Aspire to Innovate (a2i)

Government of the People's Republic of Bangladesh

ICT Division

Agargaon, Dhaka

Terms of Reference

For

"Hiring a firm for enhancement, support and maintenance of Smart Doptor platform"

Table of Contents

1. Background

The Government of Bangladesh is committed to modernizing its administrative landscape through the integration of technology, aiming to enhance the efficiency, transparency, and accessibility of public services. In line with this vision, the Doptor Platform is undergoing a significant enhancement to meet the evolving needs and technological advancements complying with the **ICT masterplan 2041**. This transformation includes integrating features like suggestion systems, efficient scheduling, task management, secure identity control, and seamless information sharing, also aligns with the objective of creating a Smart Bangladesh by leveraging emerging technologies such as AI/ML, blockchain, and data analytics.

The suggestion systems, driven by AI, provide valuable insights to help government officers make better decisions. The scheduling tool organizes tasks and meetings for improved productivity, while efficient task management ensures optimal workflow.

Secure identity management guarantees authorized access to data, ensuring confidentiality. Additionally, an information mediator simplifies data sharing and communication within the office environment.

The envisioned enhancement focuses on creating a feature-rich and intuitive Central Dashboard module within the Doptor Platform. This module aims to provide government offices and officers with a consolidated and streamlined interface, integrating critical information and functionalities in one central hub. The Central Dashboard module is designed to facilitate quick access to essential services, present insightful data visualizations, deliver real-time notifications, and enable seamless integration with other modules.By providing a unified view and quick access to core functionalities, the Central Dashboard module will play a pivotal role in the digitization journey of the government, contributing to a more efficient and responsive public administration.

The successful implementation of the Central Dashboard module will not only elevate the Doptor Platform's functionality but also contribute to the broader goal of building a Smart Bangladesh by leveraging technology to empower its public sector. This transformation is a step towards an integrated and tech-enabled governance system, ensuring a more effective and citizen-centric administration for the nation.

In essence, integrating these smart office features into the Doptor Platform represents a significant step towards a modernized and efficient governance approach, empowering government offices and officers for smarter and quicker operations.

2. About the organization & Review of the Existing System

2.1 About the organization

a2i, a multinational digital transformation organization founded in Bangladesh, accelerates the inclusive digitization of public services thereby widening access and decentralizes delivery. It evolved from the flagship Aspire to Innovate program of the government’s Digital Bangladesh Vision 2021 initiative, supported by UNDP. Bangladesh now aspires to become a prosperous, developed, poverty-free and equitable nation with its bold ‘SMART Bangladesh Vision 2041’ – an aspirational strategic plan to transform the economy to reach High-Income Country status by 2041 and achieve the 2030 Sustainable Development Goals along the way.

Vision 2041 builds on Bangladesh's remarkable journey towards mass, citizen-centric digitization over the past 13 years. At the heart of this development journey lies a simple yet powerful idea: that creating shared prosperity isn't possible unless administrative, financial, and political power is decentralized at the grassroots level. That is, unless all citizens are truly empowered.

Soon to be formally established as Bangladesh's national innovation agency, a2i builds on the Government of Bangladesh's efforts to champion the cause of 'digital equity' and fosters an adaptive, national system for collective strategizing, planning, action and learning to catalyze truly unprecedented transformations in public service delivery. It also works as an innovation intermediary through a 'whole-of-government' approach and supports the government to be on the forefront of integrating new, mission-driven innovation policy and whole-of-society approaches to achieve the SDGs. Through UNDP's Accelerator Labs network, and by leveraging the South-South Network for Public Service Innovation,, a2i is also working to support the digital progress of other least developed countries (LDCs) and many developing countries including Fiji, Jordan, the Maldives, the Philippines, and Yemen with funding, advice and technologies.

2.2 Existing System

1.2 Review of the Existing System

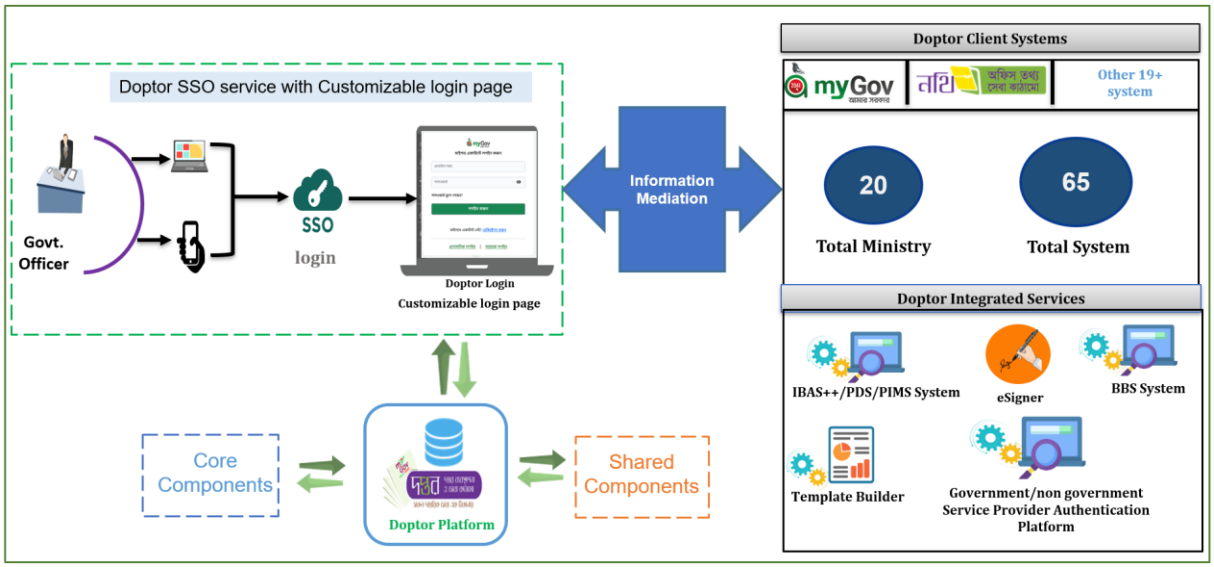


Figure : Doptor Existing High Level Architecture

1.2.1 The section provides brief description of existing system for better understanding:

Please see: ANNEXURE 01 (Page - 78)

1.3 Intended Audience

- **Government Offices:** Ministries, Directorate, departments, agencies, and entities across Bangladesh who are responsible for managing and delivering government services, internal systems such as PIMS.

- **Government Officers and Employees:** Officers and employees at different levels of government hierarchies who interact with the platform for workflow management, decision-making, and service provisioning.
- **IT Administrators and Support Teams:** IT personnel responsible for maintaining, troubleshooting, and optimizing the platform's performance and security.

1.4 Technology Platform of existing system

Application

Platform	Web Application
Programming Language	PHP, Laravel 8
Client-Side Script	JavaScript, JQuery
Style Sheet	CSS, CSS3, HTML5 & Bootstrap
Other	AJAX (Asynchronous JavaScript XML) JSON (JavaScript Object Notation) XML (Extensible Mark-up Language)
Object Oriented Programming	PHP
Framework	Laravel & CakePHP
Database	MySQL 5.7 (Percona cluster)
Cache Server	Redis
Load Balancer	NGINX, HAPROXY
Operating System	Debian, Ubuntu
Security Tools	Burp Suite
API Manager	Kong 3.3.0
Queue Manager	Laravel Queue
Monitoring Tools	iTOP, LibreNMS

2.3 Terminology

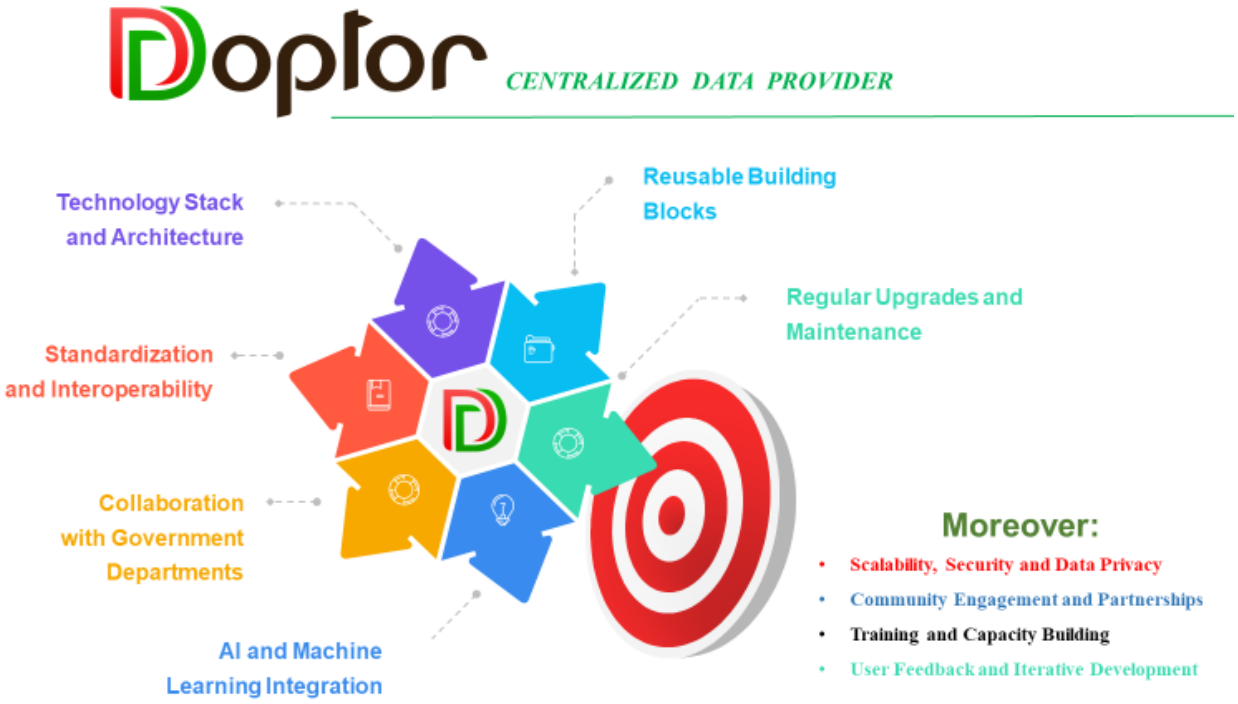
Core services: Core Services provide the foundational functionalities required for day-to-day operations **within government offices**. Example: identity management, user authentication, access control, data storage, and basic communication infrastructure And also employee information (e.g., profiles, roles), office information (e.g., organograms, locations)

Shared Services: Shared Services enable efficient **data sharing and collaboration among different government entities**, aligning with the goals of the Doptor Platform to streamline government processes and enhance service delivery. Example: payment gateways, geolocation services, notification services, APIs for data sharing, integration with external systems, standardized communication protocols, and tools that enhance collaboration among government entities.

Service market Place: Service orchestration is the automated arrangement, coordination, and management of computer-based services, middleware, and network services. The aim of service orchestration is to help automate the coordination and management of multiple software applications into a single, cohesive, and end-to-end IT service.

3. Proposed System

3.1 Objectives



The overall objectives of this assignment will be the following:

1. Ensure scalability, interoperability, and sustainability of the platform to adapt to future technological advancements and expanding user requirements.
2. To position the Doptor Platform as a centralized data provider, facilitating seamless data sharing and utilization across all government departments and agencies.
3. To integrate and consolidate as many existing digital platforms and services as possible to provide a unified and centralized experience for users. This would involve collaborating with different government departments and agencies to bring their services under the single umbrella.

