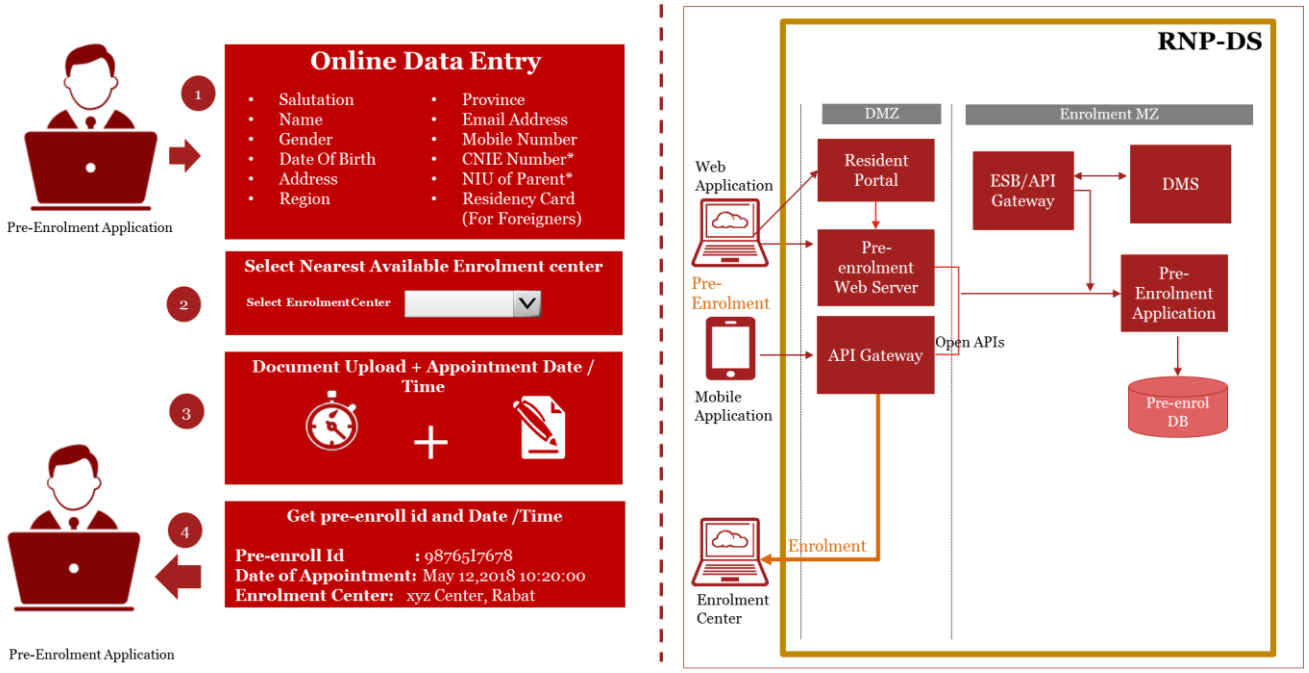


Figure 7: Pre-enrolment Process

4.2.1.3. Key Technical Features & Components

A logical overview of the technology features of the pre-enrolment application are shown in the diagram below:

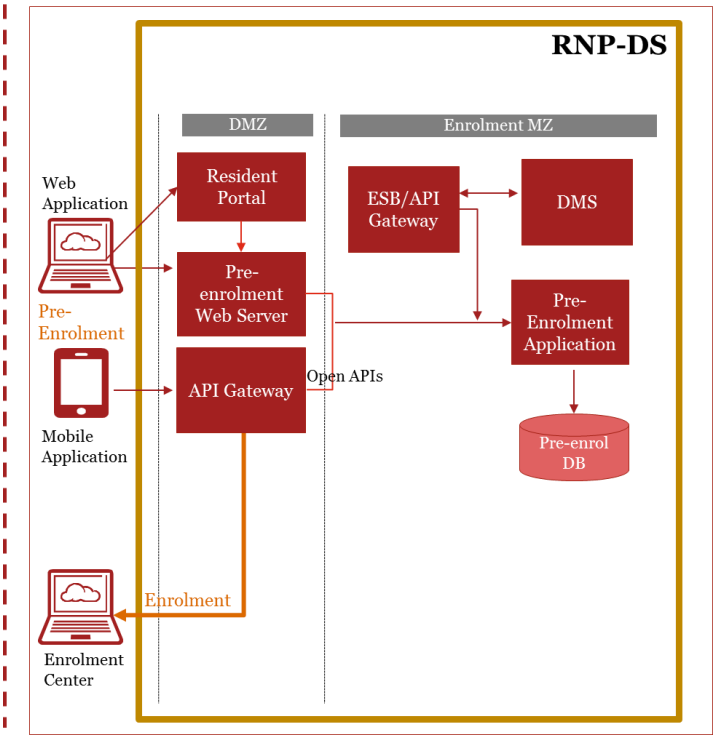


Figure 8: Pre-Enrolment Application Technology Components

The key technical components in the Pre Enrolment Architecture are listed below:

- Web Server for static html pages
- API gateway to provide the API's that need to be consumed by the mobile application for RNP
- Enterprise Service Bus(ESB)/API Gateway for hosting all the web service/API endpoints for internal consumption and external consumption by Pre-enrolment and other applications
- Application server would host the actual implementations of the APIs / Web services
- Resident can use the pre-enrolment application through a link on the Resident Portal which would be directed to pre-enrolment web server.
- **Software Development Strategy:** Bespoke Development on Open Source OTS technology Platform.

4.2.2. Enrolment Software

The function of the enrolment software would be to undertake enrolment at the RNP enrolment centre, an open source technology based software shall be used. This software will be integrated with biometric capturing devices of various manufacturers, which are compliant to identified biometric standards.

4.2.2.1. Key Functionalities of the Enrolment Software

The key functionalities of the application are provided below:

- **Software, User and Configuration Management:** Enrolment software would have the capability to configure users and devices to enable administrator and enrolment officer to login to the system using

a Desktop or a Laptop. The enrolment officer would be required to login using UIN number only to a mapped device. Necessary configurations would be setup on the desktop/laptop by an enrolment software admin. These configurations would only be available to the enrolment software admin and not to an enrolment officer.

- **Secure Biometric Login:** Enrolment software would allow the enrolment officer to login using his UIN number and biometric authentication mechanism.
- **Location and Other Master Data Download:** Location codes and other master data would be available in the local database of the enrolment software and would be regularly synchronized to ensure any changes in master data are available on the enrolment software end at all times. This synchronization would happen automatically either as a push /pull operation from the RNP Software System or Enrolment Software.
- **Pre-enrolment Data and Certificates Downloads:** The enrolment software would have the capability to download all the pre-enrolment data in advance from the pre-enrolment sever to ensure minimize network transactions during the enrolment session for residents who availed the pre-enrolment facility. Enrolment Software would only allow download of pre-enrolment information of the residents who have appointment in that enrolment center only for that particular day.
- **Demographic Data Capture:** The application would allow demographic data capture by the Enrolment Officer. Data would be populated from the pre-enrolment application or the enrolment officer would manually enter the data of resident on the basis of the physical form filled by the resident. The key fields to be entered would be name, date of birth, gender, address fields, email, mobile number, and CNIE number. As the address would be a free text, the address field would be divided into multiple entry fields where certain information such as province, region etc., would be available as drop box. The fields in these drop boxes would be populated using the master data available in the enrolment software.
- **Document upload:** The application would have the capability to scan and upload documents of the resident in case the resident is either not pre-enrolled or there is a need to change the documents. 'The registration kits (webcam, fingerprint reader, iris reader, scanner, etc.) should only operate with the enrollment software.
- **Biometric Data Capture:** The application would have the capability to capture biometrics such as all fingerprints, iris and photograph of the resident. The biometrics captured would be checked for quality using biometric quality check APIs and once a minimal acceptable quality of biometric capture is achieved, the enrolment software would enable the enrolment officer to proceed with completion of enrolment. On completion of enrolment, a Data Packet will be created to be transmitted to the RNP-DS.
- **PKI Encryption:** All data packets that will be created will get encrypted using PKI encryption technology. Only public keys are stored in the enrolment kit and the location is configured by the Admin. The public keys are not accessible to the user for any kind of modification purpose. Audit log information about these keys (Timestamp for creation/update, Hash of the key etc.) are stored on the RNP-DS, so as to enable audit of the enrolment software PKI keys to detect any tampering of keys. During the enrollment session, data entered would be maintained in memory in an encrypted form for enhanced security. All data stored would be digitally signed by the enrolment officer.
- **Local Storage & Secure File Transfer:** Enrolment software would have the capability to store information such as master data and enrolment packets in a secure fashion. The Enrolment software would have a database where all information is stored locally. It will also have the facility to securely transfer the enrolment packets to RNP-DS.
- **Audit Logging:** The audit information such as “who was enrolled, enrollment officer information, supervisor information, time taken for enrolment, location of enrolment, any exception conditions etc.” will be associated with every enrolment session which would be logged by the enrolment software. This information would be used to ensure that continuous quality is achieved while enrolment is carried out.

Even mouse clicks and other detailed information could be captured for security auditing and scanning etc. The enrolment software would also be capable of a running a scan (triggered from the RNP-DS) of the machine on a periodic basis to ensure no fraudulent activity has happened (e.g. tampering the configuration of enrolment software etc.).

- **Enrolment number generation and Receipt print:** Once enrolment information is collected and packet has been sealed with encryption, an acknowledgement number is generated and a receipt can be printed and handed to the resident.
- **Secure Sync:** A secure synchronization with RNP-Software System would enable the enrolment packets to be transferred to the RNP-DS in a secured fashion.
- **Quality Management:** To ensure biometric de-duplication and authentication, the captured biometrics should be of good quality. For ensuring that good quality biometrics are captured by the Enrolment Software, there would be quality assurance components in the Enrolment Software. These components will use biometric quality check APIs.
- **Capability to address Exception Conditions:** The enrolment software would have the capability to address exceptional conditions such as handling persons who are handicapped, people with poor quality of biometrics, people without any documents, etc. While the normal default behavior would be to capture all the biometrics, in case a person is handicapped, Enrolment Software should permit the Enrolment Officer to override the default behavior using a manual override. In such case, a photograph of the person showing handicapped hands would be need to be mandatorily captured.

4.2.2.2. Key Technical Features & Components

The important technical features and components required for enrolment software are as follows:

- Enrolment software would be capable of running on most of the leading Desktop/Laptop operating systems.
- Packets would be encrypted using 2048-Bit encryption.
- Master data synchronization should be possible using a backend batch on the enrolment software.
- Enrolment software would have administration features to enable Enrolment Software Admin to setup the public keys, master data synchronization frequencies, whitelisting of device for only valid UIN numbers of enrolment officers. The whitelisting refers to registering the Enrolment Officers and allowing them access on designated enrolment kits. Through this process, only those enrolment officers which have been registered on the given enrolment kit, will be able to access the enrolment software. The details about whitelisting of Enrolment Officers is given as Annexure-II.
- Enrolment software would have export utility, which would allow the enrolment officer to export the successfully created packets from the enrolment software to RNP-DS.
- Enrolment software would also have a packet cleanup utility that would automatically clean the client system. Once the data packet is successfully sent to the RNP-DS and specified duration for which packets must be stored within enrolment kit has elapsed, the cleanup utility will clean the packets and relevant information from the enrolment software. The duration for storage of enrolment packets within enrolment kit will be configurable from the IDMS.
- There would be API's for biometric quality compliance, transliteration and location capture.
- For security reasons, end client would be provisioned as a virtual machine which is Dongle bootable. The VM would be preconfigured hardened VM where access to keys, and data folders where sensitive data is maintained unavailable to the Enrolment Officer. Only Application components would have access to the folders.

- Enrolment Software would also have the capability to create minutiae of the raw images and sending that to the RNP-DS in case an online system is desired at a later stage. These minutia would be created using Biometric SDK built into the client layer.
- **Software Development Strategy:** Bespoke Development on Open Source OTS technology Platform

The enrolment kit for the enrolment software is shown in figure below:

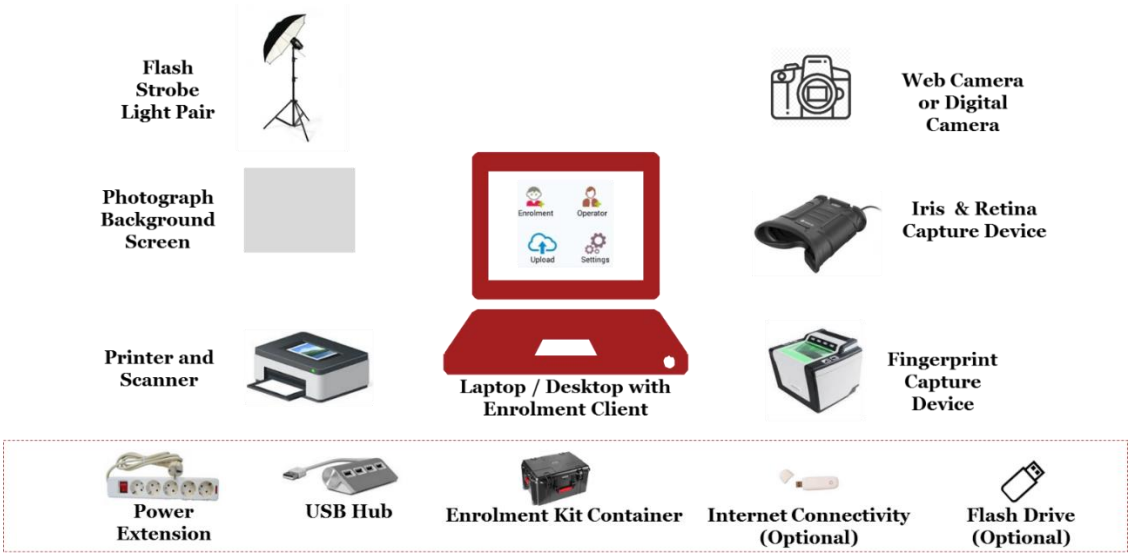


Figure 9: Proposed Enrolment Kit at the Enrolment Center

4.2.3. Identity Management System (IDMS)

IDMS module will be responsible for processing of enrolment packets through the phases of acceptance, validation, processing and dispatch of UIN.

4.2.3.1. Key Functionalities of IDMS

The key functionalities of the application are provided below:

- **Secure synchronization –** This IDMS would have capability to send response back to the enrolment software upon successful receipt of the packet in a secure fashion from the client.
- **Enrolment packet verification** – This function will perform antivirus checks to ensure packet is not corrupted during transmission.
- **PKI Decryption –** PKI decryption will be done by private keys managed by a HSM device.
- **Transaction Management** – The complete transaction lifecycle of a packet from decryption to the ID generation is broken down into various stages having relevant checkpoints assigned to each stage maintained both in memory and persistent database. This enables transaction processing restart at the point of failure rather than a rollback to the 1st stage.
- **Structural Validation and Standardization** – The module is responsible for performing structural change checks of the packets including tampering and corruption. This includes migration of data from packet into multiple standardised data stores for subsequent processing. Please refer to Annexure-V: Structural Validations for more details.

- **Interface with CNIE and EC** – For residents above 18 years, the demographic details and the photograph of the resident given at the time of enrolment will be matched against same details obtained from CNIE through APIs. For residents below 5 years (in areas where electronic civil registration is operational), the demographic data captured during enrolment will be verified from Civil Registration through APIs.
- **Demographic De-Duplication –** Data fed in the data stores from the packet is then processed in a de-duplication engine with rules checking the duplication of demographic details of the packet with other successfully processed packets stored in DS.
- **Interface with ABIS for Biometric De-duplication** – Post demographic de-duplication activity, biometric information is shared with ABIS management layer through this interface.
- **Unique Number Generation** – IDMS will access the common NIU Generator currently deployed for allocating UINs in the Civil Registration System. The UINs to be allocated in the RNP system would be sourced from the common repository of NIU generator, which will be used by Civil Registration System as well as RNP System. Thus, every successful transaction confirmed from all stages will be assigned a UIN number from the NIU Generator.
- **Event Generation** – All the participating modules of transaction processing will generate events based on the defined business rules. These alerts will be fed in a data store and will be accessed by the Business Intelligence module to generate insights supporting decision making on operational effectiveness.
- **Sequential Event Driven Flow –** The transaction processing will be done through well-defined stages running in sequence as well as in parallel based on the complexity assigned to the transaction.
- **ID dispatch** – This module will have the feature to dispatch the successfully generated UIN to the respective resident through email/SMS and physical delivery as per the defined procedure.
- **Enrolment Reporting** – MIS module will generate reports detailing the operations conducted at each enrolment center against the defined KPIs of enrolment center admin and enrolment center officer.
- **Identity Repository –** For the enrolment packets for which UIN has been allocated, the IDMS would update the identity repository that will contain UIN, Demographic Data, Biometric Templates, etc., which may be used for the purpose of delivery of authentication and e-KYC services. The application will also have the feature to update identity repository whenever an update request is received for changes in demographic/biometric data.

4.2.3.2. Technical Features Overview of IDMS

The technical features of the Identity Management System is depicted in the figure given below:

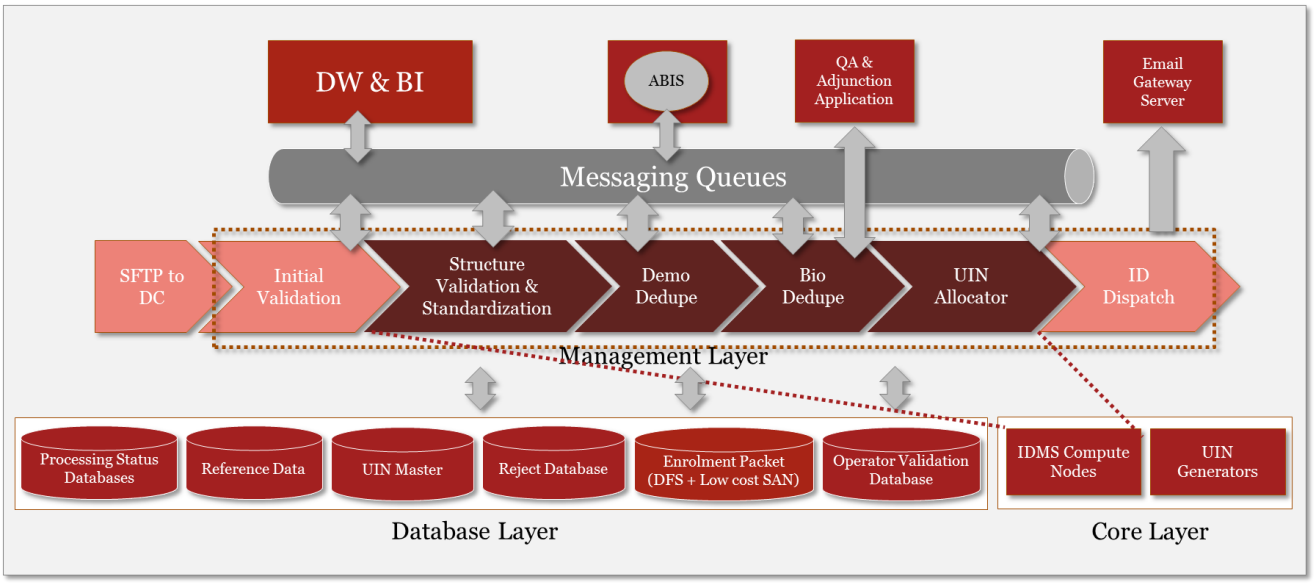


Figure 10: High level diagram depicting technical features of IDMS

In the figure given above, the key components of IDMS can be seen. The details of these components are provided below:

- **Sequential Staged Event Driven (SEDA) Components:** Packet received through Secure File Transfer Protocol (SFTP) at the RNP-DS would be passed through multiple stages in a sequential fashion.
- **Three Layers of Architecture:** The IDMS is implemented in 3 layers:
  - **Management layer** is implemented through Batch oriented middleware that orchestrates processing of enrolment data captured in packets
  - **Core layer** consisting of the implementation logic for processing the data in packets, and
  - **Database layer** to store the initial data, intermediate data and processed data. A set of messaging queues would support these layers to connect each stage in a loosely coupled fashion.
- **Event publishing and consumption:** Events generated during the journey of the packet data through the SEDA pipeline are published to message queues and consumed by consumers such as BI.
- **Integrations through Messaging & APIs:** All integrations between different layers, ABIS, Email/SMS gateway would be through Messaging and RESTful API's.
- **Integration with NIU Generator:** For UIN generation, IDMS will interface with common NIU generator. The NIU generator would be leveraged not only for RNP system but also for the proposed Electronic Civil Registry as well. Numbers that are allotted to RNP and ECR would be flagged separately once they are allotted to any of the systems.
- **Software Development Strategy:** Bespoke development on Open Source OTS technology Platform.