4. To explore the integration of emerging technologies like artificial intelligence & machine learning to enhance the functionality and efficiency of the Doptor platform. These technologies can automate processes, provide intelligent recommendations, and deliver personalized services to users.
5. To develop reusable building blocks that allow the Doptor modules to be utilized as standalone components or integrated into other government systems. This would promote interoperability and efficiency by enabling seamless integration of Doptor functionalities and services into various government applications, fostering a modular and scalable approach to system development.
6. To establish a regular upgrade and maintenance cycle to ensure that the platform remains up to date with the latest technologies, security patches, and user requirements.

3.2 Scope

The firm will be required to complete the development and deployment of the Doptor platform as an application following the SDLC methodology and perform the relevant activities accordingly within a proposed stipulated time.

The ultimate scope of this e-Government solution of a2i is to design, develop, and implement an integrated service delivery platform for all the Government systems and solutions. For detailed clarification and understanding the required high-level functional scope of major features are described in the "**Functional Requirement**" part below. Covering all the possible scopes, firms may propose their best architecture and service delivery solution for this system in their technical proposal.

Apart from this, this system's scope is described hereunder from the high-level perspective.

3.3 Functional Requirements (Development & Enhancement)

This section provides a brief scope of the project. Detailed and more accurate scope can be identified after in-depth business analysis and scope of the work may fluctuate from this brief scope explained within this section.

3.3.1 Enhancement of existing Core service framework & Core Service and Shared Service Management

Existing Feature:

- The core service framework provides office related common services like – GEO, Office, organogram, employee profile etc. So that it is capable of serving all perspectives along with retrospective eService requirements.
- Capacity to have a change log with history (GEO, Office, Employee, Organogram etc.)
- Developed 34+ APIs (https://doptor.gov.bd/blog/api-documentation-v1)

Enhancement:

- An upgraded framework built with modern technologies, ensuring compatibility with future needs.
- Updated and new API endpoints that facilitate better data sharing and integration with external systems.

- Enhanced scalability and performance through code optimization and caching mechanisms.
- Updated documentation and training materials(AV and Text) for government employees and developers.
- A well-defined migration plan to transition existing services to the upgraded framework.
    - Employee record (Service ID,etc)
    - Office data (Office code, BBS code , web Url,etc)

3.3.2 SSO, SLO and Access Management:

SSO simplifies the login experience, SLO ensures secure logout from multiple applications, and Access Management controls what users can do once authenticated. These components are essential for enhancing both user convenience and security in modern identity and access management systems.

Existing Features:

- OpenID Connect SSO implementation.
- Single Logout (SLO).
- Federated SSO via OpenID with external identity
- Introduce support for multi-option/multi-step authentication
- 2-factor authentication (2-FA) (hardware based or soft OTP)
- Time-based one-time password (OTP) based authentication
- Users and Group Management
- Introduce Account recovery with email and secret questions
- Introduce Password history validation
- Password pattern configuration
- Introduce account locking in single and multi-tenant environments
- Introduce account suspension reminders and locking of idle accounts
- Should have proper monitoring, reporting and auditing support by providing login events and session monitoring, user session termination, forced password reset and real-time security alerting for suspicious login activities and abnormal sessions based on rules
- System should provide flexible deployment mechanism by supporting clustering for high availability deployment and centralized configuration management across different development environment
- Sign in facility Mobile apps for both Android & iOS.

Enhancement:

- Implement at least two **MFA** methods (e.g., OTP, biometrics) for user authentication.
- Ensure adaptive authentication and a secure fallback mechanism for uninterrupted access.
- Comply with security standards, provide error handling, and log **MFA** events for auditing.
- Enforce strong password policies (e.g., complexity requirements, expiration) to enhance overall security.

- Implement a comprehensive logging system to track user activities and access attempts for auditing and compliance purposes
- Develop functionalities for users to manage their profiles, including password changes, profile pictures, etc.
- Integrate with external identity providers (e.g., Google, Microsoft) to enable easier and more secure login options.
- Implement secure session handling mechanisms, including session timeout and secure session termination.
- Develop a robust RBAC system to control access based on predefined roles and permissions.
- Regularly update the module to address any security vulnerabilities and ensure the latest security measures are in place
- Conduct compatibility checks with various browsers and platforms to ensure a consistent user experience.
- Continuously optimize the module for improved performance and responsiveness.
- Provide timely technical support and assistance to address any access management-related queries or issues.
- Offer training and assistance to users and administrators on effectively utilizing the access management module.
- Resolve access management-related issues, bugs, or glitches in a timely and efficient manner.

New Development:

- Implement secure multi-channel authentication options (e.g., email, SMS, biometrics) for **passwordless access**.
- Develop a robust token-based authentication system with secure token generation and adaptive contextual authentication.
- Ensure compliance with security standards, error handling, logging, and protection of token-related data.

Deliverables:

- MFA module and setup interface for users and administrators.
- Comprehensive documentation, testing artifacts, and training materials.
- Integration guidelines and a support/maintenance plan for ongoing effectiveness.
- Passwordless login module integrating multiple authentication channels.
- User-friendly interface modifications to support the passwordless login flow.
- Comprehensive documentation, testing artifacts, training materials, integration guidelines, and a support/maintenance plan.
- Upgraded module incorporating all specified features and improvements.
- Detailed documentation covering setup, configuration, and usage of the access management module.
- Detailed test plans, test cases, and testing reports to ensure the reliability and security of the module.
- Training guides and materials for users and administrators to effectively use the access management module.

- Guidelines for integrating the Access Management Module with other components of the Doptor platform.
- Detailed plan outlining the provision of technical support, regular updates, performance optimization, and issue resolution.

3.3.3 Central Dashboard:

One dashboard for all systems. It will be a configurable dashboard which will connect all of the authorized systems/platforms as well as the government office and officers.

The Central Dashboard is a central hub for users within the Doptor platform. The dashboard also offers access to account settings for easy management, consolidates essential information and functionalities for government offices and officers. It will be designed to ensure Streamline access to vital data, Enhance decision-making and Improve operational efficiency. Dashboard will provide easy access to multiple systems, solutions, or applications, improving efficiency by streamline operations and enhancing user experience.

Existing Features:

- Role Based Dashboard for Office and User

New Development:

- **Integration**

Central dashboards often integrate with various data sources and systems, such as databases, APIs, third-party applications (i.e. X-ROAD® and other applications), and hardware devices. This integration allows for comprehensive data gathering and management.

- **Search Functionality**

A search feature can help users quickly locate specific data points or information within a large dataset.

- **Real-Time Data Visualization:**

Implement real-time data visualization features to provide instant insights and analysis of key metrics, helping in timely decision-making.

- **Predictive Analytics Integration:**

  Integrate predictive analytics capabilities to forecast trends and future scenarios based on historical and current data, aiding in proactive decision-making.

- **Personalized User Dashboards:**

  Develop a system that allows users to customize their dashboards, tailoring them to their specific roles, responsibilities, and preferences.

- **Advanced Reporting:**

  Implement advanced reporting features to generate detailed, customizable reports that can be shared or exported for further analysis.

- **Data Security and Privacy:**

Prioritize robust data security measures to ensure that sensitive government data displayed on the central dashboard is protected against unauthorized access.

- **Smart Assistance:** Smart assistants, also known as virtual assistants or digital assistants, are software applications or devices that use artificial intelligence (AI) and natural language processing to provide various services and perform tasks for users.

  The dashboard will suggest users for their regular activity according to the previous settings.

Deliverables:

- **Real-Time Data Visualization**: Central dashboards typically display real-time or near-real-time data in the form of charts, graphs, tables, or other visual representations. This data could include key performance indicators (KPIs), metrics, alerts, and system status.
- **Customizable Widgets**: Users often have the ability to customize the dashboard by adding, removing, or rearranging widgets to suit their specific needs. Widgets can display different types of information, such as integrated systems, traffic analytics, user statistics, system health, etc.
- **Alerts and Notifications**: Dashboards can provide alerts and notifications when predefined thresholds or conditions are met. These alerts can be crucial for proactive issue resolution and monitoring.
- **Data Filters and Drill-Down**: Users should be able to filter and drill down into the data to get more detailed information about specific aspects or time periods. This feature helps in root cause analysis and problem-solving.
- **Predictive Analytics Integration:**
  Integration of predictive analytics models to provide future insights and forecasts based on historical and current data.
- **Personalized User Dashboard Functionality:**
  Functionality allows users to personalize their dashboards, selecting the data and metrics most relevant to their roles and activities.
- **Smart Assistance:**
  - Development and integration of the smart assistance module into the platform.
  - Development of a personalization engine that tailors content and recommendations based on user behavior.
  - Integration with popular virtual assistants (e.g., Siri, Alexa, a2i selected) for voice interactions.
- **Mobile-Responsive Dashboard:**
  A mobile-optimized dashboard ensures seamless user experience and access to critical data on mobile devices.
- **Advanced Reporting Capability:**
  A reporting feature capable of generating detailed, customizable reports for in-depth analysis and decision-making.
- **User Access Control**: Depending on user roles and permissions, central dashboards should ensure that users only have access to the data and functionalities that are relevant to their responsibilities.

- **Integration**: Central dashboards often integrate with various data sources and systems, such as databases, APIs, third-party applications, and hardware devices. This integration allows for comprehensive data gathering and management.
- **Search Functionality**: A search feature can help users quickly locate specific data points or information within a large dataset.
- **Data Export:** Users may need to export data from the dashboard for further analysis or reporting purposes. Export options could include CSV, Excel, PDF, or other common formats.
- **User-Friendly Interface:** The dashboard should have an intuitive and user-friendly interface to make it accessible to a wide range of users with varying levels of technical expertise.
- **Security Features**: Security is paramount in central dashboards. This includes encryption, authentication, and authorization mechanisms to protect sensitive data and ensure that only authorized users can access the dashboard.
- **Scalability**: The dashboard should be able to scale to accommodate growing data volumes and user loads.
- **Dashboard Sharing**: Users may need to share specific views or reports from the dashboard with colleagues or stakeholders. Sharing features can facilitate this process.
- **Documentation and Help Resources:** Providing documentation and help resources within the dashboard can assist users in understanding its features and functionality.

3.3.4 Identity Management

The primary function of Uniform Identity Management is to establish a unified identity system for government officers based on their grading system and service category. This system will facilitate seamless internal and external office communication, ensuring clarity and efficiency in all interactions.

By implementing Uniform Identity Management and the Ranking System, the Doptor platform will enhance communication, streamline interactions, and ensure that the proper protocol and precedence are maintained, contributing to a more efficient government ecosystem.

Existing system:

Currently Doptor provides a 12 digit service ID for Cadre , Non Cadre , Political Figure, Uddokta (Entrepreneur).

New Development:

Unified Identity Creation: Create a centralized identity for each government officer with unique identification credentials. Collect and store essential information, including name, designation, contact details, and service history.

Grading System Management: Implement a grading system that categorizes officers based on their rank, experience, and service tenure. Assign appropriate badges, designations, and privileges based on the grading system.

Service Category Management: Classify officers into service categories (e.g., administrative, technical, legal) for targeted communication and access control.

User Profile Customization: Allow officers to personalize their profiles with optional details such as profile pictures, professional achievements, and contact preferences.

Ranking System Management: Integrate the Warrant Of Precedence, 1986 (Revised up to July, 2020) to assign official rankings and precedence to officers.

Rank Display: Display the official rank of officers in all communication channels, emphasizing the ranking system's importance.

Inter-System Compatibility: Ensure compatibility with other government systems for seamless data exchange. Implement secure APIs for connecting with different systems.

Deliverables:

Uniform Identity Management System: A fully functional system for creating and managing unified identities for government officers.

Grading and Ranking Module: An integrated module that categorizes officers into grades and assigns official rankings as per the Warrant Of Precedence.

User Profiles: User-friendly profiles for officers to manage their identity and personalize their information.

API Documentation: Comprehensive documentation for APIs, enabling integration with other government systems.

3.3.5 Digital Service Standard Portal

The future development of the Digital Service Standard Portal in the Doptor platform aims to elevate the user experience, content management, and security of standards and guidelines. These advancements align with the objective of creating a more efficient and technologically advanced e-governance ecosystem.

Existing Features:

- Portal contains relevant information of integration guidelines to minimize in-person knowledge sharing for integration works.
- The Portal has a standard and document uploading panel using HTML structure and also using proper DDL.
- The Portal has its own document/content management system from the admin panel where documents can be listed/uploaded using various filters. Users with proper permission will be able to modify/remove standard and guideline documents as needed. Also, for each revision, the system should track versioning properly.
- The Portal has management dashboard and usage analytics and shares the data to the stakeholders and administrators
- The Portal provides an efficient search mechanism to allow users explore their queries navigating through different standard catalogs or tools of interest allowing options like keywords, different types of filters.

New Development:

- **Enriched User Experience**:

Enhance the portal's user interface and experience to be more intuitive, engaging, and user-friendly, facilitating efficient navigation and content consumption.

- **Advanced Integration Guidelines**:

Provide comprehensive integration guidelines and best practices, covering a wide array of e-services and allowing seamless integration with the Doptor platform.

- **Intelligent Search Mechanism**:

Implement an intelligent search mechanism leveraging AI/ML to enable users to find relevant standards, guidelines, and documents efficiently.

- **Dynamic Content Management**:

Introduce a dynamic content management system allowing easy updating, modification, and addition of new standards, guidelines, and documents.

- **Enhanced Document Versioning**:

Improve the document versioning system, enabling better tracking and management of document revisions, ensuring users access the most current and relevant information.

Deliverables:

- **Enhanced User Interface and Experience**:
  Redesigned user interface and improved user experience for seamless navigation and content consumption.
- **Comprehensive Integration Guidelines**:
  Detailed and extensive integration guidelines covering various e-services and facilitating smooth integration with the Doptor platform.
- **Intelligent Search Functionality**:
  AI-powered search functionality that provides relevant results and suggestions to users, enhancing their search experience.
- **Dynamic Content Management System**:
  Dynamic content management system allowing easy updates, modifications, and addition of new standards, guidelines, and documents.
- **Improved Document Versioning System**:
  Enhanced document versioning system for efficient tracking and management of document revisions.

3.3.6 Office Organogram:

The Office Organogram Builder in the Doptor platform serves as a vital tool to visually represent the hierarchical structure and relationships within a government office. It allows users to create, customize, and maintain the organizational chart, providing a clear and intuitive view of the office's framework.

Existing Feature:

- User should have option to create self-office organogram through using Existing template
- Using verification and approval mechanism

New Development:

- Develop an intuitive interface for users to create, modify, and customize the organizational chart based on their requirements.
- Integrate the organogram builder with user profiles to accurately map employees to their designated positions within the organizational structure.
- Implement real-time synchronization to reflect changes instantly across the platform, maintaining data accuracy and consistency.

Deliverables:

- An easy-to-use interface that allows users to intuitively create, edit, and visualize the office organogram.
- Implement drag-and-drop tools for seamless position arrangement and hierarchy management.
- An approval workflow integrated into the module to ensure changes undergo verification and authorization.
- Configurable access controls and permissions based on user roles to manage who can modify or view specific parts of the organogram.

3.3.7 Doptor Marketplace

In Doptor Marketplace, various modules or components work together to automate, manage, and coordinate processes and tasks efficiently. These modules collectively form a robust service orchestration framework, enabling organizations to streamline their operations, automate tasks, and ensure efficient coordination and management of services and processes.

1. **Integration Adapters/Information Mediator:** Allows integration with different systems, applications, and services to enable seamless communication and data exchange. More details see section - 3.3.22
2. **Workflow Engine:** Manages and executes workflows that define the sequence of steps for a particular process or service. More details see Section 3.3.24
3. **Template Builder** Provides a graphical or code-based interface to design, model, and define workflows and processes. More details see Section 3.3.25
4. **Task Manager:** Schedules and manages tasks based on predefined rules, priorities, or triggers within the orchestrated workflow.More details see Section 3.3.23
5. **Service Catalog:** Acts as a repository of available services, providing information and interfaces for selecting and using services within the orchestration.
6. **Notification and Alerting:** Sends notifications and alerts to stakeholders based on predefined events or conditions in the orchestrated processes.
   More details see Section 3.3.21
7. **Data Transformation and Mapping:** Converts and maps data between different formats or standards to facilitate interoperability among integrated systems.
8. **Reporting and Analytics:** Generates reports and provides analytics to analyze the performance, efficiency, and outcomes of orchestrated processes. More details see link
9. **API Management:** Manages APIs (Application Programming Interfaces) that facilitate communication and integration between various modules and external systems. More details see Section 3.3.11
10. **Service queueing /Distributed Queue manager** More details see Section 3.3.9
11. **Calendar**
    a. See section 3.3.8
12. **Email gateway**

    Integrating Email Gateway into Doptor will enable seamless communication, notifications, and updates, ensuring that the platform functions without disruption and can reach its users through their preferred channels.

Email Communication: Doptor will be able to send emails for official communication between government offices, employees, and external stakeholders with **Bulk emails** option to multiple recipients for announcements, newsletters, or mass communication. Other options like attachment handling, user defined Template, and Notification facility will be available. **Schedule** email delivery for specific dates and times, ensuring messages are sent at the most appropriate moments. **Delivery and Read Receipts** Receive confirmation of email delivery and read receipts, providing visibility into message status.

13. **SMS gateway**

    Integrating SMS into Doptor will enable seamless communication, notifications, and updates, ensuring that the platform functions without disruption and can reach its users through their preferred channels.

    Message Sending: Consulting firm will ensure that the SMS gateway will allow Doptor to send SMS messages to government employees, offices, and stakeholders. It will also Support for sending bulk SMS messages to multiple recipients simultaneously for efficient communication.

    Message Scheduling: Schedule SMS messages for future delivery, ensuring timely notifications and reminders.

    Delivery Reports and Dashboard: Receive delivery reports to track the status of sent messages, ensuring successful communication. The Central Dashboard will visualize the statistic according to the client.

    Template Support: Create and use message templates for standardized communication with predefined content.

    Integration of OCR (Optical Character Recognition), Cam Scanner, Facial Recognition, Biometric Login, and Photo Editor Tools: These modules will be integrated with Doptor using global standards to enable efficient document processing, identity verification, and image editing functionalities on mobile devices.

    Profile Aggregator Integration: Integration with profile aggregators to streamline and manage user profiles across different government systems and services, ensuring consistency and ease of use.

14. **Integration with Digital Signature:** Flexibility for approving authorities or officers to sign or add digital signatures to Application forms using external devices, providing a convenient and easy option for authentication & signing within the Doptor platform.

Marketplace Governance

1. **Event Monitoring and Handling:** Monitors events and triggers actions or workflows based on predefined rules or conditions.
2. **Security and Access Control:** Ensures secure access to orchestrated processes and data, managing user permissions and authentication.
3. **Error Handling and Logging:** Captures and logs errors, exceptions, or issues that occur during orchestration, enabling effective troubleshooting and resolution.
4. **Performance Monitoring and Optimization(System):** Monitors the performance of orchestrated processes, identifies bottlenecks, and optimizes workflows for efficiency and speed.

5. **Governance and Compliance:** Ensures that orchestrated processes comply with organizational policies, standards, and regulations.
6. **Resource Provisioning and Management:** Manages and provisions resources required for orchestrated processes, such as computing resources, databases, or network configurations.

3.3.8 Doptor Calendar

The future development of the Holiday Calendar aims to make it a comprehensive and intelligent tool that not only informs about holidays but also assists in efficient planning and organization around these holidays. These additions align with the rapidly evolving technological landscape and user expectations for intuitive and feature-rich applications.

Existing System:

- Holiday calendar will be developed and the API will be exposed for external application
- Government Bangla holiday calendar
- Government English holiday calendar
- Government Hizri holiday calendar
- Educational holiday Calendar
- Bank holiday Calendar
- The system will allow ministry / directorate level user will create calendar and share
- Holiday calendar adjustment
- Export
- Calendar relocation history
- Data sharing through RestFul APISingle and Recurring Event setup with Notifications.
- Task/Subtask list: Facilitate users to manage/maintain his/her regular task and view his/her own task at a glance in Calendar Dashboard.
- Calendar sharing mechanism: Facilitate users to set their meeting/event time in the calendar as well as sharing with the team/office/external offices.
- Invitation: Send invitation other officers and ensure necessary notifications
- Integration with Different eservices for event creation.

New Development:

- Develop a notification system allowing users to customize and receive notifications for upcoming holidays based on their preferences and roles.
- Implement AI-driven insights to analyze holiday patterns, user behaviors, and trends to provide intelligent recommendations for efficient holiday planning.
- Enable users to plan and organize events or activities associated with holidays directly within the calendar for effective event management.
- Integrate weather forecasts for each holiday, helping users plan their activities considering the weather conditions.
- Include public events, government ceremonies, or significant functions in the holiday calendar to provide comprehensive coverage of notable days. For example: MS project calendar.

- Implement features that allow users to share holiday information or plans on their social media platforms directly from the calendar, enhancing social engagement. Such as add event to calendar
- Integrate a feedback mechanism within the calendar to gather user opinions and suggestions for continuous improvement and optimization.

Deliverables:

- A fully functional notification system allowing users to set, receive, and manage personalized holiday notifications.
- AI-driven insights module providing data analysis and recommendations based on holiday patterns and user interactions.
- Enhanced language support, catering to a broader audience and ensuring a seamless user experience for non-English speakers.
- Integrated visual components providing interactive representations of holiday data for enhanced user engagement and understanding.
- Feedback mechanism allowing users to provide feedback within the calendar interface, contributing to future improvements.
- Module providing weather forecasts for each holiday, assisting users in planning their holiday-related activities effectively.
- Functionality enabling users to share holiday details or plans on their social media platforms directly from the calendar.

3.3.9 Distributed Queue Manager:

The future development of the Distributed Queue Manager in the Doptor platform aims to enhance scalability, performance, and flexibility, ensuring seamless message processing and efficient queue management. These developments align with the increasing demands for reliable and efficient message queuing systems in a distributed environment.

Existing System:

- **Queue Creation:** Users are able to create and configure queues for different types of tasks or data items.