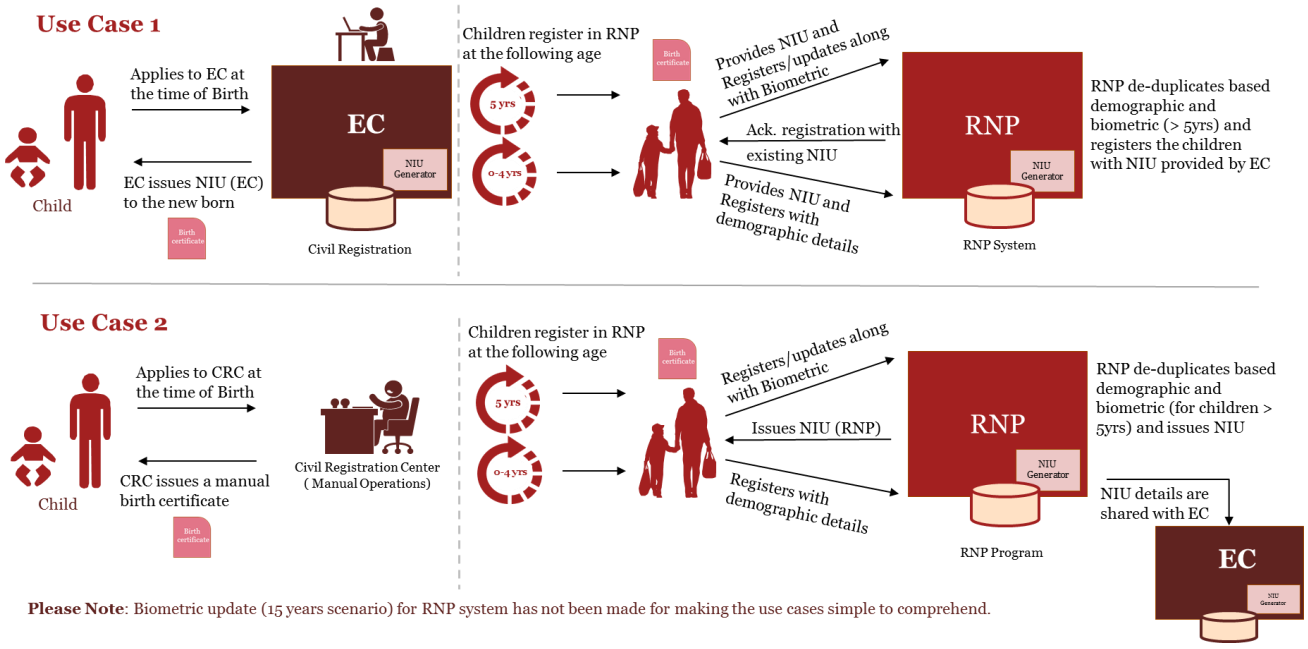
4.2.3.3. Integration of NIU Generator with IDMS and Civil Registration

Ministry of Interior is rolling out a Civil Register Program that shall provide birth certificate to children and will issue a NIU number (EC) based on demographic de-duplication. Ministry wants to retain this number for the lifetime. Separately, the Ministry is also implementing RNP Program (foundational ID program), which shall also issue a NIU post de-duplication of demographic and biometric information of the resident. The Ministry wishes to ensure that numbers issued by NIU (EC) to the children are retained for lifetime and are used by the RNP Program as well. The brief objectives of the Civil Registration and RNP Program are given below:

- Civil Registration shall enrol children at an early age (ideally after birth) and shall issue a UIN (EC) which shall remain valid for the lifetime

- Pilot project for the civil registration program has been launched in Rabat and shall be subsequently scaled to other regions in the coming years
- RNP has been conceptualized as a foundational program that shall collect demographic and biometric details of residents and issue a 10-digit UIN number after de-duplication. This UIN number shall be used by various government and private sector organizations to provide services
- Civil Registration System has an existing NIU generator and has the following features:
    - NIU Generator (EC) shall be loosely coupled with the demographic de-duplication engine using an API to ensure interoperability
    - NIU Generator will allow registration of the entire population and shall also adapt to cover the evolving population of Morocco. This means that the NIU Generator and NIU Format must ensure the enrollment of the existing population as well as children born in future.
    - UIN shall be a 10 digit random number and which shall have the last digit reserved as the check sum digit. The check sum digit shall be produced by Verhoeff algorithm
    - NIU generator works on six Business Rules
        - Currently the first digits [one (1) series] is reserved for future expansion and shall not be allocated
        - First 5 digits are different from the last 5 digits
        - First 5 digits are different to the last 5 digits reversed
        - UIN is not an ascending or descending cyclic figure
        - UIN is different from the repetition of the first two digits 5 times
        - UIN does not contain three even adjacent digits

On the basis of above mentioned requirements, two major use cases emerge. These use cases are described using the diagram given below:



Please Note: Biometric update (15 years scenario) for RNP system has not been made for making the use cases simple to comprehend.

Figure 11: Use Case of Enrolment

The use cases shown in the figure given above, are described below:

1. **Use Case-I (For areas where Electronic Civil Registration is operational):** A new born child, in these areas, will get registered through Electronic Civil Registration. On registration, Civil Registration will allot a UIN number to the child based on demographic deduplication. After birth registration, the child will visit CSC for enrolment under RNP program. For RNP registration, two scenarios are explained below:
    - **Child is less than 5 years:** The RNP system will de-duplicate using the demographic details of the child and also validate demographic data from Civil Registration through APIs. RNP system will flag the database and allot the UIN number to the child. This UIN number will be same as that allotted by the Civil Registration System. After allocation of same UIN, the RNP system will notify the allocation to Civil Registration System for record.
    - **Child is above 5 years:** RNP system will de-duplicate using the biometric details of the child and also validate demographic data from Civil Registration through APIs. RNP system will flag the database and allot the UIN number to the child. This UIN number will be same as that allotted by the Civil Registration System. After allocation of same UIN, the RNP system will notify the allocation to Civil Registration System for record.
2. **Use Case-II (For areas where manual Civil Registration is operational):** A new born child, in these areas will get registered through manual Civil Registration, i.e., the child will not have a UIN number but would have a manually issued birth certificate. After birth registration, the child will visit CSC for enrolment under RNP program. For RNP registration, two scenarios are explained below:
    - **Child is less than 5 years:** The child would provide the demographic details and manual birth registration number. RNP system will de-duplicate using the demographic details of child. RNP system will request the NIU generator for allotment of UIN number to the child. After allocation of UIN, the RNP system will notify the allocation to Civil Registration System for record.
    - **Child is above 5 years: The** child would provide the demographic details, biometric details and manual birth registration number. RNP system will de-duplicate using the biometric details of child. RNP system will request the NIU generator for allotment of UIN number to the child. After allocation of UIN, the RNP system will notify the allocation to Civil Registration System for record.

To enable the above functionalities, a common NIU generator outside RNP system as well as Civil Registration System will be implemented. NIU generator will utilize a common gallery of random numbers for allocation of UIN to both the systems. A diagrammatic representation of the above process is shown in the figure given below:

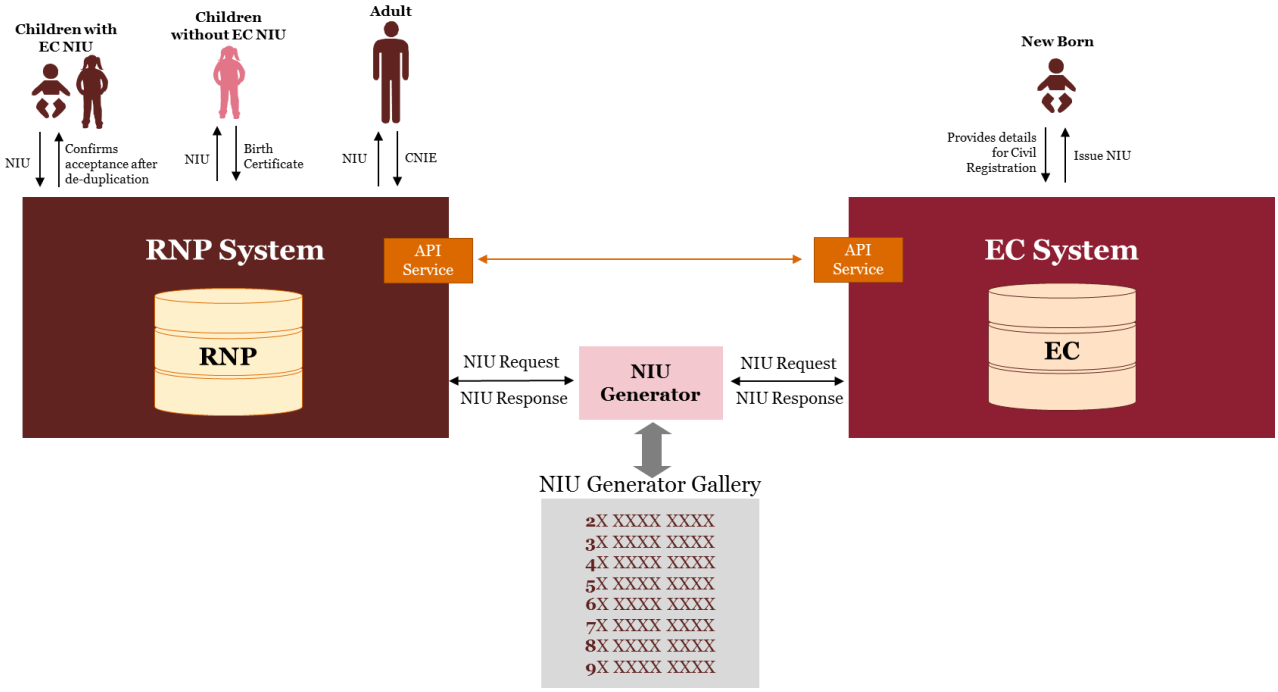


Figure 12: NIU Generator for EC and RNP Program

The requirements of the above mentioned solutions are as follows:

- Both EC and RNP system follow the same numbering format and structure for the UIN
- Systems shall exchange information regarding UINs generated
- Both system are envisaged to be de-duplicated in nature through de-duplication methodology
- Both system shall keep a track of the UINs issued by both systems to ensure that the NIUs issued to the residents / children are unique and are retained for lifetime
- All individuals shall first get birth certificate / UIN (for new born) from the Civil Registration System
- First digit for the UIN shall be reserved for future expansion
- All residents shall enrol in the RNP system. RNP system shall perform biometric de-duplication and shall issue UIN (RNP) which shall be used by other Government and Private Sector Schemes and Programs
- The child shall be accompanied by a parent(s) at the time of enrolment in the RNP program and the parent(s) UIN and their biometric details shall be collected and verified during enrolment

A common NIU generator would be implemented for both EC and RNP system and there shall be no distinction between the UINs generated from EC and RNP. However, exchange of UIN details for verification issued shall be dependent on APIs and their uptime. This mechanism would require high number of cross checks between RNP and EC issued UINs leading to higher computation for complex searches. A key factor would be high level of governance and management requirement because there will a common shared UIN repository. There is a possibility of duplicates in the EC system as it will be based on demographic de-duplication and there shall be no cross pollination of UIN from RNP. This would be limited only to the children below the age group of 5 years but post 5 years biometric information shall enable de-duplication of child records.

4.2.4. Authentication Services (Authentication and KYC) Application

The authentication services application shall deliver services such as Authentication and KYC and shall be integrated with Trusted Service Providers (TSP). The application will use UIN and one or more factors (demographic, biometric, one-time pin) based matching for validating the authenticity of resident who has been asked to authenticate by a user agency.

4.2.4.1. Key Functionalities of Authentication Services Application

The key functionalities of the application are provided below:

- **Partner Credential Lookup:** During each authentication request, the authentication packet would need to pass the TSP credentials for ensuring authentication request is coming through a genuine TSP and authentication agency.
- **Device Credential Lookup:** During each authentication request, the authentication packet would need to pass the Device credentials for ensuring authentication request is coming through a genuine registered device.
- **Reporting:** Identity services software would have the capability to produce MIS reports.
- **Transaction Management and Audit Logging:** Each authentication transaction would be logged in the TSP servers and would be load balanced across a farm of server infrastructure.
- **Data Decryption:** Each encrypted packet originating from the authentication source (POS/Mobile/Web Applications) would be decrypted, once it has been received at RNP-DS.
- **Transaction Validation:** Each transaction would be validated for an active TSP and an active device using cached data of the partners and devices.
- **Privacy Validation**: The response would depend on the privacy settings of the residents (e.g. biometrics locking status), user agency authorization (limited e-KYC or full e-KYC), etc.
- **Virtual ID:** The resident will be able to use a Virtual ID number at the time of authentication instead of UIN. For more details, please refer to Annexure-VI: Use of Virtual ID in Authentication Services.
- **Demographic Matching Engine:** Demographic matching is carried out using fuzzy algorithms in case a demographic based authentication is invoked. The fuzzy match levels can be passed as a parameter by the end user.
- **Biometric matching Engine:** A biometric matching API in the biometric SDK would be invoked to check for 1:1 biometric match against the resident database containing biometric templates along with demographic data.
- **Two Factor Authentication:** The two-factor authentication will be utilized for One-Time Pin (OTP) based authentication and e-KYC service delivery.
- **Integration with SMS/Email:** The identity application is integrated with SMS / Email server to send email/SMS whenever an identity request is made. The SMS / Email would contain the status of authentication request (Success/Fail).
- **Integration with BI & Fraud:** All authentications would generate events that would be input to BI servers and Fraud Management system. For example, in case of two requests for a given UIN from one user agency providing same biometric score there is a probability of a fraud.

- **Response Generation:** All authentication requests would only return a Yes or NO response packet, while KYC requests would return a demographic information and photograph of the resident as a JSON response.

4.2.4.2. Technical features overview of Authentication Services Application

The following figure shows the Key Technical Components of this application:

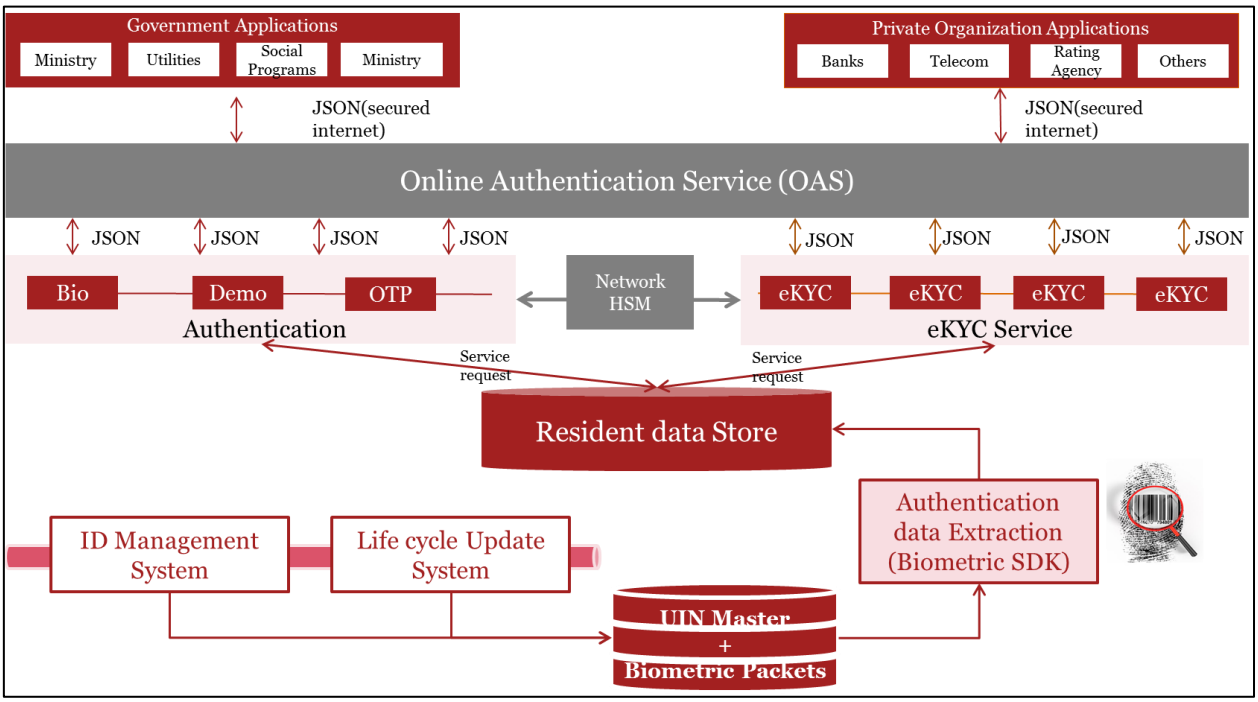


Figure 13: Identity services Technical components

- **Authentication APIs:** Authentication framework would have multiple API's exposed for authentication including demographic authentication, OTP based authentication, and biometric authentication.
- **Resident Data Store:** A resident data store would be a multi-server data partitioned server along with cached data store to contain OTP, and recently used authentication records for sub-second response.
- **Authentication Extraction severs:** Authentication extraction servers would be responsible for building the single and multi-mode biometric templates from raw biometric images. Once the templates are created, the raw images can be removed and only maintained as encrypted packet in the archive filesystem.
- **Software Development Strategy:** Bespoke Development on Open Source OTS technology Platform

4.2.5. Automated Biometric Identification System (ABIS)

This module carries out the biometric quality management and biometric de-duplication for the packets shared by IDMS.

4.2.5.1. Key Functionalities of ABIS

The key functionalities of the application are provided below:

- **System Configuration and Management –** Configuration console would be available for defining business rules
- **User Management –** Ability to manage user lifecycle authorized to access the ABIS module
- **Reporting –** Status reporting would be done for the enrolment packets processed with sufficient details on the rejection criteria
- **Transaction management –** Complete transaction lifecycle of a packet would be broken down into various stages having relevant checkpoints assigned to each stage maintained both in memory and persistent DB. The journey starts from requesting a biometric duplication in the request queue and ends at submission of a reply to response queue
- **Transaction Validation and Security –** This module would offer the feature of validating the transactions originating from IDMS and sent to ABIS for further processing. New Identity is generated under this module for referencing the package under processing. This Identity is mapped to the IDMS request through a mapping table.
- **Template Generation, Segmentation and Sequence Check –** Template generation is the process of generated biometric templates from the raw biometric images captured through enrolment software.
- **Quality Check –** The SDK provided by ABIS would perform basic quality check before the package processing is taken up by ABIS.
- **Biometric Matching Engine –** ABIS would provide a biometric matching engine to compare the generated biometric templates with the ones existing in the ABIS gallery.
- **Multi-Modal Biometric Fusion –** ABIS would have a capability to use the multimodal biometric authentication systems, which combine information from multiple modalities to arrive at a decision.
- **Biometric De-duplication (1: N) –** Biometric de-duplication would run against the gallery of biometric templates to arrive at de-duplication decision.
- **Internal Template Storage –** All the successfully de-duplicated biometric templates would be stored in the ABIS for dedupe requests of new packets.
- **Software Development Kit –** ABIS would also provide SDK for performing quality on the incoming packets.
- **Middleware Synchronization –** This functionality enables synchronization of management layers across ABIS, IDMS and Authentication to ensure seamless processing of incoming enrolment/ authentication requests.
- **ABIS Middleware –** ABIS has a response / request queue mechanism to receive messages from IDMS and allow adjudications application to subscribe for potential duplicate messages for manual adjudication.
- **Biometric Template derived from Multimodal Fusion:** The biometric template that would be used for 1: N match for a deduplication would be not based on a biometric template of a single biometric (a finger or iris) but would be a full multimodal biometric template. A multimodal biometric would be a fusion of all the biometrics, which means a single template derived after concatenation of all the individual biometric images or templates.
- **Fine tuning of ABIS for FR and FA:** ABIS would have provision to analyze and report the false acceptance and false rejection rates along with a provision to carry out detailed analysis for reasons thereof. ABIS would also have features to fine-tune thresholds and other settings for improving False Acceptance and False Rejection Rates while ensuring there is a good balance between them. In addition to the tuning of thresholds, ABIS should have the provision to utilize / add appropriate biometric algorithms

- **Manual Adjudication –** The manual adjudication module would be part of ABIS to allow quality check by operators on records that match the incoming packets biometric template. Failed biometric deduplication needs to be manually verified for their authenticity. This features will have a manual override to reject or insert the data based on the decision made over and above the results of demographic/biometric de-duplication.

4.2.5.2. Technical Overview of ABIS

The overview of the technical solution is shown in the diagram given below:

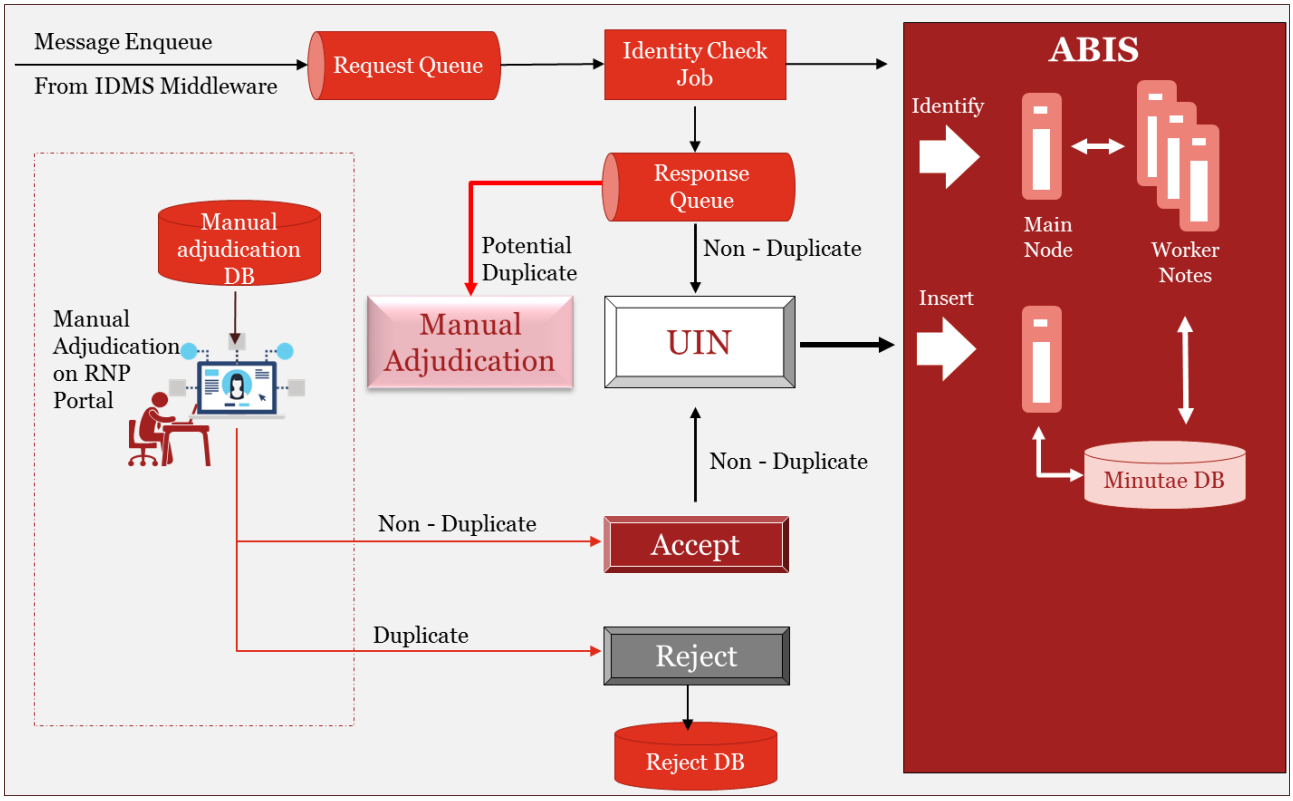


Figure 14: Technical Overview of ABIS

The figure above depicts the following main features of the ABIS:

- Insert and Identity check Programs
- ABIS management layer consisting of Request / Response queue
- Integration with manual adjudication Application.
- **Software Development Strategy** – OTS on Proprietary

4.3. Support Application Solution Components

4.3.1. RNP Portal and Mobile Application

The RNP-Portal and RNP-Mobile App would be used to access the RNP system for all OLTP transactions and retrieval of information, be it Content Management Components, Customer Relationship Management Application, Partner Management Application, Enrolment Software Management Application, Quality Check and

Adjudication Application, Pre-enrolment, UIN Status Tracking, Public and Private BI Reports/Dashboards views. **For residents and internal users (including partners), separate access would be available.**

4.3.1.1. Key Functionalities of the RNP-Portal and Mobile App

The key functionalities of the application are provided below:

- **Interface to Partner & User Management and Partner Services Overview:** RNP portal would contain catalogue for the various available partner services, including details of processes to enroll/onboard TSPs, required documentation, fees, if applicable, etc.
- **Resident Services (Pre-enrolment, UIN status, UIN Letter Download, etc.):** Resident RNP portal/Mobile App would enable residents the to check status of their UIN under processing, to download a UIN number digital card (if required in future) for printing, to submit grievance and check its status, update of certain demographic information such as mobile number.
- **Public and Internal Dashboards:** The resident portal would show dashboard from the perspectives of enrolment and identity services. These dashboards will have drill down facility to provide more details to the user, whenever necessary. The internal dashboard will be more comprehensive and may also contain the performance measures against predefined KPIs published on a periodic basis in the Business Intelligence and Analytics application. The private dashboards will be accessible by login using SSO feature.
- **Legal and Governance Framework:** The RNP portal would have details on the legal and governance framework.
- **Resources and Public Relations:** The RNP portal would have complete information on the resources and public relations.
- **Grievance Management:** The internal RNP portal would allow the CRM user to login to the CRM application using SSO and perform all call center and grievance redressal activities. Residents would be given an interface where they would be able to file grievances online.
- **Events, Notices and Circulars:** RNP portals would contain relevant public notices, events and circulars for viewing.
- **Other Application Interfaces:** The internal RNP portal would allow the application users to login into respective user applications as per their roles and credentials. For example, adjudication users would login to the adjudication application using SSO and perform all quality check activities

4.3.1.2. Key Technical features of the RNP-Portal and Mobile App

The overview of the technical solution is given below:

- Only Internal Portal would be SSO based portal with single place for different types of users to login using their UIN number along with a second factor of authentication.
- Information on resident portal would be readable by anyone (public notices, circulars etc.) or using enrolment number for tracking UIN application status or using UIN number along with OTP authentication for download of UIN letter.
- A Role based access would be available to all the users and depending on the role, the user would be able to view and access the applications available for his role on the internal portal.
- API's from different applications would be available for consumption by the web portals / mobile app.
- API's available on Mobile Apps would be exposed using the API Gateway.