New Development:

- Optimize and upgrade the queue manager to handle a higher volume of requests and ensure minimal latency for processing.
- Implement comprehensive monitoring tools and intuitive dashboards to monitor queue performance, track message processing, and manage queues effectively.
- Develop a robust error handling system with automated retry mechanisms to handle failed message processing and ensure message delivery.
- Enhance the DLQ(Dead Letter Queue) system to allow for seamless handling and analysis of undeliverable or failed messages.
- Introduce prioritization and sorting of messages within the queues based on predefined criteria to optimize message processing.
- Implement message filtering mechanisms, allowing for specific messages to be routed to designated queues based on defined rules.

- Enable seamless integration with external systems and applications for message exchange and processing, ensuring interoperability.
- Strengthen security measures to safeguard the integrity and confidentiality of the messages within the distributed queue system.
- Expand configuration options to allow for more flexible queue setups, including persistent and non-persistent queues.

Deliverables:

- Upgraded and optimized queue manager capable of handling a higher volume of messages with improved performance.
- Comprehensive monitoring dashboard providing real-time insights into queue performance, message processing, and system health.
- Robust error handling module with automated retry mechanisms to manage failed message processing effectively.
- Enhanced Dead Letter Queue system for analyzing and managing undeliverable or failed messages.
- Implementation of priority queues for prioritized message processing based on defined criteria.
- Module enabling message filtering and routing based on predefined rules, optimizing message delivery.
- Integration interfaces allowing seamless interaction with external systems for message exchange.
- Implemented security features and protocols to enhance the security of the distributed queue manager.
- Expanded and flexible queue configuration options to tailor the system to specific requirements.

3.3.10 Audit Trail:

The Audit Trail system, which currently tracks service updates, publishing, unpublishing, and desk changes, will be enhanced with new features. The new version of the Audit Trail will record all activities of users associated with the platform, including changes made to service-related data. It will provide a comprehensive history tracking facility for both service recipients and service providers. Additionally, admin users will have the ability to create reports from this component, enabling them to gather valuable insights and analyze the recorded data.

Existing Development: The current Audit Trail system can keep a record of all changes.

New Development: New version of Audit trail will have the following features-

- It will keep a record of all the activities of all the users associated with this platform.
- If any data related to the services are changed must be recorded as whom, when, and what has been changed.
- Admin users will be able to create reports from this component.
- **Cross-Device Authentication and Tracking:** Cross-Device Authentication and Tracking is a system that allows users to seamlessly access and track their information and activities across multiple devices securely. It ensures a consistent and convenient user experience, no matter which device they use.

Deliverables:

Audit Log Files: The primary deliverable of an audit trail is the collection of log files that record relevant events and activities within a system. These log files capture information such as timestamps, user or entity identifiers, actions taken, and any relevant data associated with each event.

Timestamps: Each log entry in the audit trail should include a timestamp indicating when the event occurred. Precise timestamps are crucial for understanding the sequence of events and for investigating incidents.

User or Entity Identification: Audit log entries should include information about the user or entity responsible for the action. This identification can help attribute actions to specific individuals or entities.

Cross-Device Authentication and Tracking: Cross-Device Authentication and Tracking is a system that allows users to seamlessly access and track their information and activities across multiple devices securely. It ensures a consistent and convenient user experience, no matter which device they use.

Action Details: The audit trail should document the specific actions taken, such as login attempts, data modifications, configuration changes, and other relevant events. Descriptive information about each action is essential for understanding what occurred.

Data Changes: If the audit trail is used to track changes to data, it should record the details of data modifications, including the old and new values of the data being changed.

Event Descriptions: Clear and concise descriptions of each event or action should be included in the audit trail. These descriptions help auditors and administrators understand the nature of the event.

Source or Origin of the Event: In some cases, it's important to document where the event originated. This can include the IP address or hostname of the system or device responsible for the action.

Event Categories: Events in the audit trail may be categorized to make it easier to filter and analyze the data. Common categories might include login events, administrative actions, data access, and security-related events.

Retention Policy: An audit trail deliverable should include information about how long audit logs are retained. Retention policies are often defined to meet regulatory requirements and organizational needs.

Log Rotation and Archiving: Procedures for log rotation and archiving should be documented. Log files can become large over time, so they may need to be rotated or archived to manage storage efficiently.

Access Controls: Audit trail deliverables may include information about access controls and permissions for viewing and managing audit logs. Not everyone should have unrestricted access to audit logs.

Reporting Tools: Depending on the system, audit trail deliverables may include reporting tools or mechanisms that allow users to generate reports and queries based on the audit data.

Compliance Documentation: For systems subject to regulatory requirements (e.g., GDPR, HIPAA, SOX), audit trail deliverables should include documentation demonstrating compliance with relevant standards or regulations.

Alerting and Notifications: In some cases, the audit trail may be configured to generate alerts or notifications for specific events or conditions, and these settings should be documented.

Documentation of Log Storage and Backups: Details about how audit logs are stored, backed up, and protected from tampering should be included in the deliverables

3.3.11 API Manager:

Existing System:

API Manager acts as a central gateway for availing access to all relevant service consumers. API manager provides a centralized platform which acts as a reverse proxy, receiving requests and routing API requests from clients and forwarding them to the appropriate backend services.

- API Manager acts as a central gateway for providing access to service consumers.
- It functions as a reverse proxy, receiving requests from clients and routing them to the appropriate backend services.
- The API Manager provides a centralized platform for managing APIs and their access.
- It ensures that service consumers can conveniently access the relevant APIs.
- The API Manager plays a crucial role in facilitating the interaction between clients and backend services.

New Development

It will offer a range of features and tools, including API governance, security, monitoring, and analytics, that help to ensure the quality, reliability, and security of APIs.

- Manages the lifecycle of APIs, including documentation, testing, versioning, and retirement. Offers a self-service portal to discover, explore and consume APIs, comprehensive documentation, interactive API documentation, sample code, SDKs, and sandbox environments for testing.
- Balances incoming traffic to ensure high-quality service by distributing the load across backend services. Supports management of multiple API gateways.
- Allows API consumers to request permission for specific services from administrators. Administrators can manage user access to the API gateway, including creating users, assigning roles, and setting permissions.
- Provides a dashboard with charts, graphs, and visualizations to track metrics such as response times, error rates, and usage patterns. Supports consumer-wise

reporting and data monitoring. Generates reports and visualizations to analyze API traffic.

- The API management platform supports the integration of external services and internal components, offering features for API lifecycle management, load balancing, user access management, and comprehensive metrics and reporting.

Deliverables:

API Documentation: Comprehensive documentation for the APIs is a critical deliverable. This documentation should include details about endpoints, request/response formats, authentication methods, and usage examples to help developers understand how to interact with the APIs.

API Gateway: An API gateway is often a core component of an API manager. It serves as a front-end interface that manages API traffic, handles security, rate limiting, and routing. Deliverables related to the API gateway include configuration files, policies, and routing rules.

Security Policies: API managers should provide security features such as authentication, authorization, and encryption. Deliverables related to security may include API key management, OAuth 2.0 configurations, and access control policies.

Analytics and Monitoring: API managers often include analytics dashboards and monitoring tools to track API usage, performance, and errors. Deliverables here include access to real-time and historical API usage data, performance metrics, and customizable reports.

Rate Limiting and Quotas: APIs may have rate limits and usage quotas to prevent abuse and ensure fair usage. Deliverables related to rate limiting include configuration settings and policies.

API Lifecycle Management: API managers typically support the full API lifecycle, from creation and testing to versioning and deprecation. Deliverables may include tools and processes for managing APIs throughout their lifecycle.

Integration and Extensibility: Deliverables should include options for integrating the API manager with other systems and tools, as well as extensibility features that allow organizations to add custom functionality or plugins.

Gateway Policies: Detailed policies that define how traffic is managed and secured at the API gateway level, including request/response transformation, traffic shaping, and security policies.

Version Control: If APIs are versioned, deliverables should include mechanisms for version control, such as API versioning schemes and management tools.

Health Monitoring and Alerts: Documentation and configuration settings for health checks, alerts, and notifications related to the availability and performance of APIs.

Deployment Scripts and Automation: Deliverables may include scripts or automation tools for deploying APIs, policies, and configurations to different environments (e.g., development, staging, production).

Data Transformation and Mapping Tools: If data transformation is required, deliverables may include tools and configurations for mapping and transforming data between different formats or versions.

Backup and Recovery Procedures: Documentation and procedures for backing up API configurations and data, as well as strategies for recovering from failures or data loss.

Compliance and Governance: Documentation demonstrating how the API manager supports compliance with industry standards and regulations, including GDPR, HIPAA, and others.

Training and Support Materials: Training materials, user guides, and support documentation to help developers and administrators effectively use the API manager.

Change Management Procedures: Procedures and documentation for managing changes to APIs, including version updates, deprecation notices, and communication with API consumers.

3.3.12 QR Code Generator:

New Development: QR Approach should be introduced in the Doptor Platform so that the users of Doptor can authenticate login and application for services using QR codes. QR based certificates generation will be another feature of this component. The QR code generator in the Doptor platform will serve as a reusable building block for authentication, application, and certificate generation. It enables users to conveniently verify and validate their login and services using QR codes.

Deliverables : **QR Code Generator**

3.3.13 AI-powered Digital Assistant:

New Development: The AI-powered digital assistant in the Doptor platform will be seamlessly integrated with the a2i chatbot, providing a comprehensive user experience. It will serve as a single point of contact for users, offering various functionalities for data and application management. The digital assistant will facilitate data sanitization, data readiness, and ensure smooth operations. It will continuously learn and improve, delivering personalized and accurate assistance to users. An admin panel will be provided for data analysis, enabling in-depth insights and monitoring of user interactions.

Deliverables :

- Design documents specifying the user interface, architecture, and technical specifications of the digital assistant.
- A functional admin panel for data analysis, including access controls and data visualization tools.
- A working integration of the digital assistant with the a2i chatbot, ensuring seamless communication and cooperation between the two components.

3.3.14 Doptor Authenticator:

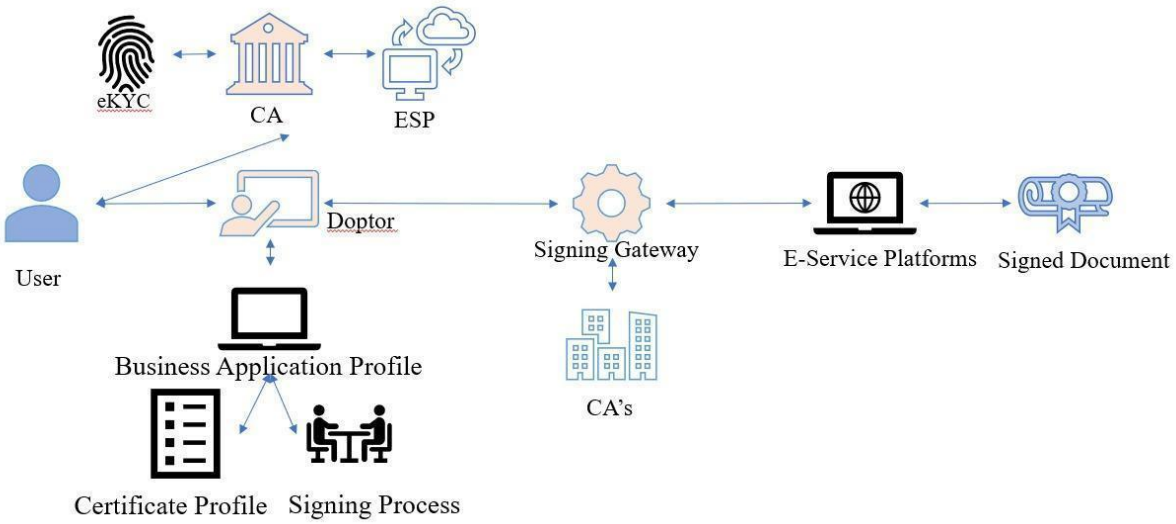
New Development:

It will provide multi-factor authentication services. It will verify the identity of users by generating unique, time-based passwords. This will help to ensure that only authorized users can access Doptor applications. The firm will determine what functionalities and features should be included in the Doptor Authenticator to meet the authentication needs of Doptor users.