- Portal Access for internal applications like CRM, Partner Management would be only available on secure lines such Secure internet, MPLS or Secured Network lines etc.
- Resident Portal would contain link to pre-enrolment application, status tracking capability for UIN application, download of UIN letter, update of certain demographic features. The resident portal would be available on the internet.
- All portals would support multilingual features.
- **Software Development Strategy** - OTS on Open Source Platform

A depiction of the Portal and Mobile App Components is displayed below.

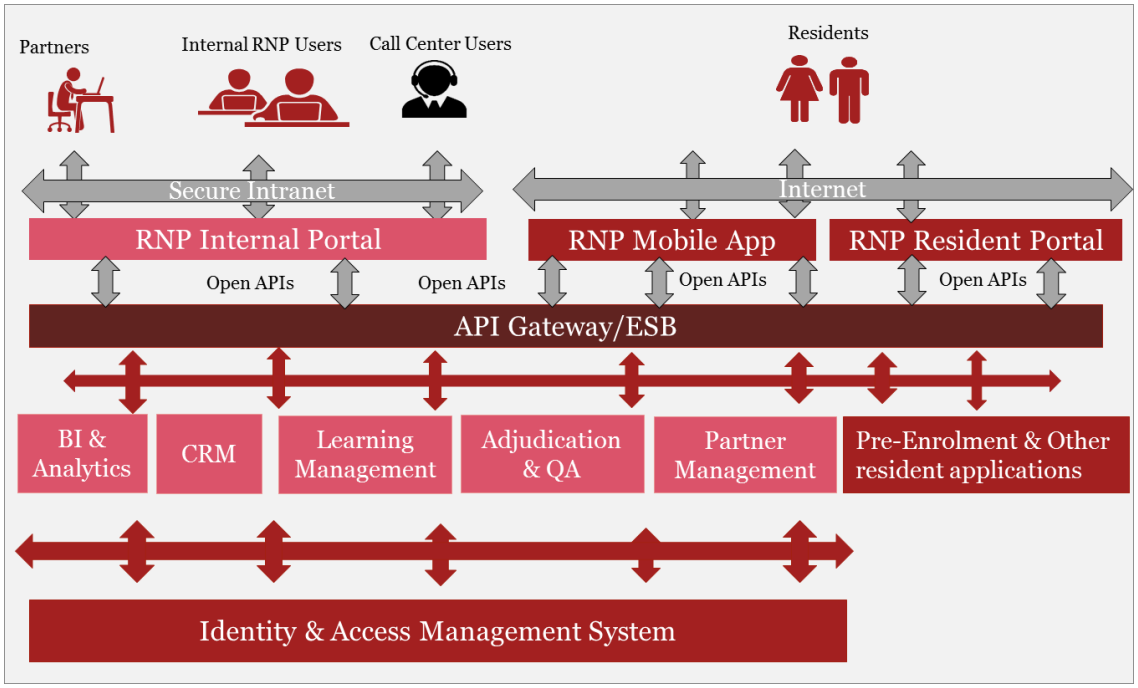


Figure 15: Portal Components

4.3.2. Business Intelligence and Data Analytics

The BI and Data Analytics component is an important building block as it would provide features/ solution to continuously improve, strengthen and secure the system from a security and performance perspective. It would also house content for public viewing.

4.3.2.1. Key Functionalities of Business Intelligence and Data Analytics

The key functionalities of the application are provided below:

- **Integration with other RNP-DS Components:** Execution of various business processes in the RNP application would generate a lot of data which would be transformed into useful insights by BI.
- **Enrolment Status Reports:** BI solution would provide enrolment status reports on a periodic basis for review to internal users.
- **Enrolment Performance Reports:** The BI Solution would provide performance of different enrolment centers, enrolment officers and overall enrolment process to continuously evaluate if there are no bottlenecks from a system, process and people perspective and take mitigation steps when needed.

- **Authentication Status Reports:** BI Solution would provide authentication status reporting on periodic basis for analysis and review by internal users.
- **Authentication Performance Reports:** BI Solution would provide authentication performance for different types of authentication carried out to point out any performance issues in any of the authentications.
- **Data Quality Management:** Data before being fed into the data warehouse would be evaluated for cleanliness and any aberrations would be filtered out by a Data Quality tool.
- **Data Warehouse:** All the data continuously generated would be available in a data warehouse. The data warehouse would be capable of storing and analyzing huge amount of structured as well as unstructured data.
- **Metadata Repository:** The data warehouse would have a metadata repository to contain business metadata.
- **ETL/Data Acquisition System:** This would include tools that would extract data from all the source systems into the warehouse. This ensure data in BI is integrated with other parts of the system to ensure data is consistent with the rest of the system.
- **Visualization System:** This is responsible for presentation of data to end users in form of rich graphical reports, dashboards, KPIs, GIS based reports, etc.
- **Integration with RNP Portal/Mobile App:** The portal and mobile application would show dashboard and many reports. For this purpose, the Business Intelligence and Analytics tool would require integration with RNP Portal / Mobile Application.
- **Public Dashboards:** Some of the aggregated statistics like Enrolment, KYC, Authentication trends would be available for public view on the RNP Portal.
- **Other Analytics:** The Business Intelligence and Analytics tool would analyze the information generated as a result of enrolment, authentication and operations.

4.3.2.2. Key Technical features of Business Intelligence and Data Analytics

The key components of the BI solution are shown in figure given below:

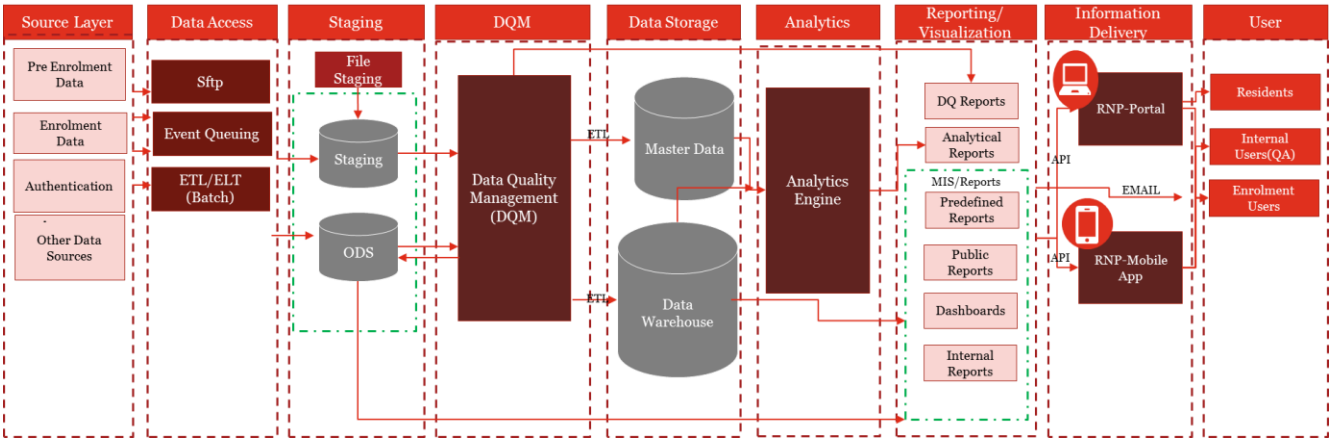


Figure 16: BI and Analytics Components

As shown in the above figure, the main components of the business intelligence system are as follows:

- Data Sources
- Data Acquisition
- Staging Layer
- Data Quality Management
- Data Storage System
- Analytics
- Reporting and Visualization
- Information Delivery Layer (Portal/ App)
- Users
- Software Development Strategy – OTS on Open Source Platform

4.3.3. Partner and Device Management

The Partner and Device management application would cater to the needs of the partner community, which includes the Trusted Service Providers and Enrolment Agencies.

4.3.3.1. Key Functionalities of the Partner and Device Management Application

The key functionalities of the application are provided below:

- **Administration and User Management of Enrolment Community:** The application would allow Administrators to setup new users as Enrolment officers by allotting them a UIN Number. This application would also allow the setup of Enrolment centers and manage the lifecycle of these centers.
- **View Statistics and KPI's for Enrolment Community:** This application would provide the capability to view statistics related to enrolment at various enrolment centers such as time taken for enrolment, no of enrolment packets that failed from an enrolment center / enrolment officer.
- **Administration and User Management of TSPs and UAs:** The application would allow administrators to setup new users as TSP/UAs along with their credentials etc. This would allow for registration of devices, services permitted (w.r.t. limited e-KYC).

- **View Statistics and KPI's for Authentication statistics:** This application would provide the capability to view statistics related to authentication Partners, such as number of authentications handled by a particular TSP.
- **Drill into individual issues:** This application would have capability to provide insights into individual performance issues of TSP or Enrolment Officers to improve their performance.

4.3.3.2. Key Technical features of the Partner and Device Management Application

The key technical features of the application are provided below:

- Application would be integrated with RNP Portal for access by administrators.
- Application would provide APIs for credentials check for TSPs during authentication and credential check during login by enrolment officer, download of pre-enrolment data.
- Application would need to provide fast access to credential data along with a high concurrency of enrollment requests or authentication/KYC requests.
- This would be a bespoke application hosted on a multi-tier architecture using a web, application and Database server. Since the Partner credentials would not change very frequently and accessed heavily we can consider caching them or storing them in the Fast Access database storing authentication information. The partner credential lookup would be exposed as an API and would be used by Authentication API's or Login API for enrolment officer.
- **Software Development Strategy -** Bespoke on Open Source Platform

4.3.4. Identity and Access Management

The function of the Identity and Access management would be to provide single sign on capability for applications such as CRM, Partner Application, Pre-Enrolment, BI, Analytics etc., along with role based access on different applications.

4.3.4.1. Key Functionalities of Identity and Access Management

The key functionalities of the application are provided below:

- **Single Sign on access:** To avoid multiple access credentials Identity and Access management would be used which will be used across the different applications of RNP Software System. A Single Sign-on (SSO) would be required to access multiple application in the RNP landscape.
- **Role Based Access:** Access to different applications from the RNP Portal would be based on Role based access where after login to portal using SSO, the ability to invoke a particular application would depend if the role is authorized to access the application.
- **Provisioning of internal and partner users:** Access and identity management would help provision users depending on their roles into different applications such as Enrolment Software Administrators, Enrolment officers, CRM Users, Partner Admins, Partner users, BI Admins, Database admins etc. Administrator can be allowed access on the basis of multi-factor authentication devices

4.3.4.2. Key Technical Features of Identity and Access Management

The key technical features of the application are provided below:

- **Single Source of provisioning to Application:** This system would allow a single point from where the lifecycle of an internal RNP user or a partner user would be managed.
- **Role creation:** The identity and access management would allow creation of different roles such as CRM User, CRM Admin, Adjudication User etc.
- **Access policies to RNP Systems:** Depending on the role assigned to the user access policies would be created.
- **Identity Store:** The identity store would contain the user details and would be essentially a directory server based on LDAP.
- **IT resources:** The Identity management system would contain the details of all the systems to whom users are to be provisioned.
- **Software Development Strategy** – OTS on Open Source Platform/COTS

4.3.5. Customer Relationship Management (CRM)

The Customer Relationship Management (CRM) Software would allow residents and ecosystem partners to log queries and grievances. The CRM Solution shall be used to manage all customer interactions with RNP and also act as a repository to be used for analysis of feedback and grievances. The key functionalities of the application are provided below:

- **Single point of customer experience:** The system would be designed in such a way to give a single view of all the interactions with the resident for at least the given time period.
- **Customer Feedback:** The CRM Solution would be capable of taking caller feedback on SMS, IVRS, RNP-Portal, and Mobile App going forward or through a KIOSK in the CSC. CRM shall be capable of generating SMS in respect of a sample of callers (such as 5th caller who spoke to agent) to get a feedback about quality of response and satisfaction level or for landline users caller satisfaction feedback can be taken over IVRS.
- **Integration with RNP:** CRM would be integrated with other systems using an API based approach where API's of other systems like BI would be available for consumption or API's exposed by CRM would be available for consumption by BI/Analytics software to derive insights and trends of the resident behavior.
- **Multilingual Support:** CRM would be capable of multilingual support in French and Arabic language.
- **Customer Analysis:** CRM would help in analysis of service to the resident by aggregating of statistics related to each resident experience while enrolment.
- **Software Development Strategy** – OTS on Open Source Platform/COTS

4.3.6. Document Management System

The function of the Document Management Software is to handle file sharing, creation, manipulation, and storage. This applies to any document that RNP deals with either on the internet or intranet. The key features of the application are provided below:

- Storage of documents of residents submitted as PoI and PoA
- Would be integrated with Pre-Enrolment and Enrolment Software
- Documents would be indexed using UIN, EIN and Pre-enrolment acknowledgement numbers
- **Software Development Strategy** – OTS on Open Source Platform/COTS

4.3.7. Knowledge Management System

The Knowledge Management is an integral aspect of any large scale enterprise projects. A dedicated portal will be established and maintained which shall be the shared repository of information and knowledge. From knowledge perspective, the software would cover, but not limited to, the documents generated by the vendor(s) and RNP authority. From learning perspective, the software would handle training and knowledge transfer of various stakeholders. The KMS system will remain an integral part of the portal where the registered users opt for different training programs and undergo training online using audio/video, online presentations. FAQs, Quiz, functional flow documents. The training records as well as training requirements for users would be maintained by the KMS. The key features of the application are provided below:

- **Training Need Analysis:** The KMS must have the capability to capture training needs of different types of users for analysis and development of new trainings
- **Training Monitoring:** The KMS should have the capability to monitor trainings completed by different users and sending reminders to users for completing the registered trainings especially mandatory trainings.
- **Training Feedback Mechanism:** The KMS should have the capability to capture feedback of trainings from Trainees for continuous improvements in trainings.
- **Training Schedules:** The KMS should have capability to publish a detailed training schedule.
- **Audio Visual Trainings:** The KMS is also required to provide Audio-Visual Trainings to the users for assistance in operating/navigating through different applications. The modules/section wise training material, especially in form of Audio-Visual content or animation, apart from PDF version, have to be uploaded in each module/sub-module/section of the RNP-Portal which can be played at any given point of time through the browser. The users should find it easy to understand the process and functionality better by seeing the audio-visual training content for that specific module/sub-module/section and work accordingly as required.
- **Training Navigational Capabilities:** These Audio Visual clips will have the functionality to start, stop, pause, back and forward options, so that user can play the training content as per his own free will and requirement. All these specific module/sub-module/section wise audio-visual training content should be integrated to form a complete training of the Portal, and uploaded on the portal for free access, download and ready reference.
- **Online Help/Reference with Search option** - It is also proposed that the training contents and user manuals will be made available to users in downloadable (PDF) format so that the users may refer/download it for their own personal reference as and when needed.
- **Language Support:** Trainings would be available in all the official supported languages in Morocco.
- **Software Development Strategy –** COTS/Open Source OTS

4.3.8. Fraud Management

The function of the fraud detection application would be to detect/prevent different types of frauds at an individual as well as organization level. The key features of the application are provided below:

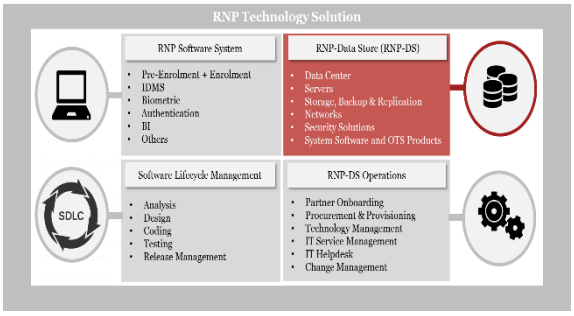
- **Detect different types of Frauds:** It is important for the RNP system to create a fraud detection module that is able to detect and minimize frauds. A few examples of fraud are given below:
    - Misrepresenting information
    - Multiple enrolment by the same resident

  - Creating invalid registrations of people who don't exist
  - Identity theft by authenticating as someone else
  - One or more of the above, without the knowledge or understanding by the resident
- **Heterogeneous system of fraud:** This application would use a combination of system based approach plus manual investigation, inspection and learning.
- **Use of Logs and audit trails:** The fraud system would be using the audit trails at the different usage points such as Enrolment Software, TSPs, IDMS etc., which are aggregated in the Data Warehouse for fraud analysis.
- **Business Rules for Fraud Engine (FE):** The fraud engine would use algorithms for fraud detection.
- **Manual Review:** A case of fraud detected by the algorithm would need to be manually inspected and then acted upon by an automatic /manual action engine.
- **Flexible Interfaces (FI):** The FI should also have a highly standardized and flexible interface that allows new algorithms
- **Software Development Strategy –** OTS on Open Source Platform

5. RNP Data Store

This sections provides details of the proposed RNP- Data Store component of the Technology Solution of the RNP. This section has been divided into following eight sub-sections:

1. RNP Data Store Reference Model (sub-section 5.1)
2. Components of Technology Platform (sub-section 5.2)
3. Design of Data Store using Cell Architecture (sub-section 5.3 and 5.4)
4. Server Components (sub-section 5.5)
5. Database (sub-section 5.6)
6. Storage and Backup Components (sub-section 5.7)
7. Network Infrastructure (sub-section 5.8)
8. Security Components (sub-section 5.9)



5.1. RNP Data Store Reference Model

The figure below represents the RNP-DS Reference model depicting the key layers that make up the RNP-Data Store covering people, processes and technologies. This section provides a brief description of each layer as follows:

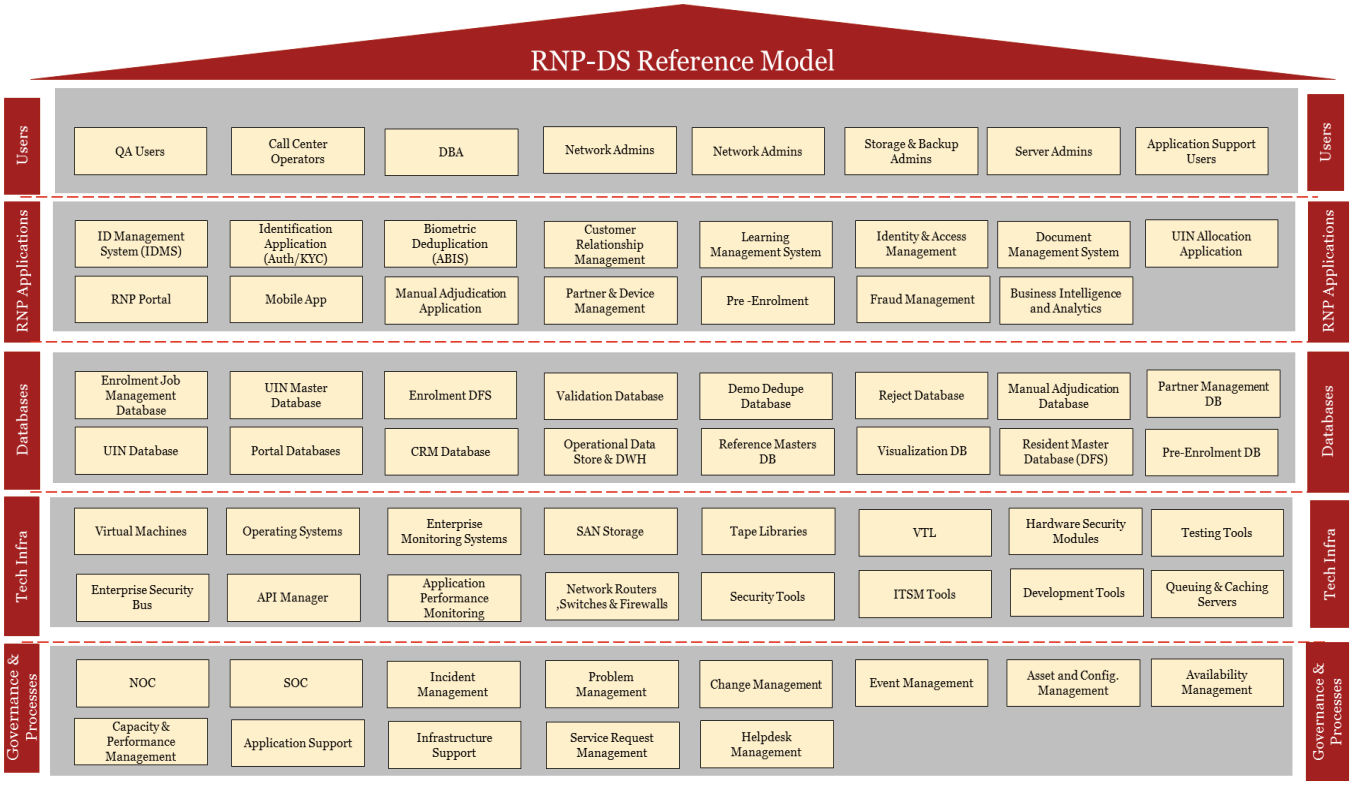


Figure 17: RNP DS Reference Model

The above reference model contains 5 layers that are described below:

- **People's Layer:** This layer comprise the users that interact with the RNP-DS, infrastructure support admins, call center & IT helpdesk operators, Application support Admins. There would be a mix of L1, L2 & L3 level people in each of these categories as per ITIL framework.
- **Application Layer:** This layer comprise the applications, i.e., RNP software systems
- **Database:** This layer represents the storage of information generated by the RNP software systems
- **Technology Infrastructure:** This layer represents the technology infrastructure of the RNP system i.e. RNP Data Store
- **Governance and Process Layer:** This layer comprise the governance, processes, and services.

5.2. Software Components of RNP-Data Store

In addition to the software applications defined in the previous section, the following software applications will also be utilized.

Technology Component	*Brief Description*	*Recommendation (COTS/Open Source Product)*
Integration Components		
Messaging Platform-Publish/Subscribe Queues	Messaging Queues for lose coupling between application components.	Open Source Product with Enterprise Support
Batch Processing	Batch processing framework for running SEDA pipeline	Open Source Batch Processing framework
Enterprise Service Bus	Enterprise service bus for application integration	COTS/Open source product with enterprise support
API Gateway	API gateway for API consumption by external and internal systems	COTS/Open Source with enterprise support
Portal Components		
Application Container	Application server	Open Source Application Server with enterprise support
UI/Portal etc.	Portal Server	Open source portal Server with enterprise support
Web Servers	Web Servers to run static web contents	Open Source Product with Enterprise Support
Distributed Caching	Caching of static data	COTS/Open source
Business Workflow and Business Rules Components		

Technology Component	*Brief Description*	*Recommendation (COTS/Open Source Product)*
BPM/Work Flow tools	BPM /Workflow management	COTS/Open Source.
Business Rules Engine	Business rules store	COTS/Open Source
Communication Components		
Email Server	Email Solution for sending and receiving mails to both internal and external users	Open Source Product with Enterprise Support
SMS Gateway	Software for Sending SMS alerts	Popular SMS Gateway software.
Data Components		
RDBMS	Relational Database management systems for storing structured data.	Open Source RDBMS with enterprise support
Large Scale random access storage	Big Data Platform to store unstructured data for Biometrics.	Open source BIG data Platform with enterprise support
Small Scale Random access distributed	NoSQL Distributed database for fast access to sub –second type of data retrieval for authentication purpose	Open Source NoSQL Database with enterprise support
System Software Components		
Client Operating System	Operating systems for running the Enrolment Software	COTS
Server Operating System	Operating system for the different servers	Open Source Product with Enterprise Support
Other Software Components		
Indexing and Key-Value Search	Search Engine for Textual Matches	Open Source Product with Enterprise Support
Encryption/Decryption/PKI	API's/Frameworks for Encryption	Open Standards based.
Software Development Life Cycle Management Components		
Testing Tools	Tools for different kinds of testing – Regression, performance, mobile , security etc.	COTS

Technology Component	*Brief Description*	*Recommendation (COTS/Open Source Product)*
Data Store Operations Components		
IT Service Management Tools	Tools for operational processes such as incident management, problem management and other components	COTS
ESM and Application Performance Management	Enterprise Monitoring of Applications and IT infrastructure from Performance , Availability and Security perspective	COTS

5.3. Design of Data Store using Cell Architecture

5.3.1. Components of Cell Architecture

The entire infrastructure is envisaged across two categories from sizing perspective - Cell and Non-cell. This is done for ease of management and procurement of infrastructure with respect to the roll-out plan. With increase in number of users and load, there would be requirement of additional infrastructure. The infrastructure set that would cater to the additional requirement on a regular basis, as per the roll-out plan is projected as a cell unit.

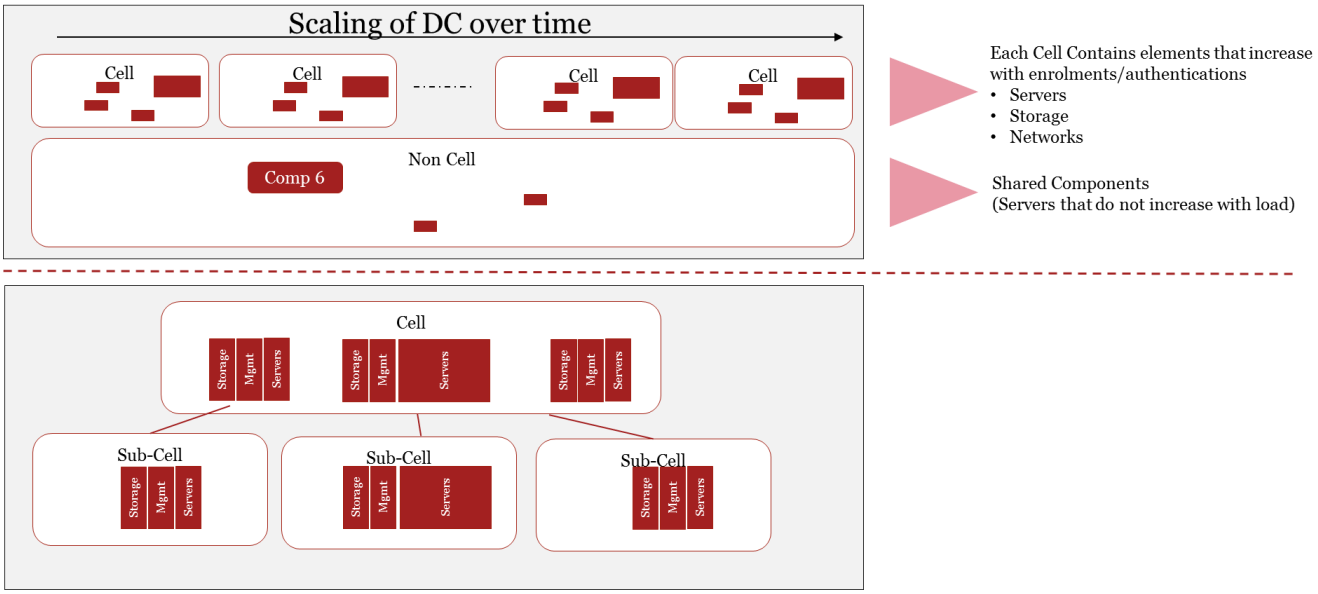


Figure 18: Components of Cell Architecture

The details of the cell and non-cell units are described below:

- A cell is a unit of "Procurement" to handle the needs of incremental for a fixed amount of population progressing in a linear fashion for meeting the demand of enrolments. Each cell can be considered as a container of sub cells with each sub cell belonging to a different functional unit in the larger system (ABIS, Enrolment, Authentication etc.). Cells are designed to smoothen the procurement process and make it more predictable in terms of hardware sizes and costs. A cell consists of elements viz. servers, storage,

network components, which are to be increased with the increase in number of users and the load on the system.

- A non-cell unit will consist of all the shared elements that keep on performing their respective functions and would not increase with load.

The benefits of such an architecture are:

- **Modularity and flexibility**: The data center would be modular in nature and each and every cell would be independent from each other so that in future if any cell component would be required to be modified and changed, there would be no lock-in in terms of technology or license. Also, the architecture is flexible to fit infrastructure components of customer choice.
- **Standard Infrastructure**: Parameters such as performance, bandwidth, through-put, protocols etc., can be standardized for each and every cell and makes the performance predictable as per each cell.
- **Ease of Procurement**: It's not necessary to buy all at one time. The deployment can start in phases as per the roll out plan, with the system initiating the roll out even with a single cell architecture.

The components of a cell and non-cell architecture are as follows:

Cell Infrastructure	Non-Cell Infrastructure
• Enrollment Servers • Authentication Servers • Biometric Servers • DFS Storage • Enrolment ODS Storage	• Intranet Servers • Core Applications Server • Dev & Test Servers • FTP Storage • BI Storage • ID Vault • BI -ODS • Portal Storage

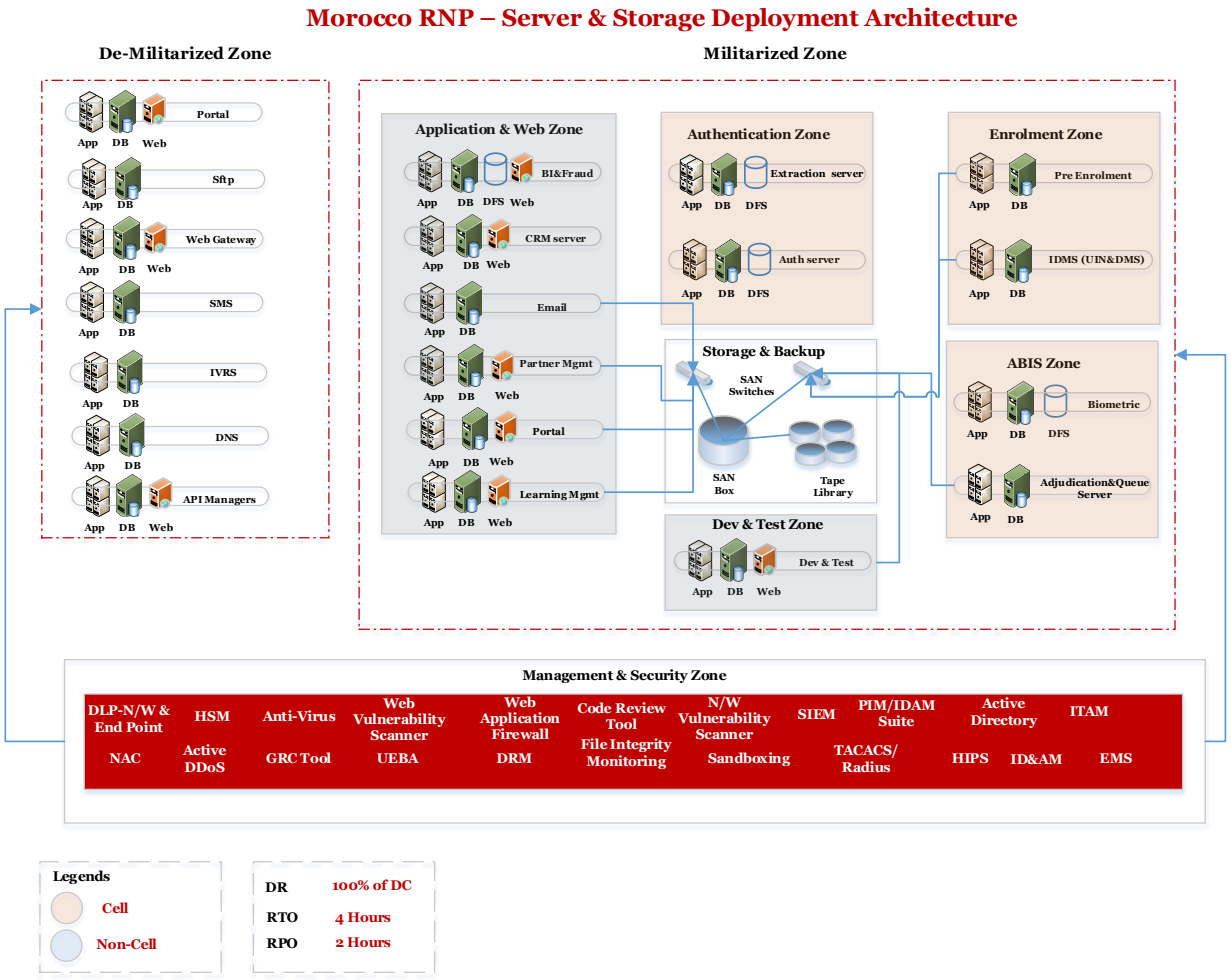
Depiction of the cell and non-cell infrastructure components is provided in the subsequent section of deployment architecture and server reference model.

5.4. Overview of Data Center Deployment Architecture

The Deployment Architecture as shown above at the proposed Data Centre has been divided into the following zones:

1. Militarized Zone (sub-section 5.4.1)
2. De- Militarized Zone (sub-section 5.4.2)
3. Management and Security Zone (sub-section 5.4.3)

The deployment architecture of the RNP-DS is provided in the diagram given below:



A brief description of different zones is given in the section below:

5.4.1. Militarized Zone (MZ)

The MZ has core application servers and database servers that are not public facing and are generally accessed by authorized officials through trusted and secured network. The MZ in the deployment architecture has been categorized into cell and non-cell, which is explained in Section 5.3.1 of the document. The Cell and Non-Cell has further been categorized into following zones:-

5.4.1.1. Cell

The details of the cells within MZ is provided below:

- **Enrolment Zone** - This shall consist of Pre-Enrolment and IDMS servers that are part of the enrollment core application and database servers. The pre-enrolment would require citizen to provide required credentials/ID proofs. This would be followed by enrolment at IDMS that requires capturing of demographic and biometric details along with photograph taken from a good quality camera. These details are then decrypted and validated and also cross checked with data provided by CNIE and stored in DMS server. This data then undergoes both demographic de-duplication and biometric de-duplication (ABIS Zone). If the records are found to be unique, the UIN Generator then generates the UIN number, which is informed to the citizen through SMS and E-mail. After generation of UIN number it is further passed to the print server for Printing of UIN letter. All servers in Enrolment Zone are connected to the SAN switches for data storage and retrieval.
- **ABIS Zone –** ABIS would be placed in this zone and would be responsible for Biometric de-duplication including manual adjudication servers in case of similar biometric matches. ABIS servers are connected to DFS storage as it requires matching of biometric of citizen with the existing biometric records.
- **Authentication Zon -** This zone accommodates all the Authentication servers, its core application and database servers. All authentication requests coming from Government Departments and other authorized authentication agencies are handled in this zone. This zone has Extraction server and Authentication server which are connected to DFS storage for matching and data retrieval authentication purposes.

5.4.1.2. Non-Cell

The details of the non-cells within MZ is provided below:

- **Application and Web zone –** This zone consists of core application servers, database servers and webservers for various activities and services viz. BI & Fraud analytics, Portal management, CRM, Partner Management, Knowledge Management and Email.
- **Development and Test Zone –** This zone consists of application and database servers of the application development and testing team. This zone has limited and authorized access to the application development team only. Application patch development, testing and UAT is performed in this zone and the patch is then pushed in the production or live environment.

5.4.2. De-Militarized Zone (DMZ)

This zone consists of application servers, database servers and web servers that are external facing and are accessed by public through untrusted public network or Internet. This zone has public facing portal for Pre-Enrolment, Grievance redressal, SMS servers, API Gateway, DNS servers, IVRS servers and SFTP servers.

5.4.3. Management and Security Zone (MSZ)

MSZ has application servers and database servers and tools that are responsible for management of servers placed in MZ and DMZ. This zone consists of following application and database servers, viz. ID&AM, EMS, etc. All the Security servers such as Incident and Access Management, SIEM, NAC and more are placed in the security zone. This zone is responsible for overall security of the Data Centers.

The Disaster Recovery Site would be 100% (or 75%) or replica of the Primary Site. The critical services that shall work from both sites on active-active mode are as follows:

- Pre-Enrolment Service
- Public Portal
- Authentication Services

5.5. Server Components

5.5.1. Server Reference Model

The figure given below represents illustrative server reference model for RNP-DS.

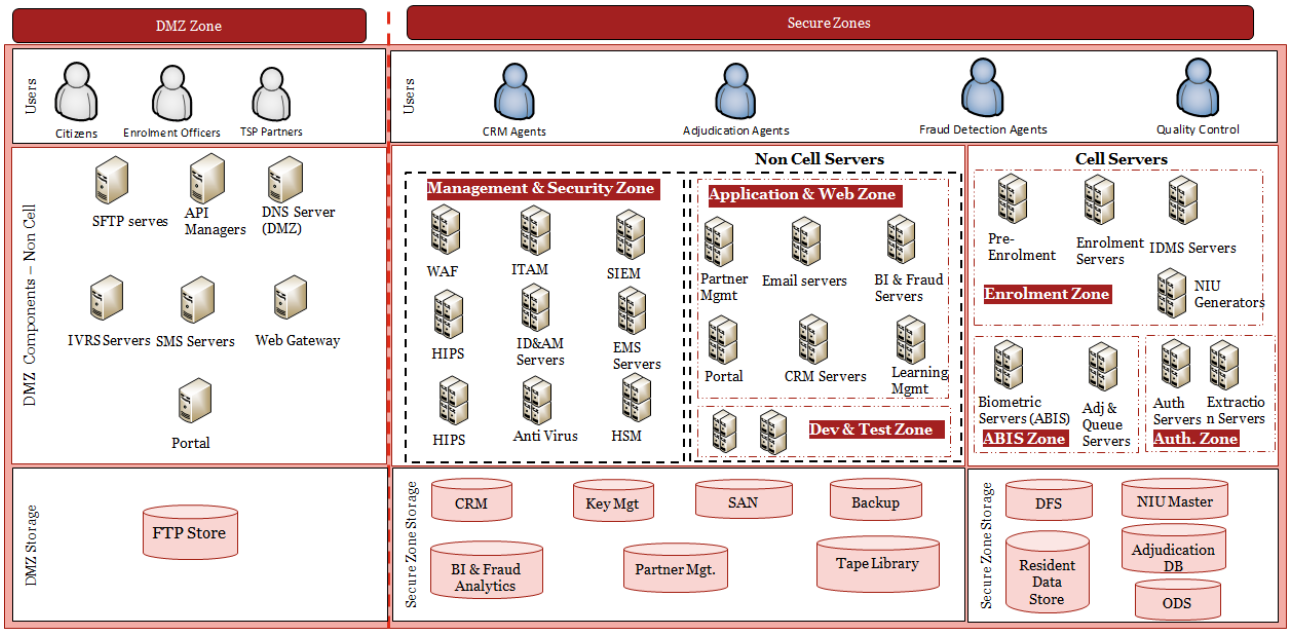


Figure 19 - Server Reference Model - RNP Technology Platform

The servers have been deployed in the above architecture as per the network zone defined and taking into consideration the security requirements. At a high level, there are two zones defined: DMZ and MZ. De-militarized zone or DMZ consists primarily of servers that would be interacting with the external world which would include:

- **Web servers** for hosting the web content of the application,
- **External DNS,** which would act as the authoritative DNS and would host the zone file for domain name to IP address resolution,
- **API servers,** which would host the API's that would be used for real time data transfer and also as an added security layer of not exposing the application,
- **Antivirus servers,** which would receive updates of the latest signature from the internet,
- **SFTP servers** for the file transfer and IVRS servers for call center services

In the next zone, the militarized zone (secure zone) has been segregated into cell and non-cell servers as defined in the diagram above.

5.5.2. Server Types

There are two types of form factors that have been considered - Rack servers and Blade servers. For both form factors, servers should be of enterprise class level. The usage of these servers is described below:

- **Rack Servers**: This has been deployed as part of DFS for hosting the biometric application. DFS works on a shared nothing architecture and rack servers are a perfect fit for the solution. These servers are complete servers with no shared components and offer sufficient room for hardware expansion.

Moreover, the space and power requirements are pretty low and now days with Intel improving the density of cores per processor, each node can hold up till 56 cores with Intel 8176 processor having 28 cores per processor. Additionally, there is sufficient slot for DAS storage, which is a must for the slave nodes where large amount of storage is a requirement.

- **Blade Servers:** This has been deployed and recommended for non-DFS stack. Blade servers as compared with rack, follows a shared architecture with 14-16 blades housed in a chassis having common power and IO (Input-Output) modules. Each blade in itself contains very few (typically 2) DAS slots and hence not a good case for DFS. Hence, they are used in non-DFS architecture with connectivity through SAN storage having block level data.

The important aspects of the server are mentioned below:

- There should be redundancies within each type of server for processor, memory, network, power and cooling components
- The servers should have some high resiliency and easy replace ability
- All servers with SAN connectivity should have HBA cards rack server.
- Servers should support hot pluggable hard disks
- The server should support virtualization and a software defined datacenter network infrastructure
- All the DFS Data nodes & DFS name nodes are connected on Rack servers to ensure performance for write & read
- Storage management servers are available based on the cell growth
- All the DFS data nodes should get best throughput
- Backup agents for DFS Data nodes are included as part of cell
- Each of the rack servers should be connected to IP KVM for management purpose
- All rack servers should be connected to L3 Access switches to ensure high availability & load balancing
- All the blade servers should have server monitoring agent to provide health & performance of the cell
- Every rack should be provided with switches & monitored PDU to ensure the PUE calculation & monitoring
- Each of the PDU also get integrated with EMS tool to get the end to end data center PUE
- Servers should support all leading enterprise level Operating Systems viz. Windows / Linux etc.

The sizing will be based upon the following principles:

- **High Availability**: All critical applications should and must be deployed in high availability with either of application level or OS level clustering solution so that if one goes down, the other node can pick up the task and complete the job taken by the primary node. Moreover, it is easier to do upgrades and patch deployments that can be done on a node by node basis and eliminate downtimes.
- **Scalability**: There are two kinds of scalability models that are available: Scale up and Scale out. Scale up is more prevalent in case of stateful applications or in legacy applications, which do not have the capability to work on a stateless basis. Moreover, with scale up, the hot add available in most of the hypervisors but there is no option of Hot subtract or reducing the configuration after the need has been met. This leads to wastage of resources. Therefore, similar to cell architecture of having multiple cells taking up the task and increasing as per the requirement, the scale out model also essentially involves spinning up a parallel node and making sure either through sticky sessions in load balancer. If it is stateless application, which does not hold any session state and hence on breaching a threshold defined (like 60% in CPU for non-ABIS applications), a new VM can be spun up and ready to take the task.

- **Virtualization**: Data File System (DFS) servers are suggested to be used without any virtualization to avoid any overheads. Non DFS servers are having a mix of both virtualized and non-virtualized servers to ensure optimum performance as well as appropriate data center footprint. Essentially for the ease of operations and management, virtual servers give the best value and also results in data center consolidation where wastage of precious CPU power is minimized.

5.6. Database

Database form one of the most critical components of the RNP-DS and store different types of data (Unstructured and Structured). Following types of database shall be employed in the RNP ecosystem:

- **Relational Database:** Data which needs to be highly ACID compliant, where there is a high requirement of consistency, transactional needs, little or no tolerance to loss of data and isolation of data with rollback capabilities would be housed in relational database. The data would be highly structured in nature and stored as per a strict schema. These database are usually used for operational data characterized by frequent, short transactions that include updates, and touch a very small amount of data and where concurrency of transactions is very important. In the present context, demographic data store (UIN Master) is an example of such requirements[6].

- **Big Data Distributed Database:** Database that exhibits high magnitude of the 4 V's (Velocity of data, Variety of Data, Volume of Data and Veracity of data). Typically data that grows very fast such as unstructured data (images, logs, media files) and have lot of noise / errors in data, qualify for this category. Such data stores typically grow into large database. These database are characterized by master – slave architectures where data is distributed and stored in a distributed file system and accessed using data locality frameworks like map reduce etc. Hadoop framework is a leading example of big data framework widely used for storage and access of unstructured data. Here, DFS would be used to store raw biometric images and photographs.

- **NoSQL Database**: NoSQL database are increasingly used in big data and real-time web applications. They became popular with the introduction of the web, when database went from a max of a few hundred users on an internal company application to thousands or millions of users on a web application. NoSQL systems are also called "Not only SQL" to emphasize that they may also support SQL-like query languages. Since the authentication framework would be based on similar requirements (Large number of users connecting through the internet, sub-second response) and need to support quick changes in database schemas NoSQL database is chosen to be the data store for Resident Data Store. Some other advantages include better horizontal scalability, simplicity of design, better HA Features, capable of handling structured and unstructured data such as demographic and photos/minutiae.