Deliverables : **Doptor Authenticator.**

3.3.15 eSign gateway

The development of the eSign Gateway in the Doptor platform is focused on enhancing security, accessibility, and user experience. These developments align with the objective of creating a more secure, efficient, and technologically advanced e-governance ecosystem.



Features:

Document Preparation: These platforms often provide tools for uploading, creating, and preparing documents for electronic signature. Users can upload PDFs, Word documents, or other file types and prepare them for signing.

Signature Capture: The primary function of an eSign gateway is to capture electronic signatures. This can include various methods such as drawing, typing, or uploading a scanned signature image.

Multi-Signature Support: Many eSign platforms support multiple signatories, allowing for documents with multiple signers in a specified order or simultaneously.

Authentication: Strong user authentication mechanisms, such as email verification or multi-factor authentication, are often included to verify the identity of signers.

User Roles and Permissions: Role-based access control allows administrators to define who can send, view, or sign documents. This feature ensures proper access and authorization.

Audit Trail: An audit trail records every action taken on a document, including who viewed, signed, or made changes to it. This provides a complete history for legal and compliance purposes.

Notifications: Automated email notifications and reminders can be sent to signers to prompt them to review and sign documents, reducing delays.

Integration: eSign gateways often integrate with popular productivity tools and business applications, such as CRM systems, document management systems, and cloud storage services.

Mobile Access: Mobile-friendly interfaces or dedicated mobile apps allow users to sign and manage documents from smartphones and tablets.

Compliance: eSign platforms typically adhere to industry-specific and regional compliance standards (e.g., eIDAS in Europe, ESIGN Act in the United States).

Data Security: Robust encryption and data security measures are in place to protect sensitive information, ensuring the confidentiality and integrity of documents.

Document Storage: The platform may offer secure storage for signed documents, enabling easy access to signed agreements in the future.

Deliverables:

Signed Documents: The primary deliverable is the electronically signed document or agreement, which is legally binding and can be stored electronically.

Audit Trail Records: Detailed logs of all activities related to the document, providing an audit trail for compliance and legal purposes.

Authentication Records: Records of user authentication methods used during the signing process.

Reports and Analytics: Tools for generating reports and analytics on document signing activities and performance.

User Documentation: Documentation, guides, and resources for users to understand how to use the eSign gateway effectively.

Compliance Certifications: Certifications or documentation showing that the eSign gateway complies with legal and industry-specific standards.

Support and Training: Access to customer support and training resources to assist users and administrators in using the platform effectively.

Integration Documentation: Documentation on how to integrate the eSign gateway with other systems and applications.

3.3.16 Data Management (Data Analytics):

Central Data Hub: Establish a centralized data hub to collect, store, and share various types of data from different servers and systems. This hub will serve as a central repository for government data, ensuring efficient storage and retrieval.

3.3.17.1 Data Transformation: Develop a structured framework to transform collected data into a usable format within the central data hub. This involves standardizing data formats, cleaning and validating data, and ensuring data integrity.

3.3.17.2 Predictive Analysis and Service Recommendation: Develop a centralized analytics platform by utilizing data analytics and predictive analysis techniques to assist in recommendations for services he/she receives and provide valuable recommendations for policy-making and service improvements at the workplace.By analyzing user, device, and service-related information, personalized recommendations can be provided to officers based on their needs and preferences.

3.3.17.3 Integration of Artificial Intelligence and Machine Learning (AI/ML): Harness the power of AI/ML technologies to enhance the capabilities of the Doptor platform and improve user services.

- **AI-powered Digital Assistant:** Deploy an intelligent chatbot on the Doptor platform to provide instant assistance, answer FAQs, and guide users in finding desired services. Seamlessly integrated with the a2i chatbot, it offers personalized and accurate assistance, facilitating smooth operations and enhancing user experience.
- **Voice Recognition and Natural Language Processing:** Integrate AI technologies for voice-based interactions and natural language understanding, enhancing user experiences and enabling more intuitive interactions with the platform.
- **Data-driven Decision-making:** Utilize AI tools and techniques to analyze large volumes of data and generate actionable insights, supporting evidence-based policy-making and governance.

3.3.17.4 Integration of Blockchain and Data Security:

- Research and implement blockchain technology to enhance data security, integrity, privacy and transparency in government transactions and data sharing.
- Explore the feasibility of utilizing blockchain for secure and tamper-proof record-keeping, particularly for sensitive government data.
- Identify scope for future blockchain integration to secure user identity management and streamline authentication processes.

Deliverables:

1) **Data Sources and Data Dictionary**:

   List the data sources that will be used in the project and provide a data dictionary describing the datasets, their fields, and their meanings. Prepare a document with all required information.

2) **Data Collection and Integration**:

   Describe how data will be collected, cleaned, and integrated. This may include Extract, transform, and load (ETL) processes, data warehousing, or data lake setup.

3) **Data Cleaning and Preprocessing**:

   Specify the procedures and methodologies for data cleaning and preprocessing, along with any software or tools to be used.

4) **Data Security and Privacy Measures**:

   Detail the security and privacy measures that will be implemented to protect sensitive data.

5) **Data Governance Framework**:

   Outline the governance framework for managing data, including roles and responsibilities, data stewardship, and compliance with regulations.

6) **Data Analytics and Reporting**:

Describe the analytics techniques that will be applied to the data and the expected reports, dashboards, and insights to be generated.

7) **Data Catalog and Metadata Management**:

   Explain how data will be cataloged, including metadata management and documentation practices.

8) **Data Maintenance and Archiving Plan**:

   Present a plan for data maintenance, including updates and archiving of historical data.

9) **Data Access and User Permissions**:

   Clarify how authorized users will access data and specify the access control mechanisms.

10) **Performance Optimization Strategies**:

    Provide strategies for optimizing data management processes and infrastructure to ensure performance and scalability.

11) **Disaster Recovery and Backup Plan**:

    Describe the disaster recovery and backup plans to safeguard data against unexpected events.

12) **Documentation and Training:**

    Explain how project documentation and training materials will be developed and made available to project team members.

3.3.17 Real-time Application (RTA) frontend:

New Development:

The implementation of a real-time application frontend will enable constant and immediate communication between systems and users, eliminating the need to manually refresh the application. By utilizing technologies like push notifications, email alerts, or in-app messages, users will receive instant updates in real-time, ensuring they are promptly informed about important events, changes, or relevant information. All platforms and users will be synchronized in real-time, ensuring instantaneous updates and seamless collaboration. This enhanced functionality will improve user engagement, simplify communication processes, and facilitate seamless interaction between the platform and its users.

Deliverables:

- RTA supported Responsive UI/UX

3.3.18 Smart Support Management:

New Development:

Doptor is planning to implement a smart support management system that will ensure efficient and responsive assistance for users in the future. Trained staff from the firm will handle users' feedback and queries through the hotline. The support team will actively monitor these channels, ensuring timely and effective resolution of users' concerns. With these upcoming smart support channels and well-trained personnel, Doptor aims to provide exceptional support services to users.

Smart support management component includes the following features-

- Support Dashboard: An advanced dashboard with comprehensive ticketing statistics, filters, and real-time data on pending, latest, trending, solved, and referred tickets. Enables efficient ticket management and informed decision-making.
- Messenger: WhatsApp can be a great medium to receive feedback and query from users.
- Email: There will be a dedicated email for doptor support. Users will be able to send their feedback/queries to this email address.
- Live Chat: There will be a dedicated team to provide live support. Users will be able to get support instantly through chatting online.
- Client Feedback Survey: This feature could allow the system to create, distribute, and collect feedback surveys from clients to gather valuable insights for service improvement and client satisfaction and service quality

Deliverables:

- Support dashboard
- Integration with ; messenger, Email, Live chart
- Survey report

3.3.19 Serverless Architecture Oriented Development:

New Development:

Serverless is an approach to software development that abstracts the server layer from the application code. The serverless approach is a cornerstone of the modern application, with its distributed components that manage their own server-side logic and infrastructure in response to application events. These components are typically Functions as a Service and third-party microservices, often running on containers.

Some typical use cases that lend themselves well to serverless architecture include:

- Auto-scaling websites: Because the serverless backend scales automatically based on runtime demand, fully functional and high performing websites can be launched without upfront infrastructure setup (and testing). The result is much faster time-to-market.
- Seamlessly integrating SaaS events into the system logic: Serverless architecture makes it easy to trigger functions based on events from SaaS platforms such as Salesforce, GitHub, AuthO, or Stripe.
- Multilingual applications: Serverless architecture makes it possible for components to work together smoothly, even if different components were developed using different development languages and frameworks.

- The firm should follow serverless architecture oriented development to make “Doptor” go serverless.
- Ensure compatibility with renowned cloud services for modern technology adoption in the "Doptor" platform. This enables scalability, high availability, and robust security, leveraging cloud-native services for enhanced agility and efficiency.

3.3.20 Building Blocks:

The following components mentioned in the TOR will serve as independent building blocks, that will be independent building blocks that can be easily configured and integrated with any platform, empowering organizations to leverage its functionality seamlessly. They are mentioned below:

1. Central Dashboard
2. Task manager
3. Holiday calendar
4. Service scheduler
5. Queue manager
6. eSign gateway

These building blocks can be utilized to enhance and customize the platform according to specific requirements, ensuring flexibility and scalability in delivering services to citizens. The above list may fluctuate from the scope explained within this section.

Deliverables: Ensure Section 3.3.20. SL No 1. To 6 as a building block

3.3.21 Notification

This module keeps users informed about activities related to their accounts and government services via email and SMS.

Existing Features:

- Notification text configuration: The current system allows the administrator to globally customize the text content of notifications.

New Development:

- **Event-wise service notification configuration:** The Doptor platform should also provide event-wise service notification configuration, allowing users to receive notifications concerning specific events such as document expiry, upcoming deadlines, and changes in service requirements.

- **Integration with other systems:** The notification module of the Doptor platform needs to be integrated with other government systems to ensure real-time delivery of notifications. This includes integration with relevant platforms.

- **Personalized Notifications:** The Doptor platform should provide personalized notifications to users based on their preferences and previous interactions. This could include customized messages, tailored recommendations, and personalized updates.

- **Multi-channel Notification:** The Doptor platform should support multi-channel notification options, allowing users to receive notifications through email, SMS, and push notifications on their mobile devices. This ensures timely and convenient delivery of notifications.

- **Notification History:** The Doptor platform should maintain a comprehensive notification history for each user, enabling them to review previous notifications and track their interactions with the platform. This helps users stay informed about their government services and ensures transparency in the notification process.

3.3.22 Integration Adapters/ Information mediator

Successful Integration with various technology, data, or service points, facilitated by the information mediator layer, is the key to the success of the Doptor initiative. The information mediator acts as a data exchange layer, enabling seamless communication and interoperability between different systems and applications. Examples of the information mediator's role include facilitating data exchange between government agencies, integrating external service providers, and connecting with data repositories and APIs. The final integration scope will not be limited to these examples, as the information mediator layer allows for flexible and scalable integration possibilities.

The Information Mediator is a critical component in the Doptor platform, ensuring the smooth flow of data and information among government systems while maintaining data security and consistency. The outlined scope and deliverables contribute to its effectiveness and reliability.

- **Integration with Government Stacks and Systems:** Integration with other government stacks and systems to enable seamless data exchange, interoperability, and collaboration between different government entities. The firm will also create the documentation on the integration scope, develop, test and monitor the integration with other systems.
- **Continuous Exploration of New Integration Opportunities:** Regular evaluation and exploration of emerging technologies and integration possibilities to enhance the capabilities and functionalities of the Doptor platform.
- **Robust Documentation and Standards:** Documentation of integration processes, protocols, and standards to facilitate future integrations and ensure consistency, scalability, and interoperability.
- **Data Integration Framework:** Develop a robust data integration framework that enables the exchange of information among government systems, regardless of their technology or data formats.

- **Data Transformation Mechanisms:** Implement data transformation capabilities to standardize data structures and formats, ensuring uniformity and compatibility.

- **Data Routing and Workflow:** Create a data routing and workflow management system to direct data to the appropriate systems and ensure efficient processes.

- **Data Security Enhancements:** Enhance data security measures to safeguard sensitive information during transmission and storage, including encryption and access control.
- **Real-time Monitoring and Reporting:** Develop a real-time monitoring and reporting system to track data exchanges, identify potential issues, and generate reports for transparency.
- **Error Handling and Recovery:** Implement robust error handling mechanisms to gracefully manage data errors and exceptions, minimizing disruptions.
- **Scalability Features:** Build in scalability features to accommodate the increasing volume of data and the integration of additional government systems.

Deliverables

- **Integrated Data Exchange Framework:** A fully functional data integration framework that allows government systems to exchange data seamlessly.
- **Data Transformation Mechanisms:** Implemented data transformation processes to standardize data structures and formats for consistency.
- **Data Routing and Workflow System:** An efficient data routing and workflow management system that ensures data is directed to the appropriate systems.
- **Enhanced Data Security Measures:** Improved data security measures, including encryption and access control, to protect sensitive information.
- **Real-time Monitoring and Reporting System:** A comprehensive monitoring and reporting system for real-time tracking and issue identification.
- **Robust Error Handling and Recovery Mechanisms:** Error handling mechanisms that gracefully manage data errors and facilitate quick recovery.
- **Scalability Features:** Added features to ensure the Information Mediator can scale with the growing data and system integration requirements.

3.3.23 Task Manager

Facilitate users to create, assign tasks and manage/maintain his/her regular task and view his/her own task at a glance in Calendar Dashboard.

Existing System:

- Dashboard
- Task creation
- Edit Task
- Delete task
- Notify
- Task Notes and Attachments
- Status Tracking

New Development:

- Task Prioritization
- Integration with Other Tools(e.g., email, chat, document sharing)
- Progress Reports
- Mobile Accessibility
- Dependencies subtask
- Data Backup and Security

Deliverables:

- Standard guideline for Task manager Integration and update standard portal
- Manual for Task manager
- Configurable Task module
- Quarterly Report

3.3.24 Workflow Engine

The Workflow Engine helps to drive efficiency in a large system by providing automation and orchestration capabilities for specified business processes within and across multiple integrated system. The Workflow engine will provides design-time mapping & modeling of business processes based on mature open standards like Business Process Model and Notation (BPMN) and facilitates the run-time execution of deployed workflows in order to orchestrate process flows from initiation to completion.

The Workflow Engine's scope aims to enhance operational efficiency, transparency, and service quality within the government office, optimizing workflows and standardizing processes to improve citizen service delivery.

The scope of a Workflow Engine in a government office context encompasses:

1. **Process Automation:** Implementing an automated system to manage and streamline various processes involved in citizen service requests, document handling, approvals, and delivery.
2. **Workflow Customization:** Providing a flexible system that allows customization and configuration of workflows based on different types of requests, ensuring adaptability to evolving administrative procedures.
3. **User Interface:** Developing an intuitive and user-friendly interface for staff to initiate, monitor, and manage workflows, enabling easy tracking of requests through various stages.
4. **Integration Capabilities:** Ensuring the Workflow Engine integrates seamlessly with existing systems and databases within the government office to access and update information efficiently.
5. **Rule-Based Processing:** Implementing rule-based processing to enforce compliance with regulations, validation of submitted data, and automated decision-making for standard procedures.
6. **Notifications and Alerts:** Incorporating notification mechanisms to inform staff and applicants about the status of requests, pending actions, and required follow-ups.

7. **Data Analytics and Reporting:** Including tools to gather process-related data, analyze performance metrics, and generate reports for continuous improvement and decision-making.
8. **Scalability and Adaptability:** Designing the Workflow Engine to scale with increased workload and adapt to evolving regulatory changes or service requirements.
9. **Security and Compliance:** Ensuring robust security measures to protect sensitive citizen data, following compliance standards and regulations for data privacy and protection.
10. **Training and Support:** Providing comprehensive training and ongoing support to staff for efficient utilization of the Workflow Engine.

3.3.25 Template Builder

The template builder's scope encompasses a user-friendly, adaptable, and integrated tool that empowers government officers to create, manage, and utilize standardized templates efficiently within the Doptor platform, enhancing productivity and consistency in administrative processes.

1. **Customizable Templates:** The template builder will allow government officers to create, edit, and customize various types of templates relevant to their administrative tasks. These templates could include documents, forms, reports, emails, or any other structured formats used within the government office.
2. **Drag-and-Drop Interface:** A user-friendly interface that facilitates the creation and modification of templates using a drag-and-drop mechanism. This enables easy rearrangement of components, addition of fields, and customization of layouts without requiring extensive technical knowledge.
3. **Standardization and Consistency:** The template builder aims to ensure standardization and consistency across documents and reports generated within the government office. It will enforce predefined formats, layouts, and branding elements, maintaining a uniform appearance across all official documents.
4. **Integration Capabilities:** Integration with other modules or systems within the Doptor platform, enabling the use of data from various sources to populate templates automatically. This could involve pulling information from databases, existing records, or other integrated systems to streamline the template population process.
5. **Version Control and History:** The template builder will provide version control features, allowing users to track changes, revert to previous versions, and maintain an audit trail of template modifications. This ensures accountability and traceability in document management.
6. **Accessibility and Permissions:** Role-based access control mechanisms to manage who can create, modify, or use specific templates. Permissions will be defined to ensure that only authorized personnel can make changes to templates and that users have access to the templates relevant to their roles.

7. **Scalability and Flexibility:** The template builder should be scalable to accommodate future requirements and evolving needs within the government office. It should support the addition of new templates, formats, and features as the organization's needs change over time.
8. **Documentation and Support:** Comprehensive documentation and user support to assist government officers in using the template builder effectively. Training materials, tutorials, and help resources will be provided to ensure that users can harness the full potential of the tool.

3.4 Non-Functional Requirements

3.4.1 Coding Convention

The firm must follow the standard coding styles to produce high-quality code for further usage of the code in terms of reusability, refactoring, task automation, language factors etc. The firm should submit a standard coding convention approach, which may include different conventions like commenting, indent style, naming etc. following the best coding practices.

Note: A comprehensive "**List of Standards"** based on the latest technology to be compiled for Doptor Web regarding the solution development and operation will be preferred in the firm's technical proposal.

3.4.2 Documentation Plan

Detailed and proper documentation of such ICT based projects like e-service application development and implementation for Government is very vital and essential. Documentation is required for any such project as reference, knowledge transfer, analysis of development and implementation history, baseline information for any modification or change, guidance etc. In this issue, Vender should show the highest-level of professionalism for delivering the standardized documentation approach at each phase of the e-Service development and implementation project. Firms should include an extensive **"Documentation Plan"** of this project in their technical proposal.

3.4.3 Perform analysis, training, and updates to the current system as required.Availability:

Ensure 2/7 availability of the Doptor platform with allowed downtime for regular maintenance and provision of a test environment.

- 24/7 Platform Access: Ensure Doptor platform is available round the clock to users for uninterrupted service accessibility.
- Scheduled Maintenance: Allow scheduled downtime for regular maintenance activities and updates to enhance platform performance.

- Test Environment Provisioning: Set up a dedicated test environment to test changes and updates before deploying them to the live platform.
- High Uptime Percentage: Aim for high uptime percentage to minimize disruptions and maximize user satisfaction.

3.4.4 Fault Tolerance:

Implement proper exception handling and recovery mechanisms to ensure system reliability and avoid irrecoverable data loss in case of transaction failures.

- Exception Handling: Implement robust exception handling mechanisms to handle errors and exceptions gracefully.
- Transaction Recovery: Ensure the system can recover from transaction failures to prevent data loss and maintain data integrity.
- Redundancy and Failover: Introduce redundancy and failover capabilities to mitigate the impact of hardware or network failures.
- Continuous Monitoring: Implement real-time monitoring to detect and respond to faults promptly, reducing downtime.

3.4.5 Supportability:

Design the Doptor platform to be modifiable, extensible, and evolvable, allowing for future additions and exploiting new technologies.

- Modular Architecture: Design the Doptor platform with a modular architecture to allow easy integration of new functionalities.
- Extensibility: Enable easy extension of existing features and capabilities to accommodate future requirements.
- API Support: Provide well-documented APIs to support integration with third-party services and applications.
- Developer-Friendly: Make the platform developer-friendly with clear documentation and guidelines for easy customization.

3.4.6 Configurability:

Allow behavior control through configuration without modifying source code or redeploying packages.

- Flexible Settings: Allow users to configure various aspects of the platform, such as user interface preferences and workflow settings.
- No Source Code Modification: Ensure that configuration changes do not require modification of the source code or redeployment.
- User Role Customization: Provide options to customize user roles and permissions to align with specific organizational requirements.
- Centralized Configuration: Store all configuration settings in a centralized location for easy management and access.

3.4.7 Scalability:

Ensure the Doptor platform easily expands to accommodate additional users, transactions, and data.

- Elastic Infrastructure: Implement an infrastructure that can scale up or down based on demand to handle increased user traffic.
- Load Balancing: Introduce load balancing mechanisms to distribute user requests evenly across multiple servers.
- Database Scaling: Design the database to scale seamlessly to accommodate growing data volumes and user interactions.
- Performance Optimization: Continuously optimize system performance to ensure smooth operations at any scale.

3.4.8 Technical Standards:

Follow standards for data exchange, API security, programming models, and application servers, ensuring interoperability and compatibility with existing systems.

- Data Exchange Compliance: Adhere to industry-standard data exchange formats such as JSON for seamless integration.
- API Security Measures: Implement security measures like JWT tokens to protect API endpoints from unauthorized access.
- Best Programming Practices: Follow best programming practices and coding conventions for maintainable and reliable code.
- Interoperability with Legacy Systems: Ensure compatibility with existing systems by adopting compatible programming models and protocols.