- **In Memory Database:** An in-memory database (IMDB, also main memory database system or MMDB or memory resident database) is a database management system that primarily relies on main memory for computer data storage. It is contrasted with database management systems that employ a disk storage mechanism[7]. Main memory database are faster than disk-optimized database because disk access is slower than memory access, the internal optimization algorithms are simpler and execute fewer CPU instructions. Accessing data in memory eliminates seek time when querying the data, which provides faster and more predictable performance than disk. In the RNP Scenario, there is data

[6] Source: www.jamesserra.com/archive/2015/.../relational-databases-vs-non-relational-databases/
[7] Source: www.opensourceforu.com/2012/01/importance-of-in-memory-databases/

that needs to be very quickly accessed and static in nature such as OTP data, TSP license credentials among others. Such data is a candidate for being stored in IMDB kind of database[8].

- **File System Archives:** This kind of data store is not made of any sophisticated database management system but simply a set of folders on a filesystems attached to farm of servers. LUNs carved out of the SAN and exposed as filesystems make up this layer with these filesystems attached to commodity servers. The index for these filesystem contents would be maintained in RDBMS. This data-store would be used to contain the raw encrypted data packets which would be accessed very rarely in case of a biometric adjudication request.

5.7. Storage and Backup Components

Storage is suggested across two different categories to cater to the system requirement. However, following are key considerations that shall be taken into account for the storage components:

- Storage should be of enterprise class level, with multi-controller architecture and redundancies across hard disks and inter-connecting ports.
- It should support SSD, SAS and NL-SAS disks. All the disks should be dual ported disks.
- It should be interoperable with different kind of servers to avoid any vendor lock-in.
- It should be modular and scalable to handle large amount of data.
- The storage should be with No Single Point of Failure (SPOF). All the components should be redundant and hot swappable including power supply, fans, batteries etc. The storage solution must support non-disruptive replacement of failed hardware component, firmware upgrades and hardware upgrades.
- Any license required to enable these RAID levels, Data/Volume replications, DC/DR/NLDC/NLDR provisions, Array management etc. should be provided for entire supported storage capacity of the array.
- The proposed storage should support all the popular enterprise operating systems.
- The storage solution must support virtualized server environments proposed as well as other popular Virtualization environments like VMWARE, HyperV etc.
- The storage solution must support auto-tiering i.e. automated data movement at sub-LUN level between at least three storage tiers such as SSD, SAS, NL-SAS and SATA. Required software licenses for auto-tiering should be supplied for entire usable capacity.
- The storage remote replication solution should provide zero RPO with synchronous mode of operation. The storage remote replication solution should ensure data consistency on the remote storages

In the current setup, the following kinds of storage are proposed:

5.7.1. Distributed File System

A distributed file system is basically multiple servers with shared nothing model where the local disks of the server would be used to store the data. The Hadoop Distributed File System (HDFS) is a distributed file system designed to run on commodity hardware. It has many similarities with existing distributed file systems. However, the differences from other distributed file systems are significant. HDFS is highly fault-tolerant and is designed to be

[8] Source: https://stackoverflow.com

deployed on low-cost hardware. HDFS provides high throughput access to application data and is suitable for applications that have large data sets. [9]

In the setup designed, this is being handled by the Hadoop Rack servers, the direct attached storage of which would be used for storing the biometric data.

5.7.2. Storage Area Network (SAN)

Storage area network or SAN would be deployed to cater to the block service requirements for rest of the Non-Hadoop infrastructure that includes the web, app and DB tier. The SAN layer has three layers:

1. **Storage layer:** These would be the setup of SAN controllers and disk array enclosures. There are two options that are being widely adopted are All Flash Storage and Hybrid Storage. These options are described below:
    - **All Flash Storage**: Solid State drives have higher IOPS and the least latency offering as there are no moving parts in the SSDs. Moreover, these all flash drives because of the way SSDs work offers inline deduplication and compression that essentially increases the density of data and reduces the rack space and power requirement. Although slightly expensive than the discrete storage, with inline deduplication and compression, the price of all flash storage would soon near the price of discrete.
    - **Hybrid Storage**: These storage drives consists of mixture of SSDs, SAS and SATA drives. Although hybrid storage offers a great means for applications who have diverse tier (of IOPS) requirement, and it's cost effective too, but inline deduplication and compression is not available. But this kind of storage is fit for the use case where only a tiny portion (~25%) requirement is for flash and rest is for less IOPS.
2. **Switch layer**: Since SAN runs on a separate Fiber channel network that is different from TCP/IP or LAN, so it requires a different layer of SAN switches (such as those of Cisco MDS series or Brocade). These switches depending upon the number of servers(and their HBA ports) and the size of storage(which decides number of SAN controllers front end ports) would further decide if the no of ports has to be separated into Access and distributed SAN switches.
3. **Servers Layer**: As mentioned above HBA ports from Servers would be attached to the switches and then to the storage.
4. **Backup Target**: Backup also works on SAN network and should be of two types:
    - LAN based where data from the servers through backup agents is pulled onto a media server orchestrated by a master server and pushed to the backup target either through a Source based deduplication(at the host end) or a target based deduplication(at the backup target end).
    - SAN based where the backup data is identified directly from the SAN storage and there is no need for a Media Server.

5.7.3. Tape Library

Every data cannot be stored on a backup disk library (consisting of optical disks) and therefore there is need to dump data onto tapes that have magnetic storage and are much cost effective than optical disks.

In this entire aspect of storage and backup, it is critical to have a backup software which performs this entire activity of moving data from storage servers to backup disk target and then to tape library and do a restore when

[9] Source: https://hadoop.apache.org/docs/r1.2.1/hdfs_design.html; https://hadoop.apache.org › Hadoop › Apache Hadoop Project Dist POM

required. Also all backup software work on a backup and retention policy and an archival policy shall have to be defined as per business requirement.

5.8. Network Infrastructure

The network infrastructure components and solution architecture proposed to meet the RNP project requirements, considering the network security requirements is detailed in this section.

5.8.1. WAN and Internet connectivity

The WAN and Internet connectivity should be provisioned to provide communication link between RNP applications and users. The various WAN and internet connectivity requirements for RNP project are detailed below:

- **Internet connectivity**: Internet link will be used to provide access of public web portals and pre-enrolment portals to residents. It's proposed that two separate internet links with dual routers should be provisioned for high availability.
- **Internet for enrolment centers:** The enrolment centers should be connected using internet connectivity. The data center (DC and DR) should have dual last mile and dual routers to terminate internet connectivity.
- **P2P leased lines for TSPs, UAs and Government offices**: The TSPs, UA and other Government departments will be providing/using the authentication services and thus should have secured P2P private leased line to connect with the data center. UAs will be integrated using the API and the integration will be managed by the integration servers placed in DMZ. Thus, the UAs will only be able to communicate with application placed in secure zone, after secure integration using a secure key at DMZ level. The data center (DC and DR) should have dual last mile and dual routers to terminate connectivity, these router are also to be used to be used for other Fibre and P2P connectivity, except data replication.
- **P2P leased line for CNIE validation:** The enrolled new residents' data will be validated with the CNIE data thus a secured link should be installed between Data Centers and CNIE validation server locations.
- **P2P leased line for call center and helpdesks:** The call center and helpdesk for support services will be located at a remote location. Thus, to access the CRM portal a secured P2P private leased lines should be deployed in high availability.
- **Data Center Replication:** The data center replication link between DC and DR (Secondary DC) should be provided using a separate fibre link with a separate dedicated router pair in high availability.

The above mentioned network links will be used to carry sensitive data thus the network links should be secured with well-defined security infrastructure. The network security measures proposed for RNP infrastructure are listed below:

- **Network Segmentation**: The network segments with different security risks should be segmented separately. Thus its proposed that:
    - VPN WAN and P2P networks and internet should be terminated and secured separately
    - The data center network should be segmented based on security and application access requirements. The detailed proposed segmentation approach is given in next section
- **Data center perimeter security**: The internet and P2P links should be secured suing a perimeter security in the Data centers.

- **Data encryption:** IP-Sec based WAN encryption should be used for P2P links. This will secure data transmitting from Data center to enrolment Center, TSPs and Government offices.

The illustrative network architecture between data center and various user locations is given in the figure below. The detailed data center network architecture is detailed in the next section.

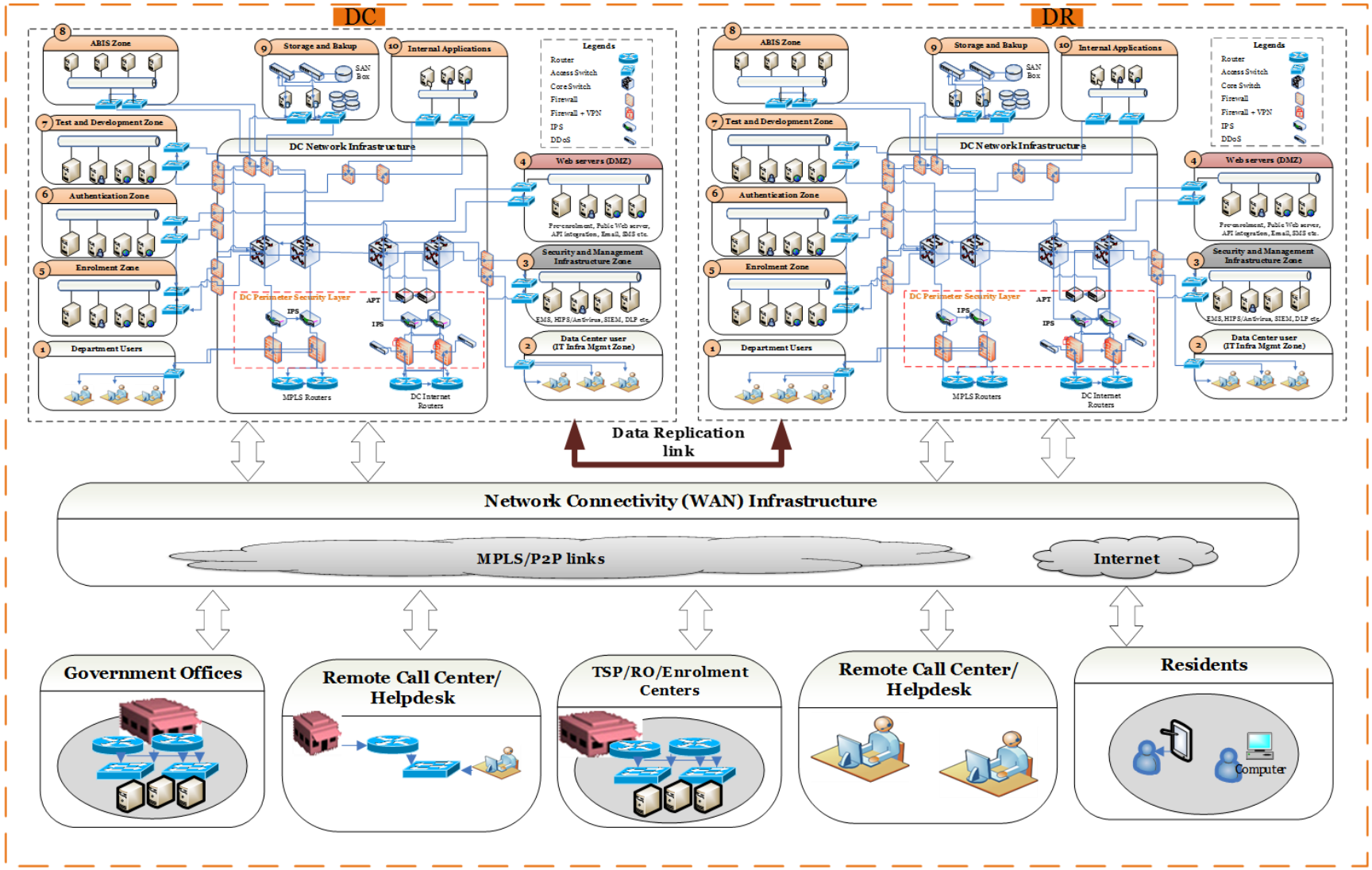


Figure 20: Network Architecture

5.8.2. RNP Data Store Network

The RNP application deployed in this data center will serve all users and business process. Thus, all network and security infrastructure components are proposed to be deployed in high availability at Primary and Disaster Recovery data center to ensure no single point of failure and meet the resiliency and security requirements. The overall network infrastructure to be deployed in data center is divided into multiple zones based on the criticality, data flow and security requirements of individual zones.

An illustrative architecture of data center with multiple zones, is detailed and illustrated in Figure 20. The zone 1-2 are the local user zone, zone 3 is security and management zone, zone 4 is DMZ having access from outside and 5-10 are MZ zones further segmented basis the criticality.

1. **User Zone (Zone 1 and 2):** All users collocated with Data Center facility, including administrators should be able to access application only after due authentication. Such traffic should also pass through the firewalls with specific policy being configured. Two separate user zones are proposed to be configured in Data center for Department users and infrastructure management. These zones are depicted as zone 1 and 2 in the Data center network design respectively.

   Access to infrastructure hosted in this zone: N.A. (These zones will not host any infrastructure)

2. **Security and Infrastructure management zone (Zone-3)**: This zone will host applications to be used for IT, network and security infrastructure management such as EMS, HIPS/Antivirus, SIEM, DLP, etc.

   Access to infrastructure hosted in this zone: Only from Zone-2 (Users room Infrastructure Management zone only) after Firewall and other security measures.

3. **Web servers and other public applications - Demilitarized zone (Zone-4):** This zone will host public web portal and other public application require internet access such as Pre-enrolment, CRM web gateway, email web gateway, SMS etc. require to be accesses/updated by external users. Only this zone will be accessible from internet and SMS provider.

   Access to infrastructure hosted in this zone:

   - *WAN: From all WAN network segments after Firewall and other security measures*
   - *Within DC: Zone-2, 3 and internal applications require communication with enrolment zone*

4. **Enrolment Zone (Zone-5)**: Enrolment zone will host applications require to communicate with the enrolment software such as FTP.

   Access to infrastructure hosted in this zone

   - *WAN: Only from MPLS or P2P links connecting Enrolment centers and CNIE validation server.*
   - *Within DC: Zone-2, 3 and internal applications require communication with enrolment zone*

5. **Authentication Zone (Zone-6):** This zone accommodated all the Authentication servers and application. All authentication requests are handled by this respective zone.

   Access to infrastructure hosted in this zone

   - *WAN: Only from MPLS or P2P links connecting TSPs and Government offices*
   - *Within DC: Zone-2, 3 and internal applications require communication with enrolment zone*

6. **Test & development Zone (Zone-7):** This zone will house the servers used for application testing and development. Separate zone should be created for this and zone should not able to communicate with secure application zone. This is optional and would depend on the Application Development model being offshore or onsite model.

Access to infrastructure hosted in this zone

- *WAN: Only from MPLS or P2P links connecting system integrator development center (if required)*
- *Within DC: Zone-2*

7. **ABIS Zone (Zone-8):** This zone will house the ABIS infrastructure and related applications to be access only by other applications.

   Access to infrastructure hosted in this zone

   - *WAN: None*
   - *Within DC: Zone-2 and internal applications require communication with this zone*

8. **Storage and backup Zone (Zone-9):** This zone will house the data backup application to be used for BI, Fraud analysis and analytics. Web portals and other related applications to be used by internal departmental users from Zone-1. Separate zones may be created using the same firewall for zone 8 & 9.

   Access to infrastructure hosted in this zone

   - *WAN: None*
   - *Within DC: Zone- 2 and internal applications require communication with this zone*

9. **Internal Application zone (Zone-10)**: This zone will house RNP internal applications and Data base servers such as BI, Fraud, internal portals, CRM etc. This zone will be the accessed only by internal users located in zone-1.

   Access to infrastructure hosted in this zone

   - *WAN: None*
   - *Within DC: Zone 1, 2 and internal applications require communication with this zone*

10. **DC network and Perimeter security:** This segment of the network will connect with all external connectivity such as Internet, MPLS, P2P etc. to provide DC access to users. Being the perimeter to the DC infrastructure various perimeter security controls such as Firewall, IPS and anti-Advance Persistent Threat (APT), DDoS devices are proposed in high availability. The WAN network connectivity along with WAN router will be provisioned as mention in the previous section.

    The Data Center network architecture proposed for RNP is illustrated in Figure below.

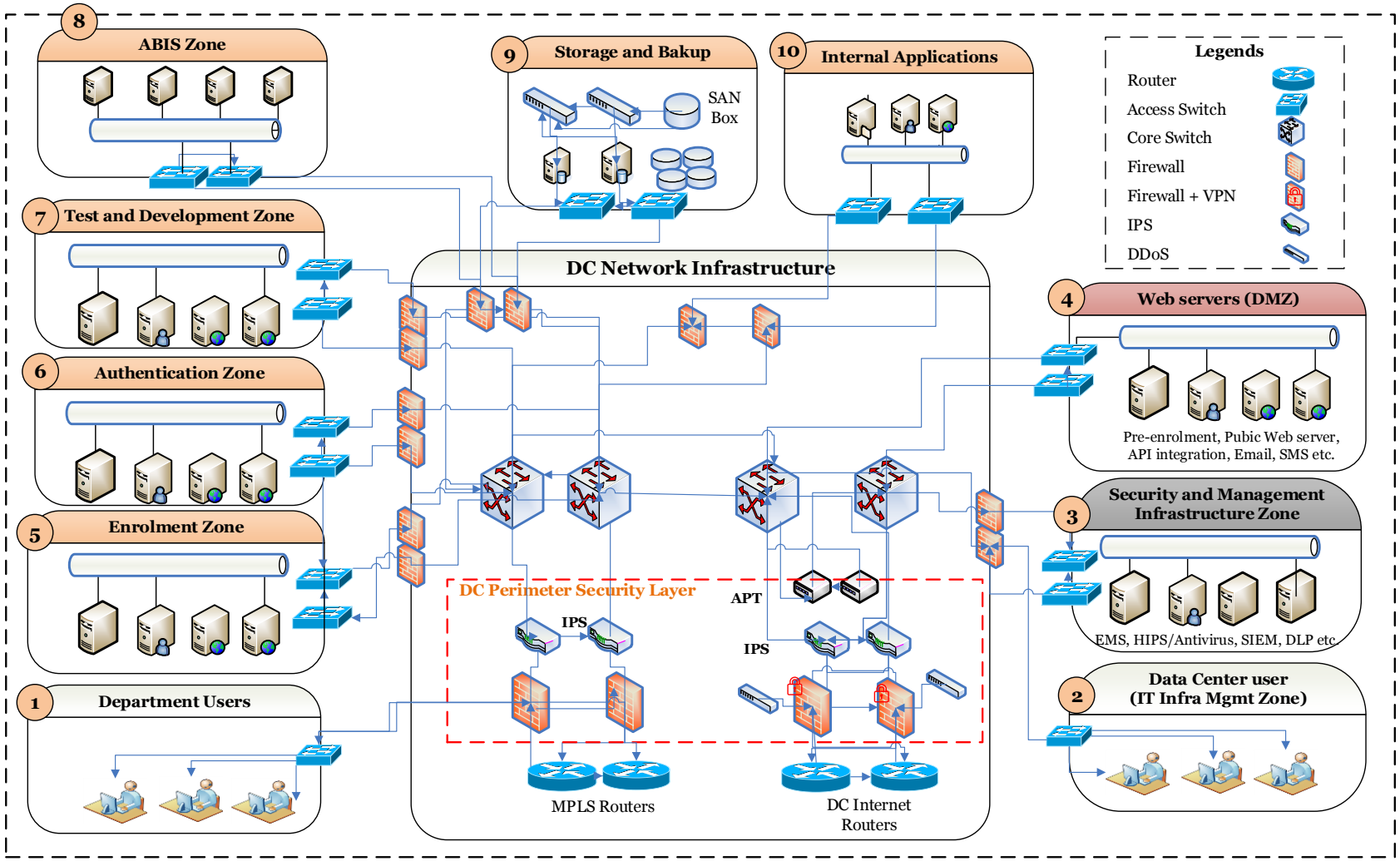


Figure 21: DC Network Architecture

5.8.3. Network and Network Security Components

S. No.	Network Component	Description
1	Routers - Internet	Router for internet connectivity
2	Routers - Intranet/MPLS/P2P	Router for internet connectivity
3	Core Switches	Core switch for DC/DR
4	DC Access Switch	Server farm access switch
5	Firewall - Internet	Perimeter Next Generation firewall for internet
6	Firewall - Intranet/MPLS	Perimeter Next Generation firewall for intranet (MPLS/P2P links)
7	IPS - Internet	Perimeter IPS for internet
8	IPS - Intranet/MPLS	Perimeter IPS for intranet
9	MZ/DMZ firewall	Internal firewall for MZ, DMZ security
10	APT and Network malware prevention	Advance security threat prevention
11	DDoS	Protection against Distributed Denial of services attack from internet.
12	SSL VPN Solution	SSL VP N solution for Internet users to security access applications
13	SIEM Tool	Security Incident and Event management solution for security logs correlations and alters
14	42U Network Racks	Network racks for DC and DR

5.9. Security Components

The RNP is a complex system in which many competing requirements from diverse stakeholders must be balanced. Security and privacy of personal data has to be fundamental in design as the system is collecting, storing, processing and/ or transferring large volumes of data related to the personal identity of the citizens. A lot of information is collected including but not limited to details about – name, address, sex, citizenship, and biometric information. When creating a database of this magnitude, it is imperative that privacy and security of personal data becomes a key design consideration. Hence, an effective and efficient security framework needs to be defined.

To establish a robust security architecture, it is important to identify major risks and threats to the RNP system:

- **Potential of data aggregation and profiling:** The RNP collects the sensitive Personally Identifiable Information (PII) data including biometrics for all the citizens of Morocco, thus providing a huge opportunity to illegal entities to aggregate data, profile and misuse it.
- **Identity Theft:** Identity theft is misuse of another individual's personal information to commit fraud. Identity theft (sometimes called identity fraud) occurs in many ways, but the basic elements are the same. Criminals gather personal information by stealing mail, workplace records, or other information, or they use high-tech methods such as hacking of websites, fraudulent email (phishing), social media sites, or purchasing information from companies selling background information about individuals.
- **Denial of Services:** Along with enrolment, NPR also provides authentication services. With DDOS attack, the perpetrator can make an authentication device or authentication network unavailable temporarily or indefinitely disrupting the services.
- **Unauthorized data capture:** Biometrics and other sensitive Personally Identifiable Information (PII) can be captured at the time of enrolment or authentication in plain text, stored and misused.
- **Data Leakage due to unsecure transmission and storage of PII:** Data transmission over insecure channels such as open Wi-Fi or HTTP can expose the data to unauthorized users/hackers and lead to data theft. Storage of such sensitive information in unencrypted format or in unencrypted data bases may lead to unauthorized or illegal access to resident's sensitive data.
- **Tampering with code to conduct faulty enrolments:** Biometrics of residents can be captured and stored in the enrolment software by tampering with the code for the software/enrolment packets.
- **Internal threats:** These include issues like data leakage by employees, suppliers, contractors, third party stakeholders among others.
- **External threats:** Data leakage due to hackers, malware, virus, phishing attacks etc.
- **Breach of Privacy:** Privacy is one of the biggest concerns of the biometric solution. If the servers storing biometric information is hacked, it could have extremely serious consequences for individuals.
- **Error in biometric devices during authentication:** False reject and false accept. This is usually due to the particular biometric technology being unable to read the characteristics of a given person for various reasons. The false accept is a scenario in which the device accepts an unauthorized person, and the false reject is the scenario in which the device falsely rejects an authorized person
- **Tampering with keys:** Public keys stored in enrolment software could also be tampered with.

Technology is ever-evolving and security threats ae increasing day by day. To tackle the ever-changing cyber landscape and formulating a secure and trusted Digital ID program for Morocco, security needs to be embedded in the initial design of the architecture and not as a side-product.

5.9.1. Security and Privacy Framework Components

Figure 22 - Security & Privacy Framework Components

5.9.1.1. Legal and Regulatory Framework

A strong legal and regulatory framework will lay the foundation of a healthy NPR. In this regard, the following needs to be done:

- A **legal framework encapsulating security as a primary function** should be created. This needs to be done to develop a security and privacy policy based on the best practices and industry standards.
- A legal **act needs to be developed, along with detailed regulations and guidelines** encapsulating all security features, Do's and Don'ts and other mandatory measures which should be applicable to all stakeholders. These need to be implemented diligently across the spectrum. Along with this, an Information Security Policy also needs to be formulated (as part of Deliverable L10 – Information Security Plan) which would be applicable to the organization as well as the ecosystem partners.
- **Penalization and disciplinary action**: NPR with its large and dynamic ecosystem consists of numerous staff members and ecosystem partners who are involved at various levels in handling the critical and sensitive information. As such any non-compliance to the regulatory act, security policies and controls can have an adverse impact. Hence, it is imperative that the government as well as the NPR monitors the compliance and takes adequate action in case of non-compliance and levy adequate penalties.

5.9.1.2. Security Governance Model

A strong governance model for security needs to be implemented with clear accountability, independence and empowerment to make decisions and continuously improve the security posture of RNP program. In this regard, the following needs to be done:

- A separate **security division should be created, which functions independent of other departments** such as operations or maintenance to govern after the complete security framework and reports directly to the head of the organization.
- A **detailed information security plan and policy** should be devised for the organization that is understood and followed by all employees, contractors, or any other person with access to your private, non-public personal data. Information security and privacy is required to be built into the strategy without sacrificing the functionalities of the RNP system. Hence, the Information security policies and procedures need to be stablished to lay the foundation for establishing, implementing, maintaining and continually improving the Information security management system
- **Adequate budget for cyber security implementation** needs to be provided
- Competent staff / agency to establish and maintain the security should be deployed
- Strong **Incident and crisis response mechanism** needs to be built to ensure timely response, investigation, media management and stakeholder management post a security incident.
- A continuous security monitoring program should be established to evaluate the performance of security of RNP.
- Partner with the various government and private agencies to enhance the security of RNP.

5.9.1.3. Security Certification

The objective of Certification is to ensure effectiveness of the security implementation and management through the use of the information security policy and components, security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review.

Following levels of certification should be obtained for the RNP system:

1. **Complete Infrastructure Certification:** Complete infrastructure including the central data repository should be ISO 27001 certified by a recognized body. Following activities would broadly include the ISO 27001 certification:
    - Risk Assessment
    - Development of ISMS Policies and Procedures
    - Training and Awareness
    - Pre-certification Assessment
    - Final certification
2. **Data Centre Certification:** Complete assessment of the data center by a recognized body against national/international standards such as TIA 942 including following areas broadly:
    - Network architecture and technology
    - Building Management system
    - Physical and environmental controls
3. **Authentication and Enrolment biometric devices:** Only certified biometric devices ensuring **c**ompliance to industry standards from an certification agency in Morocco body should be displayed covering following parameters:
    - Hardware
        - Visual & functional

- Physical & Dimensional
- Environmental (Durability /Climatic – Temperature, Humidity, Shock/Vibration, Dust etc.)
- EMI/EMC

- Image Quality
- APIs and software application
  - Functional
  - Authentication APIs
- Performance
  - False Reject Rate (FRR)
  - Acquisition Time

4. **Third Party applications:** All applications which capture residents PII for purposes such as authentication should be certified by a recognized body ensuring comprehensive device level security features in order to avoid unencrypted data capture.
5. **Internet Facing Portals:** An audit certification of RNP portal(s) from an independent third party to ensure compliance to security standards and best practices.

Apart from this, network and security devices should be procured from the OEMs which get their devices certified from specified certification agency.

5.9.2. Enhancement in the security posture

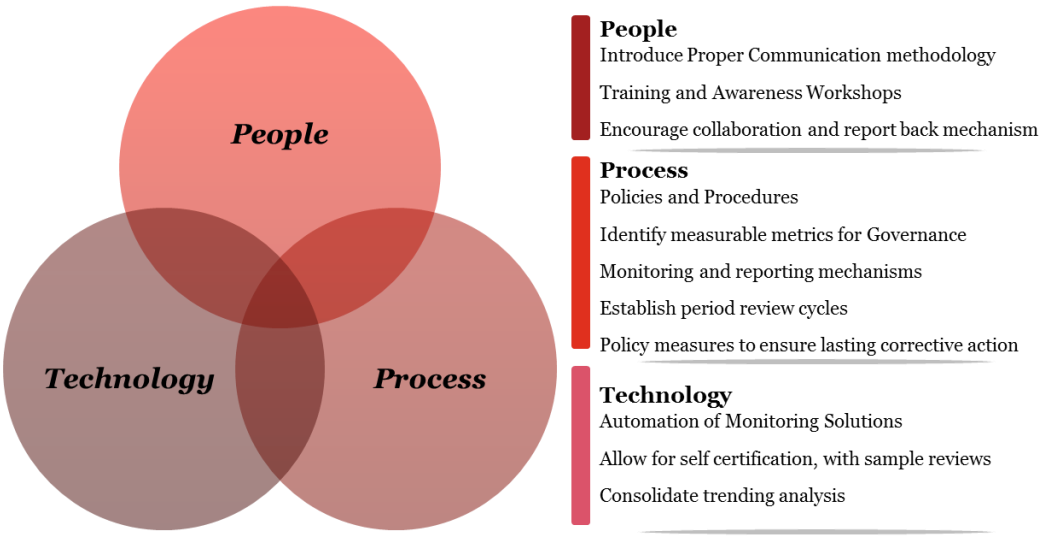


Figure 23 - Security Posture Enhancements

The technology components along with associated operating processes/procedures and people have specific risk profiles that need to be mitigated comprehensively and effectively.

5.9.2.1. People

The accountability for information security at RNP needs to be established with clearly defined roles and responsibilities. A well laid down security organization structure operationalises the security with clear line of communication and accountability. At the same time, the staff, including external partners, should be encouraged to adopt security practices and accountability fixed with each one to ensure a safe and secure ecosystem is built.

In order to increase the accountability and credibility of the organization, it is important to devise a strong/robust governance structure for managing security. An independent body, like CISO office, can be constituted to oversee the security governance, risk, compliance and performance for the organization in order to enhance governance, entitlement and access to information, data protection and overall perimeter security. All the assessments conducted by such a body must be independent of the MoI's management and be answerable to the senior management of MoI. This will ensure unbiased and effective results.

Segregation of duties and fixing accountability

- **Risk Owners:** It is important to identify clearly who are the risk owners. A CISO or CIO should be appointed to guide through the cyber related issues and develop an extensive information security policy for MoI. Risk Owners shall be accountable for their respective division risks.
- **Data Protection Officers:** A data controller or data protection officer must be appointed to see the implementation of the legal requirements.
- **Steering Committee:** A Steering Committee involving the management of MoI, CISO and division heads shall be constituted to take unbiased decisions on risk management, security solutions, etc. The decisions related to technology and security would be overseen and implemented by MoI.

5.9.2.2. Process and Technology

Processes and procedures are required to implement the legal requirements and ensure compliance with policy. High level security processes that need to be implemented are listed below:

- **Data repository:** It essentially contains information that RNP intends to store and retain. This data store consists of various records such as demographic data, biometric data, enrolment records, authentication records, ecosystem information etc. Since this repository contains information that is of paramount importance to identify a resident and establish trail of events specific to a record, it needs to be protected at every stage of its lifecycle.
- **Network security components**: Devices/products/solutions to provide secure storage, processing and transmission environment in the RNP data network. This could include controls such as firewall, anti-malware, encryption, logical access control etc.
- **Device Level Encryption**: It should be ensured that the biometrics are encrypted as and when they are captured at the device itself. Registered devices can be used for the same.
- **Key Management:** Key management is crucial to success of identity and authentication services for all stakeholders other than residents. It helps an establishing identity, confidentiality/ integrity and ensures in non-repudiation of system users. HSM should be used for effective key management
- **Application security**: Applications would act as the interface for information exchange so security of the presentation layer, application logic layer and the database layer needs to be considered.
- **Logging and auditing**: Logs provide useful information to support troubleshooting, forensics, audits, trend analysis, internal investigations, incident response and optimizing system and network performance. It is essential that RNP collects, periodically reviews, and securely archives the security log data for a defined period of time.

- **Access management:** Implement processes that allow tracking and recording the persons/entities who have access to or custody of nonpublic personal information and the time of such access or custody
- **Asset management:** In case any mobile devices, unauthorized devices, or software is in use, inventory and management of such assets is important
- **2-factor authentication:** Combination of password and OTP/ Biometrics can be implemented to ensure secure login and avoid unauthorized access.
- **USB based software:** USB based enrolment software only which boot up only through USB, are encrypted within USB, is like a sand box and no other computer applications could interact, would not work on any other system than the one which it is mapped with.
- **Continuous monitoring & Audits**: Continuous Monitoring of the ecosystem is extremely necessary in a dynamic environment like that of RNP which has multiple servers, applications, database, and ecosystem partners. Apart from the technological security monitoring, it is also important to have a monitoring process for the internal and external ecosystem partners to ensure their compliance with the security controls as defined. This will provide continuous awareness of IT security, threats, and vulnerabilities and executive-level, risk based reporting to inform RNP's decision-making.
- **Robust Perimeter Security:** The data center hosting the servers should be protected by firewalls, Intrusion Prevention systems (IPS) and others. The perimeter should be continuously monitored by a robust Security operations center (SOC) for security threats on a 24x7 basis.
- **API based interaction**: Interaction of the various Ministries/ Departments with the data center should be through APIs only hence restricting the level of access.

Some indicative security procedures (SoPs) that will be developed as part of the security policy are listed below:

1	Patch Management	**18**	Remote Access
2	Third Party Management	**19**	Identification and Authentication
3	System Security	**20**	Audit and Accountability
4	Security exception	**21**	Monitoring and Review
5	Personnel Security	**22**	Security Assessment
6	Physical and Environment	**23**	Encryption
7	System and Services Acquisition	**24**	Risk Assessment
8	Configuration Management	**25**	Portable Media
9	System and Communication Protection	**26**	Wireless Network
10	Information Document Management	**27**	Mobile Phone
11	Maintenance	**28**	Malicious Code Protection
12	Email Security	**29**	CDA (Critical Digital Assets)
13	Awareness and Training	**30**	Contingency Plan
14	Incident Response	**31**	Business Continuity Plan
15	Media Protection Procedure	**32**	Cloud Computing

16	System Control & Integrity	**33**	Crisis Management Plan
17	Access Control	**34**	Information & Operation Technology Sub-policies

The detailed list is provided in the L10, the key indicative security components that need to be deployed are:

#	*Security Technology Component*	*Purpose / Threats Avoided*	*Priority*	*COTS/ Open Source*
1	Firewall	To provide a barrier to control network traffic both into and out of organization's Internet-connected network, or between different segments of an internal network. Firewalls also provide protection against threats including denial of service (DOS) attacks.	P1	COTS
2	Web Application Firewall	Filters, monitors and blocks HTTP traffic to and from a web application. By inspecting HTTP traffic, it can prevent attacks stemming from web application security flaws, such as SQL injection, cross-site scripting (XSS), file inclusion, and security misconfigurations.	P1	COTS
3	DLP – Network and Endpoint	To identify, monitor and protect data in use, data in motion on network, and data at rest in data storage area or on endpoints.	P1	COTS
4	IDS/IPS	To inspect network traffic to identify signs of malicious activity and policy violations, enabling organizations to respond before a threat actor causes significant harm to IT systems.	P1	COTS
5	Email Gateway	To prevent data loss, perform email encryption, protect against known and unknown malware. By detecting and blocking malware, spam, phishing attempts and other malicious content, can significantly reduce the number of attempted and successful attacks against an organization	P1	COTS
6	Web Gateway	To filter unwanted software/malware from user-initiated Web/Internet traffic. Used for black box testing or dynamic testing of the web applications	P1	COTS

#	Security Technology Component	Purpose / Threats Avoided	Priority	COTS/ Open Source
7	Web Vulnerability Scanner	Tool used for web application security. Scans and identifies vulnerabilities in web applications.	P1	COTS
8	Code Review Tool	To conduct security code review of an application's source code in order to ensure that the application has been developed so as to be "self-defending" in its given environment.	P1	COTS
9	Network Vulnerability Scanner	Vulnerability management tool to find security loopholes in the networks.	P1	COTS
10	HSM	Dedicated crypto processor that is specifically designed for protection of the crypto key lifecycle. It protects cryptographic infrastructure of organizations by securely managing, processing, and storing cryptographic keys inside a hardened, tamper-resistant device.	P1	COTS
11	Antivirus solution	Used to prevent, detect and remove malicious software.	P1	COTS
12	SIEM solution	To get full visibility of the infrastructure via logs. Provides enterprises with network security intelligence and real-time monitoring for network devices, systems, and applications.	P1	COTS
13	PIM/IDAM suite	To secure, manage and track user access to privileged accounts	P1	COTS
14	Active Directory	Centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories.	P1	COTS
15	ITAM	Asset Management tool	P1	COTS
16	HIPS	To protect hosts against local, application and network based attacks.	P1	COTS

#	Security Technology Component	Purpose / Threats Avoided	Priority	COTS/ Open Source
17	Network Access Control	To implement policies for controlling devices and user access to their networks. NAC can set policies for resource, role, device and location-based access and enforce security compliance.	P2	COTS
18	Anti DDoS	To prevent DDoS attacks	P2	COTS
20	Database Activity Monitoring	To independently monitor and audit all database activity, including administrator activities. To generate alerts on policy violations, provide real-time monitoring and rule-based alerting.	P2	COTS
21	Anti-APT	Advanced Persistent Threat Protection solution	P3	COTS
22	Anti-Phishing	To prevent Phishing attacks	P3	COTS
23	UEBA	To conduct social engineering	P3	COTS
24	DRM	To enable secure file sharing, access and storage	P3	COTS
25	File Integrity Monitoring	To detect potential threats with real-time alerts for changes to files, folders, registry settings, and unauthorized access	P3	COTS
26	Sandboxing	To execute untested or untrusted programs or code from unverified or untrusted third parties, suppliers, users or websites, without risking harm to the host machine or operating system	P3	COTS
27	TACACS/RADIUS	Centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.	P3	COTS

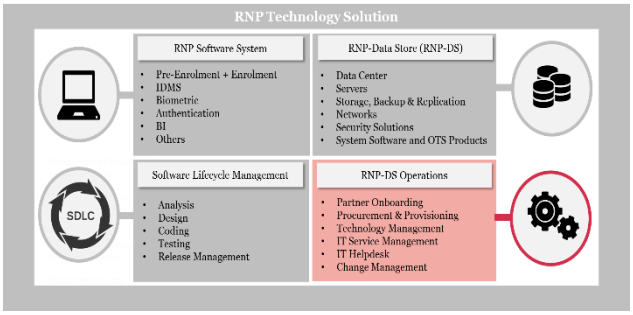
Note:

1) A tentative priority for security components is assigned with P1 being the highest priority and P3 being the lowest

2) Detailed security architecture along with the information security plan will be provided in the forthcoming deliverables

6. RNP Data Store Operations

The RNP solution has been categories into 4 broad aspects, i.e., RNP Software System, RNP-Data Store, Software Lifecycle, and RNP–DS Operations. This section covers the fourth component of the RNP solution, i.e. RNP–DS operations.



This section provides an overview of the activities of the project relating to two broad areas: Designing to commissioning of the entire infrastructure and the operations and maintenance.

The section also includes sub key activities like partner onboarding, procurement and provisioning, technology management, IT Service Management, IT Helpdesk, Change Management, etc.

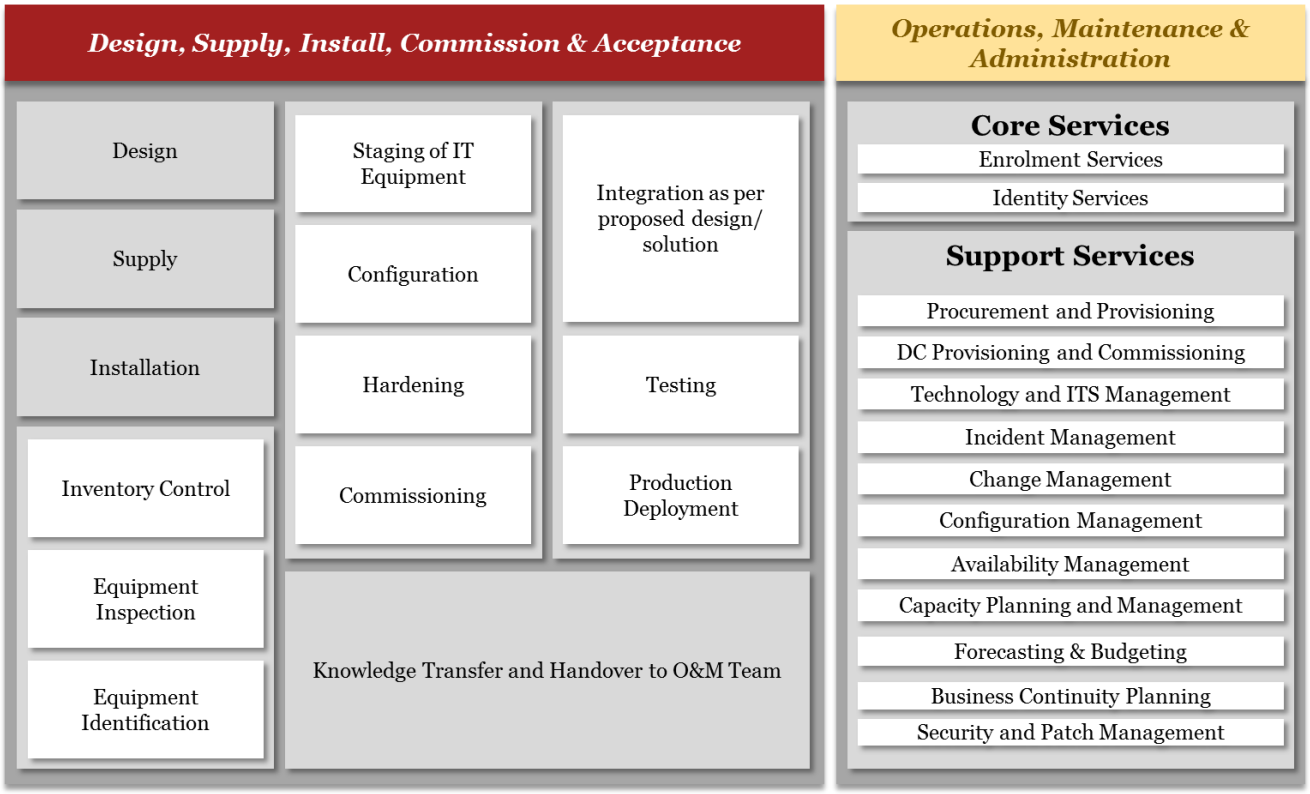


Figure 24 - Data Store Operations

6.1. Design, Supply, Install, Commission & Acceptance

As part of the overall lifecycle, the infrastructure has to be designed as per the deployment design. The IT Infrastructure will be supplied and installed at the data center, commissioned as per the specifications mentioned for each type of server, storage, network components, etc. Acceptance of these equipment would be done as per the acceptance criteria and aspects like mapping of servers with the right set of applications, mapping the LUNs of storage for right level of database servers, setting up firewall equipment with appropriate ports for creation of zones, etc.

6.1.1. Servers

The brief of activities for servers is defined for each component as below:

- Design of servers will be done based on the final sizing requirements arrived, taking into account the redundancy and high availability requirements. This would include necessary provisions like redundant ports availability, HBA cards, and redundant high performance hard disks for operating system, application, etc.
- Supply of servers need to be done keeping in mind the go-live of the entire system, as the procurement and installation activities take time
- Depending upon the type of server – rack / blade, the server would be mounted in the racks as per the installation schedule with some spaces between IUs to reduce noise level
- Power and peripheral devices will be plugged in properly and AC power would be supplied to server through power PDUs
- OS hardening would be done during the installation of servers to improve security
- Testing of the servers with respect to the installed images of OS and application would be done, to avoid any mismatch in the configurations and also to avoid any errors during the development, testing or production phase of applications
- Deployment of the servers for production environment would be done, only after thorough checking of the configurations with respect to each server.
- Maintenance of the servers would be carried out, with appropriate physical cleaning, and all cables will be appropriately stacked and numbered, interconnecting through access switches and storage components.

6.1.2. Storage

The brief of activities for storage is defined for each component as below:

- Design of storage component will be done based on the final sizing requirements arrived and the IOPs requirement. Based on the same, a multi-controller storage solution would be taken with a mix of different type of disks. Buffer at storage disks also need to be taken for global hot spares within the storage solution, providing redundancy and high availability at disk levels.
- Supply of storage equipment is to be aligned with the procurement of servers so that appropriate card installation and interconnecting switches are deployed appropriately.
- Installation of the storage components starts with identification of the right set of servers, applications and data sets.
- The next key step as part of installation activity of storage is to configure each disk array with appropriate RAID levels.

- The SAN topology would be defined with respect to each zone viz. test, development, testing, production etc.
- Interconnection would be done through pair of switches to ensure high performance and redundancies across the architecture.
- SAN management software would be used for the entire setup and configuration with servers. This will also help in testing of the storage devices through checking appropriate mapping of servers.

6.1.3. Backup Target (Virtual Tape Library)

The brief of activities for backup target is defined for each component as below:

- The sizing of Virtual tape library is done basis the amount of backup and the inline deduplication and compression that is estimated based upon the file type.
- It would be defined that for which type of data LAN based backup would be done and for which SAN based backup would be configured.
- Normally backup can be classified into agent-based or agentless. Depending upon the data type, the same would be configured.
- Deduplication can again be source based or target based, which is also contingent upon data type.
- Depending upon the backup policy it would then be decided which data has to be kept for how much duration on the virtual tape library before tape out can happen.