3.5 Support & Maintenance:

- Continuous monitoring of query execution in Database, tuning database and tuning codes & queries to minimize response time.
- Fixing all bugs in the system irrespective of its nature and complexities.
- Enhance and/or re-arrange existing feature of extended development of any supplementary feature within the existing technology framework complying with core SRS.
- Updating training manual adjusting the changes in the system.
- Adjust and update system in compliance with any security test, load test or IT audit conducted by the client.

3.5.1 Layer Based Support Management:

The vendor team needs to follow the layer-based support management system. Layer based support management is a term that refers to the IT support of the system around different levels or tiers of service. Each level or tier has a specific function and responsibility and is staffed by personnel with different skills and expertise. The purpose of layer based support management is to provide efficient, effective, and satisfactory service to customers and end users. The vendor team needs to follow a three-layer support system.

- Helpdesk Support (1st Layer Support)
- Issue Management (2nd Layer Support)
- Technical Support (3rd Layer Support)

3.5.1.1 Helpdesk Support (1st Layer Support)

The vendor team needs to provide the basic help desk resolution and service desk delivery. It is also known as first-line support for the citizens and system users. This support tier will handle basic customer issues, such as system usage help, profile management help, etc.

- Attend to user's phone calls
- Support agents will communicate through multiple channels for example phone, email, Online Support Ticketing System etc.
- Conduct basic troubleshooting using questionnaires to find out the level of support needed
- Create tickets for 2nd layer support
- Solve common queries such as username and passwords issues, office enrollment.

3.5.1.2 Issue Management (2nd Layer Support)

- Issues investigation
- Issues Categorization, Prioritization, and Escalation.
- Basic level troubleshooting of application, database, and infrastructure.
- Collaboration and coordination among the layers
- Collecting feedback from both service recipient and service provider end and adjusting feedback through the proper communication and coordination with Doptor team.
- Prepare customized support reports for the management.

3.5.1.3 Technical Support (3rd Layer Support)

- Core applications, Database, and Infrastructure level bug fixing.
- Accommodating change requests at Core applications, Database, and Infrastructure level
- Continuously analyze user and system logs and take necessary actions if required.
- Taking prompt preventive action solely or with the help of the core development team if any misconfiguration or anomaly is found in the Core applications, Database, and Infrastructure.
- Periodically health checking of Core applications, Databases, and Infrastructure.

3.6 Quality Assurance and testing activities

Quality Assurance Management within the Doptor Platform System aims to ensure the delivery of a high-quality system that meets the specified requirements, adheres to industry standards, and provides a seamless user experience. It involves establishing quality processes, conducting thorough testing, and implementing quality control measures throughout the development and maintenance life cycle. For the overall management ISO 9001/AS 9100/ Six Sigma/CMMI can be followed by tailoring according to need.

Scope of work:

1. Quality Planning: Develop a comprehensive quality management plan that outlines the objectives, processes, and resources required to ensure the quality of the Doptor Platform.
2. Requirement Validation: Verify and validate the requirements of the system to ensure they are complete, accurate, and aligned with stakeholder expectations.
3. Test Planning and Execution: Plan and execute testing activities, including functional, performance, security, and usability testing, to identify defects, ensure system reliability, and validate system behavior. To ensure maximum quality of the platform both manual and automated tests will have to be performed.
4. Defect Tracking and Resolution: Establish mechanisms to track, prioritize, and resolve defects identified during testing or reported by users, ensuring timely resolution and quality improvement.
5. Quality Control and Process Compliance: Implement quality control measures to monitor adherence to defined processes, standards, and best practices throughout the development and maintenance lifecycle.
6. Documentation and Audit: Maintain comprehensive documentation of quality processes, test plans, test cases, and test results. Conduct periodic quality audits to identify areas for improvement and ensure compliance with quality standards.

Deliverables:

- **Quality Management Plan:**
  a. Detailed documentation outlining the approach, objectives, scope, and processes for managing quality assurance within the Doptor Platform.
  b. Description of quality planning, testing methodologies, defect tracking, and quality control measures.
- **Test Plans and Test Cases:**
  a. Development of comprehensive test plans that outline test objectives, scope, test environments, and test schedules.
  b. Detailed test cases and test scripts covering functional, performance, security, and usability aspects of the Doptor Platform.
- **Defect Tracking and Resolution System:**
  a. Implementation of a defect tracking system to capture, prioritize, and resolve defects identified during testing or reported by users.
  b. Documentation of defect resolution processes, including bug fixing, retesting, and validation of fixes.
- **Quality Control Measures and Compliance Documentation:**
  a. Establishment of quality control measures to monitor adherence to defined processes, standards, and best practices.

b. Documentation of quality control mechanisms, quality audits, and compliance with quality standards.

- **Quality Audit Reports and Improvement Initiatives:**

  a. Documentation of periodic quality audits, including findings, non-compliance issues, and areas for improvement.

  b. Recommendations for quality improvement initiatives, including process enhancements and best practices adoption.

Functional Testing:	Validate that all features and functionalities of the Doptor platform work as expected according to specified requirements.	
Performance Testing:	Evaluate the platform's responsiveness, speed, and stability under varying loads and conditions.	
Security Testing:	Identify vulnerabilities and weaknesses to ensure the platform is resistant to unauthorized access and data breaches.	
Usability Testing	Assess the user interface, user experience, and ease of use of the platform.	
Compatibility Testing	Ensure the platform works seamlessly across various devices, browsers, and operating systems.	
Integration Testing:	Validate the interaction and integration of different modules and components.	
Regression Testing:	Confirm that recent updates or changes haven't negatively impacted existing functionalities.	
User Acceptance Testing (UAT):	Involve end-users to validate that the platform meets their expectations and requirements.	

3.6.1 Load Test

Software load testing is a type of performance testing that evaluates the behavior and performance of a software system under normal and anticipated peak load conditions. It involves subjecting the software application to simulated user traffic and workload to

assess its response time, scalability, and reliability. The primary goal of load testing is to identify performance bottlenecks and ensure that the software can handle the expected user load without degradation in performance.

key aspects and objectives of software load testing will be:

1. Performance Assessment.
2. Response Time Analysis.
3. Stress Testing.
4. Resource Utilization.
5. Performance Optimization.
6. Failover and Recovery Testing
7. Capacity Planning

The consultant firm will be responsible to perform a load test on the overall Doptor Platform , rectifying the artifacts and resolving accordingly.

3.7 Workshop, Training & Knowledge Transfer:

The firm will cover the costs of workshops, training for the Doptor initiative. These activities will bring stakeholders together to enhance existing systems, equip staff with necessary skills, ensure data security, and leverage emerging technologies. Capacity development will focus on enhancing technical expertise and fostering innovation. The firm's commitment to continuous learning will drive the success of Doptor. The below sections may fluctuate from the scope explained within this section.

3.7.1 Workshop:

SL	Workshop type	Participant Number	Duration	Meal	Number of seasons
01	Workshop on review deliverables and technology upgrade	50	Full Day	(Standard Lunch, And Two Times standard snakes for morning and afternoon)	3
02	Workshop on UI/UX Design for Portal and MarketPlace	40	Full Day	(Standard Lunch, And Two Times standard snakes for morning and afternoon)	4

- The firm will handle all logistics for the workshops, including venue arrangements, catering services, transportation, and participant remuneration, creating a conducive environment for knowledge sharing, collaboration, and alignment of strategies among participants from diverse backgrounds.
- A series of workshops will be conducted to promote knowledge sharing and enhance collaboration. This includes Yearly Review Workshops and Source code & Architectural Document Handover in the last quarter (3 sessions), External Workshops focusing on UI/UX, Enterprise Architecture, Integration, Serverless Architecture, Infrastructure, Emerging Technology (4 sessions), etc. These workshops will facilitate valuable discussions and enable participants to stay informed about the latest developments and industry trends in their respective domains. The number of workshops may be subject to change, based on the urgency or specific demands arising during the project execution, to ensure successful completion of the scope and objectives.

3.7.2 Training/Knowledge Transfer/Capacity Development:

- Training sessions will be organized to equip staff with the necessary skills and knowledge related to the Doptor platform.
- Knowledge transfer initiatives will be implemented to share domain-specific knowledge and best practices among team members.
- These training sessions will cover a wide range of topics, ensuring comprehensive understanding and proficiency among staff members.
- Capacity building programs will be implemented to enhance technical skills and knowledge of the team members.
- The focus will be on emerging technologies and industry best practices to stay updated with the latest trends and advancements.
- No of personnel

3.8 Security and Privacy Policy

The system's authentication and permission system are robust to ensure the highest level of security. The following measures will be placed to prevent any kind of security breach:

- **Invalid Input:** Validating and purifying incoming data for data integrity and user access.
- **URL Restriction:** Limiting access to URLs based on user permissions and prohibiting unauthorized URL access.
- **Protected Administration Panel:** Securing the admin panel with SSL encryption and different URLs to prevent data hijacking.
- **Password Hashing:** Using one-way algorithms and random salts for password hashing.
- **Session and Cookies:** Regenerating user sessions and cookies uniquely for improved security.
- **Disclosure of Sensitive Information:** Suppressing and logging errors to prevent sensitive information exposure.
- **CSRF Prevention:** Generating automatic tokens to prevent Cross-Site Request Forgery attacks.

- **SQL Injection Prevention:** Implementing prepared statements and proper escaping to prevent SQL and Code injections.
- **Cross-Site Scripting Prevention:** Filtering user-submitted content to prevent XSS attacks.
- **SSL Encryption:** Ensuring SSL encryption for communication between user browsers and the administration panel in Doptor.

3.9 Change Management Plan

The Change Management process shall include the following functionalities:

1. **Change Request Management**: Establish a systematic process (Following CMMI/ITIL/any standard) for submitting, evaluating, and approving change requests, considering their impact, priority, and alignment with Business as well as organizational objectives.

2. **Change Planning and Documentation:** Develop change plans that outline the objectives, scope, timelines, resource requirements, and risks associated with proposed changes. Document all changes and associated processes (Incident Management, Problem Management, and Release Management).

3. **Stakeholder Communication:** Establish effective communication channels and strategies to keep stakeholders informed about upcoming changes, their benefits, and potential impacts. Provide regular updates and address concerns or queries.

4. **Training and User Support**: Develop training materials, conduct training sessions, and provide user support to ensure users understand the changes, their implications, and how to utilize the updated feature effectively.

5. **Change Implementation and Testing:** Execute changes following a structured and controlled approach, including proper testing, validation, and quality assurance. Minimize disruptions and errors during implementation.

6. **Post-Implementation Evaluation:** Monitor the effectiveness and performance of implemented changes, gather feedback from stakeholders, and evaluate the impact of changes on the Nothi's efficiency and user satisfaction.