6.1.4. Tape Library

The brief of activities for tape library is defined for each component as below:

- It would be important to finalize the backup and restoration policy based upon critical and non-critical data that further has to be defined based upon business criticality
- Design of tape library component will be done based on the final sizing requirements arrived, the backup policy, window and the redundancies to be maintained at drive level. Based on backup window, the number of drives are to be identified which will take simultaneous backup of data as per the mapping of back-up software. Number of cartridges would also need to be taken into account based on the back –up policy (incremental / full – backup) and frequency of backup.
- Supply of backup system would be done along with server and storage equipment.
- The tapes are labelled by backup software automatically. The tape drives uses the Barcode labels to distinguish between the tapes. Tapes management is an important task including the transfer of tapes to a safe place on account of security concerns
- The Storage and backup team would perform:
    - Initiating and monitoring the backups and Re-initiating the backups if required.
    - Maintenance of backup infrastructure
    - Intimating the authorized personnel for monthly tape movement
    - Sharing the backup logs
    - Maintaining the backup and restore procedures
    - Performing the restoration
    - Ensuring that the tapes are always stored inside the fire-proof cabinet

6.1.5. SAN switches

The brief of activities for SAN Switches is defined for each component as below:

- SAN switches are configures in HA in active-active mode
- To ensure that sufficient throughput is available between front end ports of the storage and interconnect modules of the blades/HBA ports of the rack servers
- To ensure that the switch would have No Single Point of Failure (SPOF) and all the components should be hot swappable without even scheduled down time.
- To ensure that fiber cabling is done in the right manner using structured cabling where individual fiber pairs are aggregated together into a cable and terminated on a patch panel

6.1.6. Network Components

The brief of activities for Network Components is defined for each component as below:

- All network components, i.e., Switches, routers should be configured in HA with no single point of failure in DC and DR
- All network security components, i.e., Firewall, IPS, APT, DDoS should also be deployed in HA with no single point of failure in DC and DR
- The network ports, process and memory should not be utilized more than 70 percent
- Dynamic protocols such as OSPF, BGP etc. should be used to configure WAN links in HA
- IP planning should be undertaken properly to avoid conflicts
- Separate IP pool should be defined for network management

6.2. Operations, Maintenance and Administration

The activities under the phase of the project can broadly be categorized into operations which are core to the functioning of the RNP program and operations which support these core operations. The overview of core services is covered in Section 6.2.1 and overview of support services is covered in Section Support Services6.2.2. Detailed Operations, Maintenance and Administration activities would be submitted as part of the L4 deliverable.

6.2.1. Core Services

The core services can be classified as those services which directly affect the operations of the RNP program. As the program involves two major aspects i.e. enrolment and identity services, the core services have been described under these heads:

6.2.1.1. Enrolment Services

Enrolment is one of the key services under the RNP program. In this service, the residents are enrolled in the RNP program using the enrolment kit at the enrolment center. The support activities for enrolment services shall cover the following aspects:

- **Maintenance of Enrolment Software**: The software utilized for the purpose of enrolment may need to be enhanced to accommodate changes and improvements. The improvements may be related to

location dictionary, name dictionary, performance upgrade, etc. The changes or maintenance may be related to bug fixes, renewal of encryption certificate, new OS support, new device support, etc.

- **Maintenance of Enrolment Kit**: The hardware utilized for the purpose of enrolment may need to be maintained to ensure it is fit for performing enrolment. The services may include hardware maintenance/replacement, software upgrades, patches, etc.
- **Training of Enrolment Manpower**: The training of enrolment officers and support staff is an important part of the enrolment operations to ensure good quality of enrolment.
- **Quality Assurance**: The services of assuring quality of enrolments including sampling and blacklisting/suspending the enrolment operator is covered under this aspect.
- **Manual Adjudication**: The enrolments flagged during the biometric deduplication may undergo a manual process of adjudication where authorized officers may re-verify the results of automated matching.
- **Archiving of Physical Forms**: The application forms and supporting documents provided by the resident at the time of enrolment along with a copy of enrolment acknowledgement may be stored physically, if required under the legal framework. The service will comprise collection, secure storage, upkeep and retrieval of these documents.
- **Letter Personalization, Distribution and Issuance**: This is the process of personalization of the letter issued under the program, their distribution either directly to residents home or to nearby center, and the issuance of these letters from the nearby CSC(s) is another core service.

6.2.1.2. Identity Services Partner Onboarding and Device Management

Service Delivery is one of the key outcome under the RNP program. For this purpose, a federated model is planned to be adopted. In this federated model, there will be agencies which will be connected directly to the RNP solution through secure and dedicated network. These agencies will be known as Trusted Service Providers (TSP) and will be responsible for extending the services to the other agencies. In addition, there will be agencies which will utilize the identification services in their operations and process. These agencies, known as User Agencies (UA), will submit the request for identification services to RNP through TSP. The UA will deploy the biometric capture devices at their point of services and these biometric devices will have to be pre-registered with the RNP solution. The devices so authorized after the registration will be known as 'Registered Devices'. The support activities in identity services shall cover the following aspects:

- **Onboarding of Trusted Service Provider**: The service of onboarding the TSP involves administrative procedure, technical integration support, compliance audit, maintenance of secure keys for data exchange, etc.
- **Onboarding of User Agencies**: The service of onboarding the UAs involves administrative procedure, technical integration support, compliance audit, maintenance of secure keys for data exchange, etc.
- **Registration of Devices**: The service of maintaining and updating the list of registered devices for all the UAs

6.2.2. Support Services

6.2.2.1. Procurement and Provisioning

The setting up and operations of RNP solution will require procurement, supply and installation of entire IT infrastructure. The IT infrastructure includes servers, storages, back up, networking, load balancers, security equipment, operating systems, database, licenses, help desk system and other related IT infrastructure required

for running and operating the envisaged system. The IT infra procurement will be planned with following considerations:

- **Phased Deployment**: The entire infrastructure will not be procured at the start of the project. The non-cell components can be procured at the start of the project. The cell components may be procured as per the prescribed schedule to support increase in enrolment workload. The ownership of IT infrastructure shall lie with the Ministry of Interior.
- **Ensure redundancy**: The redundancy should be built-in to ensure defined service levels are met

In order to ensure that the infrastructure meets requirements, the minimum technical specifications will need to be defined for all major components. All the IT infrastructure procured under the project will need verification and acceptance by the RNP team. After the verification and acceptance of the IT infrastructure, it will be provisioned in the DC/DR of the RNP project.

For all hardware components, warranties/AMCs will required to be ensured for entire project duration and for software components the support from OEM to be obtained for prescribed components. A mechanism should be established to verify these details on annual basis.

6.2.2.2. Data Centre Provisioning and Commissioning

The entire RNP Solution will have to be deployed on a dedicated data center model with specified requirements. There should be sufficient capacity (compute, network and storage capacity offered) available for near real time provisioning during any unanticipated spikes in the user load. The redundancy should be built into the architecture (at all levels) and load balancing to meet the service levels.

While the initial sizing and provisioning of the underlying infrastructure (including the system software and bandwidth) may be carried out for the first phase; subsequently, based on the growth in the user load (peak and non-peak periods; year-on-year increase), data center will scale up using the 'cell architecture' with appropriate compute, memory, storage, and bandwidth requirements to support the scalability and performance requirements of the solution and meet the SLAs.

The ownership of all virtual machines, templates, clones, and scripts/applications including application code (all versions) created for the RNP system, and all licenses purchased under the project should be with RNP. This shall include the right to request (or should be able to retrieve) full copies of these virtual machines at any time.

As part of the data center architecture deployment, backups of all the data including but not limited to files, folders, images, system state, database and enterprise applications shall be configured, scheduled and managed.

6.2.2.3. Technology Management and IT Service Management

The operations and maintenance of all the components of the RNP System after Go-Live date will be an on-going activity in the O&M phase. During O&M phase, service levels will be monitored on a continuous basis. After Go-Live, if any system/sub-system/appliance that is deployed during the O&M phase should be augmented in the RNP system only after proper induction procedures are followed including hardening and security testing. A suitable Performance Improvement Process (PIP) will be implemented in the project. PIP program applies to all the processes of RNP System for which a detailed approach may be finalized by the system integrator.

The broad details of technology management activities are mentioned below:

- **Application Support and Maintenance**: Application support includes, but not limited to, production monitoring, troubleshooting and addressing the functionality, availability and performance issues, implementing the system change requests, etc. This ensures the application software is in good working order; changes are performed and upgrades are applied to applications. All tickets related to any issue/complaint/observation about the system may be maintained in an ITIL compliant comprehensive incident management/problem management solution. The major activities to be performed include but not limited to the following:

- SLA compliance monitoring
- Availability of Annual technology Support for system updates, upgrades and OEM support
- Onsite Application software maintenance support
- Problem identification and resolution
- Change and version control through the approved Change Management process
- Maintain configuration information for application software and any system documentation
- Organize provisioning of trainings to personnel as per the requirement
- Maintain system documentation such as HLD, LLD, SRS, Traceability matrix, source code, FRS, user manuals, SOPs, etc.

- **IT Infrastructure Support and Maintenance:** IT infrastructure includes servers, storages, back up, networking, load balancers, security equipment, operating systems, database, enterprise management system, help desk system and other associated IT infra required for running and operating the envisaged system. IT Service Management (ITSM) processes aligned to ITIL framework for all the IT Services would be defined and managed as part of this project. IT infrastructure support and maintenance would include, but not limited to the following:
  - Warranty support for deployed IT infrastructure
  - Preventive maintenance of all hardware and testing for virus periodically as per predefined checklist for identified components
  - Asset Management to manage the entire lifecycle of every component in the RNP system
  - Management of DC and DR sites in compliance with industry leading ITSM frameworks like ITIL, ISO 20000 & ISO 27001
  - Overall System Administration, Maintenance and Management
  - Storage Administration
  - Database Administration
  - Network Administration
  - Backup/Restore/Archival
  - Monitoring and administering the network within the Data Centre/DR etc. to maintain optimum performance of the entire network of RNP System
  - Management of the overall security posture of the entire RNP system
- **IT Helpdesk:** This includes running centralized helpdesk setup and operations for RNP project. The help desk will serve as single point of contact for reporting/resolution of all tickets (queries, errors, incidents, issues either application or infrastructure or operations related). The helpdesk will be able to handle technical queries raised by the officials at enrolment centers or enrolment administration officers, TSPs, User Agencies, and other users for the RNP system.

6.2.2.4. Incident Management

The IT Service Desk support functions are complemented with a resilient Incident Management process. Incident Management processes would be defined to monitor progress of open incidents/ issues for their resolution (end to end life cycle of incidents). RNP will leverage an Enterprise IT Service Management tool to register, categorize and prioritize Incidents and apply a pre-agreed Service Level to each and every Incident for its effective resolution and prompt monitoring of the system. This will ensure that the best possible levels of service quality and availability are maintained.

Following are the key considerations for the proposed RNP's Incident Management processes:

- For IT Service Management, ITIL v3 is the proposed framework and ISO/IEC 20000 is the proposed quality standard
- All incidents should be recorded, reported and open to audit through logs
- All incidents are stored in a common repository and updated throughout their lifecycle
- Information on the status and progress of incidents will be available to the incident reporter for the affected service
- Predetermined restoration targets shall exist for incidents based upon the defined Service Levels
- Incidents will be prioritized and resolved based on the impact and urgency assigned them
- A full escalation management policy will exist to ensure unresolved incidents gets resolved
- All aspects of major incidents are controlled and coordinated by the Incident Manager

6.2.2.5. Change Management

It is envisaged that due to the evolving nature of the project requirements, especially with the number of enrolments and identification services, there would an increase in the required infrastructure unit 'cell', thus, changes in the system are inevitable. These changes may require modification to the software, infrastructure and underlying processes. All such changes should be discussed, managed, and implemented in a constructive manner.

The change management procedure and institutional framework should be established keeping in mind the following objectives:

- To protect the RNP System environment from uncontrolled changes
- To minimize the occurrence of unintended affects during the implementation of necessary changes
- To avoid implementation of any changes which is not reviewed, approved or analyzed
- To control the impact of changes and minimize the effect on effective as well as efficient service delivery

The key considerations for the proposed RNP's Change Management procedure are as follows:

- Every change to the Configuration Items (CIs) on production should be recorded in the Change Management Database (CMDb) which shall be part of the EMS in Management layer. Change Management processes should be followed in order to optimize the risk exposure and to minimize the severity of any impact and disruption
- All incidents caused by a change must be linked to that change
- Sticking to the Change Schedule is very important in order to reduce the unplanned work
- RNP Change Management must be the first point of call for any change; all third party releases must be approved by RNP before external submission.
- The release shall be verified against the agreed acceptance criteria and approved before deployment
- This policy is also applicable on the patches
- The service acceptance criteria for all changes are the service level targets defined in the SLA. RNP will test every release against this target before going to the production environment.

6.2.2.6. Configuration Management (Updates / Upgrades)

Configuration Management would include identification, recording and reporting of IT components in the production environment for RNP, including their versions control, constituent components and relationships among the components, access controls, policy services and other associated business functions.

The primary goal of the Configuration Management process is to support the economic provision of services; allowing efficiency and effectiveness by means of control over the infrastructure and services. In that sense, Configuration Management has the responsibility of providing a logical model of the infrastructure and the services as delivered by RNP to the citizens and other stakeholders.

6.2.2.7. Availability Management

The availability management process for the RNP system will have the following objectives:

- Ensure IT Services are designed to deliver the levels of availability required by the business
- Provide a range of IT availability reporting to ensure that agreed levels of Availability are measured and monitored on an on-going basis[10].
- Optimize the availability (resilience, reliability and maintainability / serviceability) of the IT infrastructure to deliver cost effective improvements that deliver tangible benefits to the business and user
- Achieve over a period of time a reduction in the duration of Incidents that impact Service Availability
- Ensure shortfalls in IT availability are recognized and required corrective actions are identified and progressed
- Create and maintain a forward looking Availability Plan aimed at improving the overall Availability of IT Services and infrastructure components to ensure existing and future business availability requirements can be satisfied[11].

The key considerations for the proposed RNP Availability Management are as follows:

- Implementation of a well-defined availability policy/ guidelines which are aligned with customer expectations for delivery of services from the RNP system.
- Infrastructure should be deployed from the Availability requirements perspective
- Availability Management Process must adhere to the existing security policies and procedures
- An Availability Plan will be utilized to track and manage availability requirements and data
- Data on reliability, maintainability, resiliency, and serviceability must be collected and monitored
- IT utilizes a continuous process improvement to attain and maintain level of service availability

6.2.2.8. Capacity Planning and Management

Capacity management at RNP will be required to ensure that IT processing and storage capacity provisioning match the evolving demands of the business in a cost effective and timely manner. Capacity Management Processes include Performance monitoring, Workload monitoring, Application sizing, Resource forecasting, Demand forecasting and Modeling.

RNP's Capacity Management Process will be designed to work in parallel with application, system development and project management including change procedures. Further, capacity planning and management is required

[10] Source: www.hci-itil.com/processes/AM.html
[11] Source: www.hci-itil.com/processes/AM.html

within all other IT Service Management processes and policies to conform to the best practices of the Information Technology Infrastructure Library (ITIL).

Capacity Management is a balancing act between costs and supply:

- Cost against Capacity – the need to ensure that processing capacity and storage purchased for a project is not only cost justifiable in terms of needs, but also makes the most efficient use of resources
- Supply against Demand – making sure that the available supply of processing power and storage meets the demand.

Following are the key considerations for the proposed RNP Capacity Management Process:

- For IT Service Management, ITIL v3 is the proposed framework and ISO/IEC 20000 is the proposed quality standard
- The Service Management tools are required to facilitate the data gathering for the Capacity
- All Capacity issues should be recorded, reported and open to inspection via audit
- All Capacity information is stored in a common repository and updated throughout its lifecycle
- Ministry of Interior will be accountable for ownership, monitoring, tracking and resolution of each capacity related issue
- A Capacity Plan must be a live plan which can be referred to for capacity changes
- A Capacity Plan must be updated in-line with Business Plans and associated requirements
- The Capacity plan should be under change control
- Anticipated changes shall be evaluated to determine their effect on current capacity levels

6.2.2.9. Forecasting and Budgeting

RNP will have defined forecasting and budgeting for the IT services, asset and infrastructure, processes and monitoring framework. Financial management for IT services is an integral part of service management. It provides the essential management information to ensure that services are rendered efficiently and economically. An effective financial management system will assist in the management and reduction of overall long term costs, and identify the actual cost of services.

This provisioning enables accurate and vital financial information to assist in decision making, identify the value of IT services, and enable the calculation of Total Cost of Ownership (TCO) and Return on Investment (ROI). The practice of financial management also enables the service manager to identify the amount being spent on security counter measures in the provision of the IT services.

6.2.2.10. Business Continuity Planning and Disaster Recovery Management

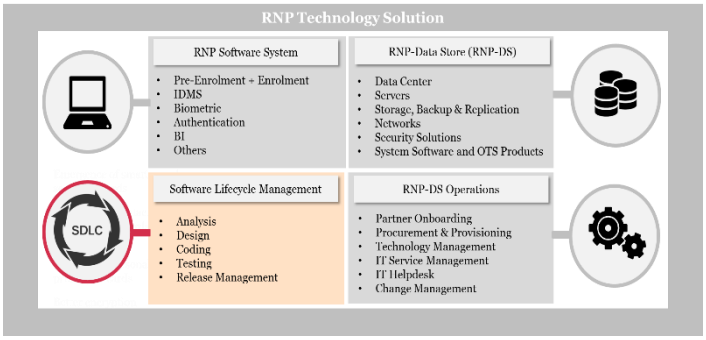
BCP or DRM is defined as the way of recovering from a disturbance to, or a destructive incident in regular business operations impacting the services. Key considerations for the proposed RNP DR are:

- DR site is required to provide a comprehensive IT infrastructure offering core services such as virtual environment, computing, network and connectivity, and other supporting services
- DR must have replication built-in feature, storage replications, etc. for each critical service and application
- The Primary and Secondary sites will be configured in Active/ Active (critical components) and Active/Passive as finalized in the technology solution in deliverable L4

- Both RPO and RTO will be discussed and agreed between RNP and System Integrator during the RFP stage
- Virtual servers for DR will be implemented to maximize the reliability and availability of the applications
- RNP will monitor and manage DR components 24x7
- A detailed disaster recovery plan must be in place for RNP to ensure that the processes and policies for handling the disaster situation and recovery models are followed for continuity in business operations and service delivery

7. Software Lifecycle Management

The RNP solution has been categories into 4 broad aspects i.e. RNP Software System, RNP-Data Store, Software Lifecycle, and RNP – DS Operations. This section covers the fourth aspect of the RNP solution i.e. Software Lifecycle Management.



This aspects deals with the entire lifecycle of software i.e. requirement gathering and analysis, solution design, solution development, solution testing and solution release management.

7.1. SDLC Overview

In this report, the RNP software system and RNP – Data Store have been describe in detail. The overview of methodology which may be adopted during the software lifecycle management is described in this sub-section.

For the software lifecycle management, an iterative model will be utilized. This model can be considered as multiple cycles of "waterfall" model. The cycles are divided into smaller and easily managed iterations. Each iteration passes through a series of phases, so after each cycle you will get a working software. The model is depicted in diagram given below.

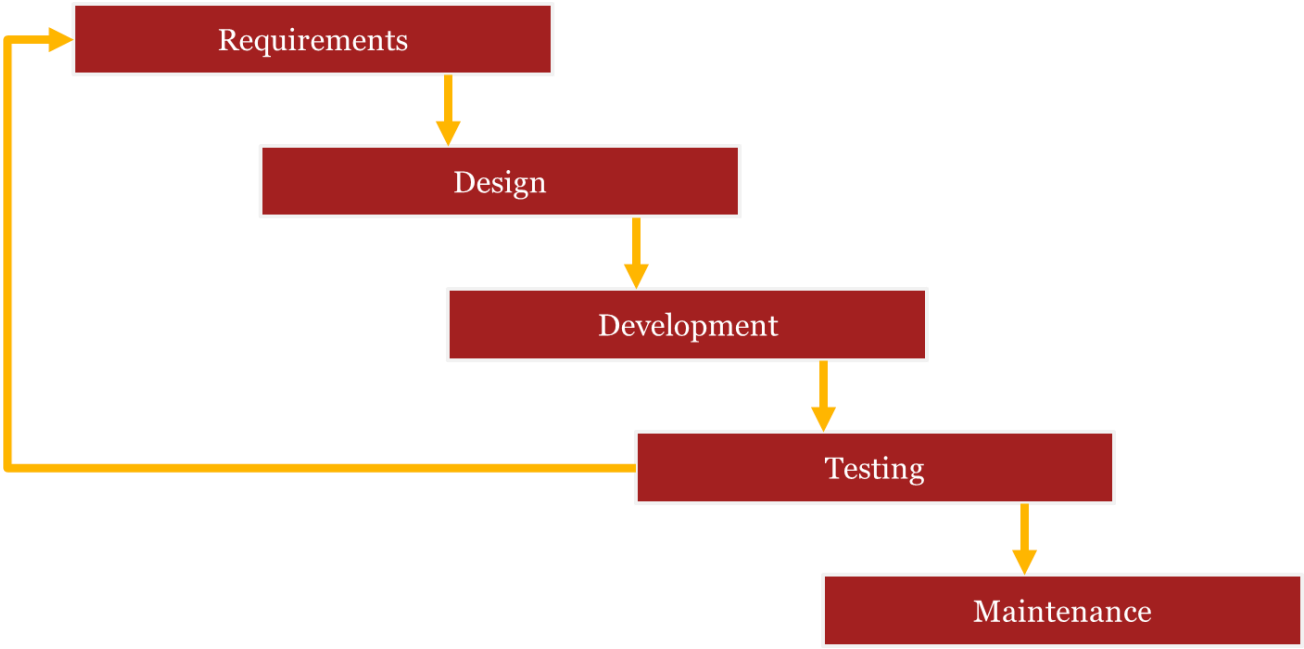


Figure 25 - Software Development Lifecycle

7.2. SDLC Management

The overview of methodology which will be adopted during the software lifecycle management described in the above sub-section. This methodology covering 5 stages has been covered in the detail in this sub-section.

7.2.1. Requirment Analysis

This step will cover a detailed assessment of the business and IT solution requirements. During this step, an exhaustive requirements gathering exercise will be carried out with the RNP team for understanding the requirements. These activities under this step will be carried out by the selected vendor(s). While doing so, the selected vendor(s) may be expected to do at least the following:

- Translate all the requirements into detailed Functional Requirement Specification (FRS) document
- Develop and follow standardized templates for capturing requirements and system documentation
- Maintain a traceability matrix from SRS stage onwards for the entire implementation
- Obtain the required sign-offs from user groups formed by the RNP

The functional details of the envisaged system will be covered in report on '*L4 - technical and functional requirements specifications for the computer systems*'. Thus, the selected vendor(s) shall have to study and adopt L4 as a starting point and fine tune the requirements. However, some of the requirements may undergo changes at the time of implementation. The selected vendor(s) may be have to accommodate such changes till the approval of requirements document by the RNP team. All major changes post this for each phase shall be handled through change control process.

7.2.2. Design

The RNP solution should be built in compliance with the design principles and other details mentioned in this document as well as in '*L4 - technical and functional requirements specifications for the computer systems*'.

A good design is important to achieve high reliability, low cost, and good maintainability. The designs will be carried out at two levels – High Level Design and Low Level Design. In the high level design, an overview of entire system will be developed specifying the main components and interfaces. A high-level design provides an overview of a system, product, service or process. This will be useful to identify critical components and interactions of all components. In the low level design, the components defined in the High Level Design will be refined for the purpose of actual software development. During this stage the selected vendor would be expected to deliver the following artifacts / documents:

- Detailed Application, Data and Infrastructure Architecture Definition Document
- A High Level Design Specification document including the GUI wireframes, UML use cases, UML designs, Conceptual Data Model, Logical & Physical Data Model for different application modules, API Specifications (Signature /Contract), Stored Procedures Specs etc.
- Low Level Design, where algorithms and logic of the important API's stored procedures etc. is detailed out
- Traceability matrices updated with design features against the requirements

7.2.3. Solution Development

In this step, the necessary software will be developed to meet the requirements gathered and design prepared as discussed in the previous section. As far as possible, the open source technologies and products may be utilized

for solution platform. In this phase of development, the development team would be constructing the different modules of the applications using the chosen languages/ tools. Development would be happening in parallel for different modules and wherever there is an integration need, manual stubs would be utilized so that there is no dependency on any other module and construction can happen seamlessly. In this stage the selected vendor would be required to deliver the following:

- Coding and Unit Testing Plans, guidelines and standards.
- Setup of a version controlled repository
- The complete code of the different modules using version control. These modules could be bespoke or customized OTS. In case of customized OTS the customized code would need to be shared in a version controlled repository
- Unit Test Results

The important aspects of this stage are provided below:

- **Development and Testing Environment**: Until the hardware required for the project is procured and installed, the development and testing environment can be hosted on temporary infrastructure on-site or off-site.
- **Processes**: While developing the application and carrying out on-going maintenance, the processes may be in compliance with CMMi Levels. The source code documentation should be done in a descriptive and intuitive manner using an easy to understand language.
- **Intellectual Property Rights (IPR)**: The ownership & Intellectual Property Rights (IPR) of the source code of the developed solution would be in the name of the Ministry of Interior. In case of a COTS product, the IPR of any customization done on the COTS product would be in the name of the Ministry of Interior.
- **User Friendly:** The application software developed by the Service Provider has to be user friendly so that users can access it without having extensive training.
- **Parallel Activities:** The lifecycle for each phase should be independent, i.e. different teams should work in parallel to complete the track activities per the given timelines.
- **Periodic Audit:** The periodic audits may be performed to measure license compliance against the number of valid End User software licenses and ensure consistency with the terms and conditions of license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions.
- **Supporting Tools and Accessories:** Any other tools & accessories required to complete the integrated solution per requirements may also be procured as part of the solution. For the integrated solution, the following may be required:
    - Software and licenses
    - Software Code
    - Tools, accessories and documentation
    - System Documentation (including licenses) both in hard copy and soft copy

As defined in this document, certain components of the solution will be developed afresh (bespoke development) while other components will be implemented by doing customization of OTS/COTS products. The list of such components is provided below:

Key Components	Bespoke Development	OTS/COTS Customization
Pre-enrolment Application	√	
Enrolment Software Application	√	
Identity Management System	√	
Identity Services Application	√	
Fraud Management	√	
Automated Biometric Identification System		√
RNP Web Portal and Mobile Application	√	
Business Intelligence and Analytics		√
Partner and Device Management	√	
Customer Relationship Management		√
Document Management System		√
Identity and Access Management	√	√
Knowledge Management	√	√

7.2.4. Testing

In this step, testing strategy including the traceability matrix and relevant test cases shall be finalized. Further, the testing will be performed for various components of the software developed/customized along with the solution as a whole. The testing will be comprehensive and will be carried out at each stage of development as well as implementation.

To ensure that the RNP system is performing as per the requirements and design, it is essential to carry out the testing. The demonstration of testing will be done prior to Go-Live as well as during project operations phase. For the acceptance of the developed solution, the acceptance criteria will have to be well-defined. A comprehensive system should be set up that would have the capability to log & track the testing results, upload & maintain the test cases and log & track issues/bugs identified.

The testing will be carried out in multiple phases as defined below:

- **System Testing**: A test plan will be prepared along with test cases. Using these test cases, the testing may be performed through manual as well as automated methods. For each phase of application development, comprehensive system testing may be performed.
- **Integration Testing**: In this type of testing, the individual software modules are combined and tested as a group. For this purpose, integration test plans and test cases will be prepared. The integration testing will be performed through manual as well as automated methods. Integration testing would include all data exchanged between various stakeholders. Integration testing would be performed for each phase of the application development.
- **Security Testing (including Penetration and Vulnerability Testing)**: To ensure that the solution is compliant with security requirements including security controls in the application, network layer, private cloud/data center infrastructure, and security monitoring systems this testing will be essential. The solution will pass vulnerability and penetration testing for rollout of each phase. The solution will also pass web application security testing for the portal and security configuration review of the baseline infrastructure. The security testing will need to be carried out in the exact same environment/architecture as the one set up for production. During the Operation and Maintenance phase

of the project, vulnerability assessment and penetration testing will need to be conducted on a yearly basis.

- **User Acceptance Testing**: The other forms of testing are performed by technical personnel, this testing is meant to be performed by actual users to ensure developed solution meets the functional requirements. This allows for any issues to be addressed before go-live. UAT is to be carried out in a similar environment as the one proposed to be set up for production. The issues and bugs identified during this step are fixed before the solution gets deployed in production deployment. The changes in the application as an outcome of UAT are not considered as a change request.
- **Performance and Load Testing (Benchmarking)**: The benchmarking exercise is intended at evaluating the ability of the RNP solution/architecture to scale up to the intended usage. The benchmarking process does not intend to simulate all the aspects of RNP Solution. However, all the design parameters, all components and related interfaces shall be considered during benchmarking. The benchmarking shall be performed within the data center for pre-defined volume. The solution benchmarking shall be as per the production deployment and solution architecture.
- **Mobile Testing**: This exercise is essential to check the integration, security and performance of the mobile applications that would be developed for RNP. Since the client in the mobile app is a rich client with multiple components, residing on the mobile device/Smartphone/Tablet, this testing becomes important. Some of the key areas of consideration while testing this are mobile security, ability to cleanup mobile devices for lost mobiles, etc.

7.2.5. Release Management

The release management is used for the distribution of people, documents, software and hardware across the entire solution. The release management ensures that software and hardware are licensed, tested, and certified. Thus, the released software and hardware is assured to function as intended when introduced into the production environment.

The goal of release management is to maintain and protect the production environment. Release management controls the release of new configuration items (people documents, software and hardware) into the production environment. The following are the high level activities:

- Plan releases as per the requirements for the approved changes
- Build release packages for the deployment for approved changes (one/many) into QA/Staging /production
- Design, test and implement procedures (mechanisms) for the distribution of approved changes to QA/Staging /production environment
- Effectively communicate and manage expectations of the customer/internal stakeholders/end customer during the planning and rollout of new releases
- Monitor, Control, and Report the distribution and installation of changes to all concerned stakeholders.
- Deploy the release as per guidelines

For the release, the following process may have to be defined:

- Release Planning Process
- Release Building Process
- Release Testing Process
- Release Deployment Planning Process

- Release Deployment Process
- Enrolment Software Release Management Process
- Server Release Management Process

7.3. Continuous Build

The RNP system development should be highly modular and parallel development should be carried out for faster execution. All application modules within the same technology platform should follow a standardized build and deployment process. There should be instrumental process or tool to also capture the end user behavior like the response time, browsing history, etc.

The application is to be developed, tested and released that adhere to:

- Smaller batch sizes
- Automated testing
- Rollback procedures
- Continuous integration
- Continuous deployment
- Test driven development

Following are some of the requirement to manage the development process along with virtualization of services:

- A dedicated 'development / customization' environment should be proposed and setup. Separate development and testing environment for application development and testing should be taken into account. There should be sandbox environment to test the APIs. Any change, modifications in any module must follow industry standard processes like change management, version control and release management in large and complex application development environment.
- Should be able to create complete, scalable environment for the design and deployment of virtual services for use across co-located and distributed development and testing teams.
- Application source code could be maintained in version control and could be broken up into a number of projects. Source control projects are created to abstract related set of modules or feature that can be independently included in another application.
- Should be able to simulate delayed asynchronous responses with a transactions per second (TPS) metric using Performance Batch Simulation.
- It is mandatory to create, update and maintain all relevant documentation throughout the contract duration
- Should enable unit, functional and load testing against virtual services.
- Should have support for end-to-end testing of virtual services with integration to proposed testing solutions.
- Should be able to modify data, network, and performance models easily according to changes in test conditions and performance needs.
- Should be able to create simulations of real-world application behavior.
- Should be able to expose virtual services for parallel development and early functional testing.
- Should be able to define and visualize topology diagrams to understand dependencies and boundaries of underlying systems on the level of remote API calls.

- Should ensure that a bug tracking tool is maintained for proper tracking of all bugs fixes as per various tests conducted on the application
- Should be able to virtualize database access, including Java Database Connectivity (JDBC), and manipulate resultant virtual data services.

7.4. Container Architecture

For development and deployment, the container based architecture is proposed for seamless application development & deployment. Components should be developed as micro services.

Service provider should use a Container Architecture tool for entire development life cycle for example, developing, shipping, and running applications. With container architecture, the developer teams can separate the applications from the infrastructure and treat the infrastructure like a managed application. It can also help to ship code faster, test faster, deploy faster, and shorten the cycle between writing code and running code. It allows the developers to develop on local containers that contain the applications and services. It can then integrate into a continuous integration and deployment workflow. The following objectives can be achieved by a Container Architecture:

- Faster delivery of the applications
- Easy Deployment and scaling
- Achieving higher density and running more workloads

8. Enterprise Reference Model for RNP Solution

The overall Enterprise Reference Model for RNP-Morocco is shown under. This represents a single view of the key components of the RNP Enterprise including some of the future components of Morocco Stack.

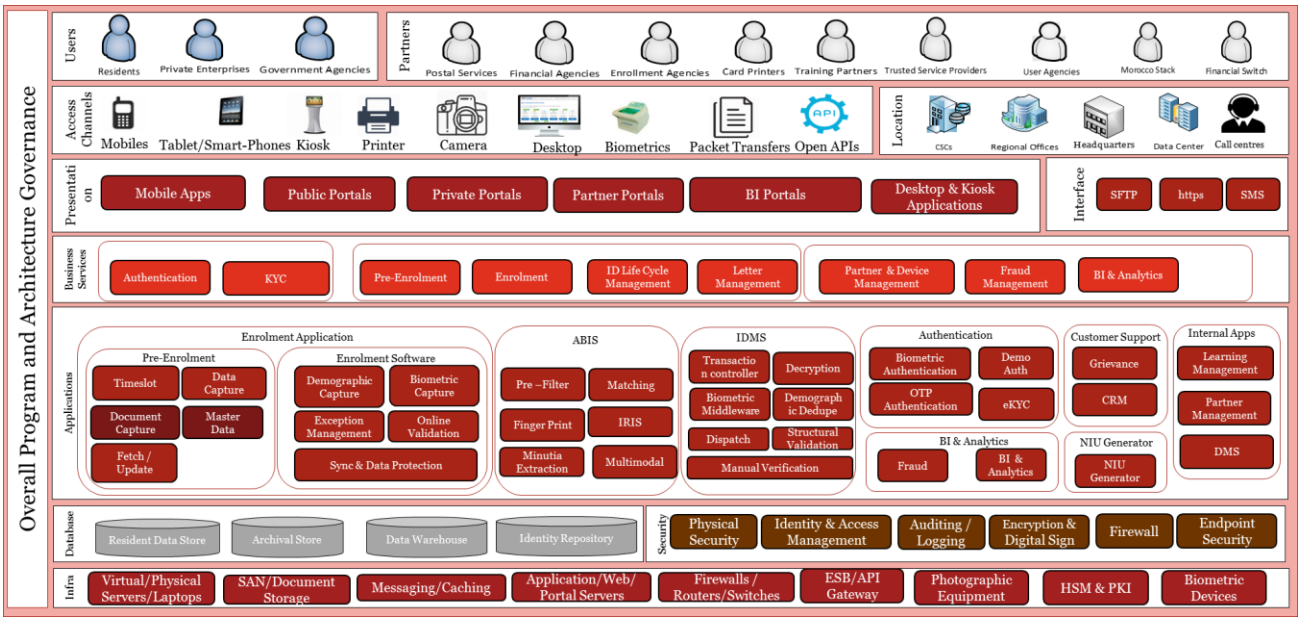


Figure 26: Enterprise Reference Model for RNP System

The main layers that need to integrate well for the overall success of the RNP-Program are shown in the diagram

1) Users
2) Partners
3) Access Channels
4) Locations & Physical Infrastructure
5) Presentation Layer
6) Interface layer
7) Business Layer
8) Application Layer
9) Data Layer
10) Security Layer
11) IT Infrastructure
12) Overall Governance

9. Assumptions and Parameters for Sizing

For the purpose of sizing of infrastructure for the program, the parameters have been defined. For these parameters, a high level estimation has been carried out. In some cases, the assumptions have been made.

9.1. General Statistics

Parameter	Description	Sizing Estimations
Current Population	Estimated Population in 2018	35.2 million (Source: Census 2014)
Estimated Population	Estimated Population in 2028	38.7 million (Source: Census 2014)
Annual Growth (%)	Net growth rate (birth minus death)	1.22%
Annual Birth Rate (%)	Number of Birth in 2018	Annual Birth Rate (17.6 / 1000)
Annual Death Rate (%)	Number of Death in 2018	Annual Death Rate (5.4 / 1000)
Average No. of Births	Annual number of births in the period 2018-2028	600,000 per annum (Source: Census 2014)
Average No. of Deaths	Annual number of deaths in the period 2018-2028	200,000 per annum (Source: Census 2014)

9.2. Estimation of Enrolments

Parameter	Description	Sizing Estimations
Biometric Enrolments	Number of Registration carried out till now	Yet to start
Enrolment Duration	Time to cover entire 85% population	May 2021
Enrolment Target	Entire Population	36.13 million (as on 2021)
Annual New Enrolments	After one-time coverage	Annual Birth Rate (17.6 / 1000)
Annual Existing UIN Deactivations	After UIN generation (due to deaths)	Annual Death Rate (5.4 / 1000)
Biometric Updates	At 5 years	0.60 million per annum
Biometric Updates	At 15 years	0.64 million per annum

Parameter	Description	Sizing Estimations
Demographic Updates	Change in demographic details	1,750,000 per annum (5% of Population)

9.3. Estimation of Authentication and e-KYC requests

Parameter	Description	Sizing Estimations
Authentication	Daily Authentication Requests	650 million per annum @ 1.8 million per day [5% of population]
Authentication Example 1	Tayssir Authentications in schools on a daily basis	185 million per annum [estimated as 0.74 million (per day) x 250 working days]
Authentication Example 2	RAMED Authentications at hospitals	22.8 million per annum [estimated as 7.6 million x 3 visits per person per year]
Authentication Example 3	DAAM Authentications	0.31 million per annum [estimated as 0.077 million beneficiaries x 4 times per year]
KYC	Daily KYC Requests	650 million per annum @ 1.8 million per day [5% of population]
e-KYC Example 1	Banks	0.17 million per annum [assumed as 17 million accounts x 1% growth rate]
e-KYC Example 2	Banks	0.35 million per annum [assumed as 2% coverage of new bank accounts under Financial Inclusion on annual basis]
e-KYC Example 3	Telecom	0.2 million per annum [increase in number of mobile connections on annual basis]
e-KYC Example 4	Government and Private Sector	20.00 million per annum [assumed as 5% of the population per month]

9.4. Sizing of Packets for Enrolment and Identification Services

Parameter	Description	Sizing Estimations
Size of Biometric Packet	Demographic, Photograph and 10-Fingerprint in raw form	8 MB is 6 MB Raw Packet +2 MB for document scan
Authentication Packet		3-5 KB/ 30-35KB
eKYC Packet		30 KB

9.5. Estimation of Users

Parameter	Description	Sizing Estimations
Total User	Total Number of Users	150 Users
Kit Operators	Field Operators	2000
	Working Hours	8 hours x 22 working days per month
Verification	CNIE Verification	10 per shift
	Working Hours	8 hours per shift x 2 Shift
Adjudicators	Manual Adjudication	10 per shift
	Working Hours	8 hours per shift x 2 Shift
Contact Centre	Helpdesk Personnel	10 x 2 Shift
	Number of Supervisors	1 (First Shift) + 1 (Second Shift)
	Contact Centre Seats	11 (minimum)
	Waiting time	2 Minutes (maximum)
	Working Hours	8 hours per shift x 2 Shift
IT Helpdesk	Helpdesk Personnel	5 (First Shift) + 5 (Second Shift) + 2 (Third Shift)
	Number of Supervisors	1 (First Shift) + 1 (Second Shift)
Network Operations Centre	Number of Users	3 (First Shift) + 3 (Second Shift) + 1 (Third Shift)
	Working Hours	8 hours per shift x 3 Shifts
Security Operations Centre	Number of Users	3 (First Shift) + 3 (Second Shift) + 1 (Third Shift)
	Number of Supervisors	1 (First Shift) + 1 (Second Shift)
	Working Hours	8 hours per shift x 3 Shifts
Administrators	DBA, Network Admin, Server Admin, Storage Admin, etc.	21 (DC) + 4 (DR)
	Working Hours	8 hours per shift x 3 Shift
Internet Subscriber	No. of Internet Users	22.5 million (September 2017)
	No. of Internet Users	16.9 million (September 2016)
	Annual growth rate	Annual growth of 33% (10 years)
Estimated Users	No. of Internet Subscribers	10% of Internet Subscribers
Concurrency Citizen	Concurrency of Internet Users	2.5% of estimated users
Permanent Service Centres	Citizen Service Centres	2000

Parameter	Description	Sizing Estimations
Workload Volume	Number of Registrations Per Day Per Kit	30 enrolments (One enrolments in 15 minutes x 8 hours)

9.6. Technical Parameters

Parameter	Description	Sizing Estimations
Network Connectivity *(For future usage the router sized for 2-5 Gbps is recommended)	Network Connectivity (DC-DR Replication Link)	Initially 1 Gbps connectivity between DC and DR x 2 lines*
	Network Connectivity (Enrolment Users + Pre-Enrolment) at the Data Centre	Initially 1 Gbps internet connectivity*
	Network Connectivity (Auth., eKYC) at the Data Centre	Initially 100 Mbps leased line
	Network Connectivity (Web Portal) at the Data Centre	Initially 100 Mbps internet connectivity
CPU	Utilization upper limits	60% only for non-ABIS component
Re-size/ headroom	Virtual Cores, Memory, and Storage Seamlessly	25% of the base capacity, only for non-ABIS components in permanent Data Centre
Storage	Static & Transaction data	4,100 TB
Reports	Total	25 types of reports
	Break-up	5 Complex Report Type, 10 Medium Report Type, 10 Simple Report Type
Communication with External Systems	External interfaces that are likely to interact with the RNP System	Private Sector (Telecom Companies, Banks, etc.), Government Departments (Transport, Tax Revenue, Immigration, etc.), and Benefit Programs (RAMED, Tayssir, DAAM, etc.)
RTO and RPO	For Pilot, the DC-DR will be in same city. Subsequently, the DC and DR will be more than 100 KMs apart	Annexure-III
Online data retention	NID Data	Always
	Biometric Centre data	Always
Backup window	Incremental data back up every day and full back up every week	6-8 hrs

10. Annexures

10.1. Annexure-I: Consent Procedure

10.2. Annexure-II: Whitelisting procedure of Enrolment Officers

10.3. Annexure-III: RTO and RPO

S. No.	Process	Criticality	RTO	RPO	Business Rationale for RPO and RTO
1	Enrolment	High	24 hours	~ZERO	**RTO:** Enrolment is an offline process and officers are required to upload packets once a day hence 24 hrs. is affordable **RPO (Enrolment Databases):** It is a business requirement that no data shall be lost in the ecosystem (IDMS and enrolment agencies)
2	Authentication	High	~ZERO	~ZERO	**RTO:** Authentication is an online process and it is anticipated that majority of government and private organizations in Morocco will use this service to be able to provide further services. Hence RTO is 0 **RPO (Authentication databases including logs):** It is a business requirement that no authentication data shall be lost
3	Critical Portals	High	~ZERO	~ZERO	**RTO:** These portals could be resident facing and any downtime could have major reputational impact **RPO (Logs databases and enrolment, Authentication databases):** It is a business requirement that no data is lost from the logs database. Authentication and Enrolment databases also have ~ZERO RPOs
4	CRM	High	~ZERO	~ZERO	**RTO:** CRM is a resident facing service and any downtime could have major reputational impact **RPO (CRM database, call recordings etc.):** It is a business requirement that no data is lost from the CRM databases and maintenance of the databases also may be necessary for compliance to legal requirements.

S. No.	Process	Criticality	RTO	RPO	Business Rationale for RPO and RTO
5	SOC	High	~ZERO	~ZERO	**RTO:** SOC is a very important security operation for IDMS. SOC should never be down as logs from various devices are collected by SOC tool and it is important that logs are always available for investigation purposes **RPO (Logs file system, SOC configuration etc.):** It is a business and legal requirement that logs are always available
6	Email	High	~ZERO	~ZERO	**RTO:** Email is very critical service as lot of other services depend upon email such as email to residents when UIN generated or when resident authenticates **RPO (Emails):** Email is a very critical service and lot of internal and partner communications take place on email hence it is a critical service.
7	Other Portals	Medium	~ZERO	~ZERO if data other than logs ~24 hrs if only logs	**RTO:** It is understood that these portals are not resident facing and criticality **RPO (Logs databases and enrolment, Authentication databases):** It is a business requirement to ensure there is no data loss in case data other than logs is present.
8	NOC	Medium	~ZERO	~24 hrs.	**RTO:** It is understood that NOC is an important process to monitor the availability of service **RPO (Ticketing database etc.):** Ticketing database is not a critical database and hence loss of 24 hrs. of tickets can be afforded
9	Office	Medium	24 - 48 hours	N/A (No data is stored)	

10.4. Annexure-IV: Manual Adjudication Process

10.5. Annexure-V: Structural Validations

10.6. Annexure-VI: Use of Virtual ID in Authentication Services