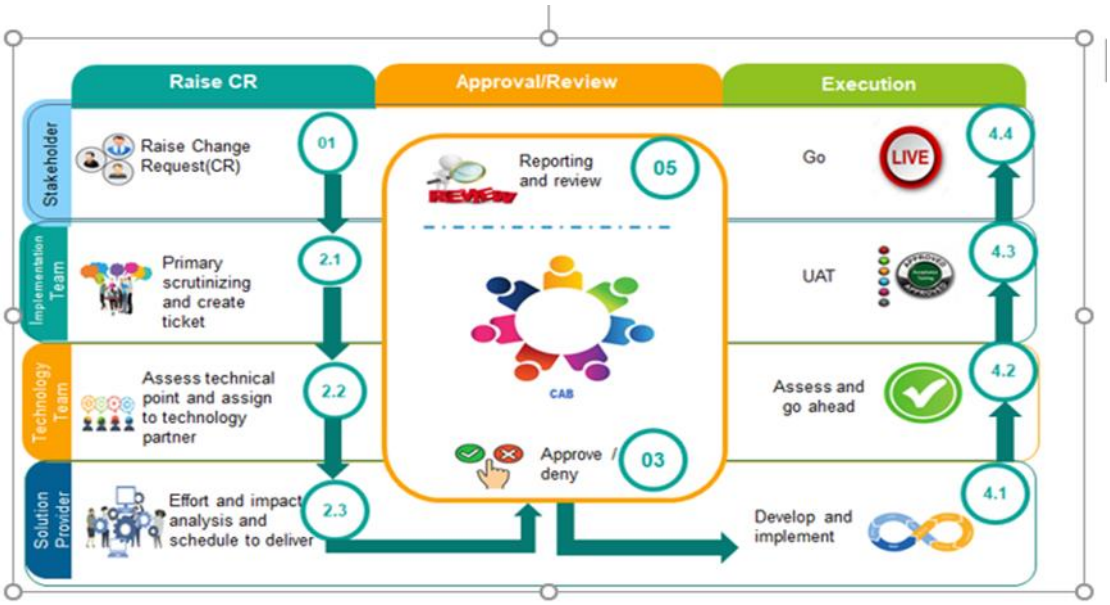


Figure: Existing change management Process

Deliverables

1. **Change Management Plan:**

   Detailed documentation outlining the approach, objectives, scope, and timelines for managing changes within the Nothi System. Change request processes, evaluation criteria, and approval mechanisms are described.

2. **Change Request Forms and Templates:**

   Development of standardized forms and templates for submitting, evaluating, and approving change requests. Documentation of change details, including impact assessment, risk analysis, and resource requirements.

3. **Communication and Stakeholder Engagement Strategies:**

   Documentation of communication plans and strategies to effectively engage and inform stakeholders about upcoming changes, benefits, and potential impacts. have to prepare the communication materials, such as emails, support Tool and presentations, to keep stakeholders informed.

4. **Training Materials and User Support:**

   Training materials, user guides, and documentation explaining the changes, their implications, and how to effectively use the updated Nothi. Conducting training sessions and providing user support to ensure smooth user adoption of the changes.

5. **Change Implementation and Testing Reports:**

   Documentation of the change implementation process, including testing activities, quality assurance measures, and implementation schedules. Reporting on the

outcomes of the change implementation, highlighting any issues, resolutions, and lessons learned.

6. **Post-Implementation Evaluation and Improvement Reports:**

   Evaluation reports assessing the effectiveness of implemented changes, gathering feedback from stakeholders, and identifying areas for further improvement. Recommendations for continuous improvement to enhance the efficiency and user satisfaction of the Nothi.

4. Expected Deliverables & Payment Schedule

The assignment is scheduled to last for 24 months. The selected firm will be required to sign separate agreements, including an SLA and NDA, for smooth implementation of the contract.

Deliverables:

SL	REf. Name	Major Deliverables
1	D-1	Inception Report
2	D-2	Technical Document - SRS, FRS, Data dictionary, EA diagram, HLD, Test Report, QA Report,
3	D-3	3.3.1 Enhancement of existing Core service framework & Core Service and Shared Service Management
4	D-4	3.3.2 SSO, SLO and Access Management:
5	D-5	3.3.3 Central Dashboard:
6	D-6	3.3.4 Identity Management
7	D-7	3.3.5 Digital Service Standard Portal
8	D-8	3.3.6 Office Organogram:
9	D-9	3.3.7 Doptor Marketplace
10	D-10	3.3.8 Doptor Calendar
11	D-11	3.3.9 Distributed Queue Manager:
12	D-12	3.3.10 Audit Trail:
13	D-13	3.3.11 API Manager:
14	D-14	3.3.12 QR Code Generator:
15	D-15	3.3.13 AI-powered Digital Assistant:
16	D-16	3.3.14 Doptor Authenticator:
17	D-17	3.3.15 eSign gateway
18	D-18	3.3.16 Data Management (Data Analytics):
19	D-19	3.3.17 Real-time Application (RTA) frontend:
20	D-20	3.3.18 Smart Support Management:

21	D-21	3.3.19 Serverless Architecture Oriented Development:
22	D-22	3.3.20 Building Blocks:
23	D-23	3.3.21 Notification
24	D-24	3.3.22 Integration Adapters/ Information mediator
25	D-25	3.3.23 Task Manager
Non Functional Requirement		
26	D-26	Support & Maintenance
27	D-27	Analysis report, Test Report , Plan document, Technical Document, Load Test Report
28	D-28	Workshop, Training & Knowledge Transfer
29	D-29	Security and Privacy Policy
30	D-30	Change Management Plan

Sl. No.	Major Areas	Deliverables	Deadline	% of Amount
1	D1: Inception Report	D-1 Inception report with proper project plan	15 days after signing the contract	05% (upon accepted by client)

2 (Q1)		D-1 Inception Report D-2 Technical Document - SRS, FRS, Data dictionary, EA diagram, HLD, Test Report, QA Report, D-3 3.3.1 Enhancement of existing Core service framework & Core Service and Shared Service Management D-4 3.3.2 SSO, SLO and Access Management: D-6 3.3.4 Identity Management D-7 3.3.5 Digital Service Standard Portal D-8 3.3.6 Office Organogram: D-13 3.3.11 API Manager: D-14 3.3.12 QR Code Generator: D-16 3.3.14 Doptor Authenticator: D-17 3.3.15 eSign gateway D-19 3.3.17 Real-time Application (RTA) frontend: D-23 3.3.21 Notification D-24 3.3.22 Integration Adapters/ Information mediator D-26 Support & Maintenance D-27 "Analysis report, Test Report , Plan document, Technical Document, Load Test Report" D-28 Workshop, Training & Knowledge Transfer Workshop on review deliverables and technology upgrade - 6 Workshop on UI/UX Design for Portal and MarketPlace -2 D-29 Security and Privacy Policy D-30 Change Management Plan	End of 04 months after signing the contract	10% (upon accepted by client)

3 (Q2)		D-2 Technical Document - SRS, FRS, Data dictionary, EA diagram, HLD, Test Report, QA Report, D-3 3.3.1 Enhancement of existing Core service framework & Core Service and Shared Service Management D-4 3.3.2 SSO, SLO and Access Management: D-6 3.3.4 Identity Management D-7 3.3.5 Digital Service Standard Portal D-8 3.3.6 Office Organogram: D-13 3.3.11 API Manager: D-14 3.3.12 QR Code Generator: D-16 3.3.14 Doptor Authenticator: D-17 3.3.15 eSign gateway D-19 3.3.17 Real-time Application (RTA) frontend: D-23 3.3.21 Notification D-24 3.3.22 Integration Adapters/ Information mediator D-26 Support & Maintenance D-27 "Analysis report, Test Report , Plan document, Technical Document, Load Test Report" D-28 Workshop, Training & Knowledge Transfer Workshop on review deliverables and technology upgrade - 6 D-29 Security and Privacy Policy D-30 Change Management Plan	End of 08 months after signing the contract	20% (upon accepted by client)
4 (Q3)		D-3 3.3.1 Enhancement of existing Core service framework & Core Service and Shared Service Management D-5 3.3.3 Central Dashboard: D-9 3.3.7 Doptor Marketplace D-10 3.3.8 Doptor Calendar D-11 3.3.9 Distributed Queue Manager: D-12 3.3.10 Audit Trail: D-15 3.3.13 AI-powered Digital Assistant: D-18 3.3.16 Data Management (Data Analytics): D-20 3.3.18 Smart Support Management: D-21 3.3.19 Serverless Architecture Oriented Development: D-22 3.3.20 Building Blocks:		

		D-24 3.3.22 Integration Adapters/ Information mediator D-25 3.3.23 Task Manager D-26 Support & Maintenance D-27 "Analysis report, Test Report , Plan document, Technical Document, Load Test Report" D-28 Workshop, Training & Knowledge Transfer Workshop on review deliverables and technology upgrade - 6 Workshop on UI/UX Design for Portal and MarketPlace -2 D-29 Security and Privacy Policy D-30 Change Management Plan		
5 (Q4)		D-2 Technical Document - SRS, FRS, Data dictionary, EA diagram, HLD, Test Report, QA Report, D-3 3.3.1 Enhancement of existing Core service framework & Core Service and Shared Service Management D-5 3.3.3 Central Dashboard: D-9 3.3.7 Doptor Marketplace D-10 3.3.8 Doptor Calendar D-11 3.3.9 Distributed Queue Manager: D-15 3.3.13 AI-powered Digital Assistant: D-18 3.3.16 Data Management (Data Analytics): D-20 3.3.18 Smart Support Management: D-21 3.3.19 Serverless Architecture Oriented Development: D-22 3.3.20 Building Blocks: D-24 3.3.22 Integration Adapters/ Information mediator D-26 Support & Maintenance D-27 "Analysis report, Test Report , Plan document, Technical Document, Load Test Report" D-28 Workshop, Training & Knowledge Transfer Workshop on review deliverables and technology upgrade - 6 D-29 Security and Privacy Policy D-30 Change Management Plan	End of 12 months after signing the contract	15% (upon accepted by client)
6 (Q5)		D-2 Technical Document - SRS, FRS, Data dictionary, EA diagram, HLD, Test Report, QA Report, D-7 Service Orchestration/Management D-14 AI-Powered Digital assistance D-17 Data management D-20 Serverless Architecture Oriented Development D-21 Building Block D-26 Support & Maintenance		

		D-27 "Analysis report, Test Report , Attendance Sheet , Plan document, Technical Document" D-28 Integration Scope D-29 Workshop, Training & Knowledge Transfer Training (ToT) on Organogram Builder/ Service Portal - Industry & Tech People Govt. (System Analyst) - 4 Workshop on review deliverables and technology upgrade - 6 D-30 Security and Privacy Policy D-31 Change Management Plan		
7 (Q6)		D-2 Technical Document - SRS, FRS, Data dictionary, EA diagram, HLD, Test Report, QA Report, D-3 3.3.1 Enhancement of existing Core service framework & Core Service and Shared Service Management D-26 Support & Maintenance D-27 "Analysis report, Test Report , Plan document, Technical Document, Load Test Report" D-28 Workshop, Training & Knowledge Transfer Workshop on review deliverables and technology upgrade - 6 D-29 Security and Privacy Policy D-30 Change Management Plan	18 months after signing the contract	
8		Closing Report		5% (upon accepted by client)

5. Work Distribution & Team Composition

SL	Position	No. of Person	Qualification	Job Description
1.	Team Lead	1	i) Minimum Academic requirement is graduation in Computer Science and Engineering/ICT degree from a recognized University ii) Minimum 5 years of experience in managing large scale IT projects with a total of 10 years of experience in ICT industry.	The Team Lead is responsible for the day-to-day operational management of the Doptor project, including overseeing the work and preparation of project progress reports. The chosen candidate will be responsible for regular reporting to the client and ensuring effective communication throughout the project. They will also be responsible for overseeing all technical aspects of the Doptor project implementation, including analyzing the user requirements, developing software design specific to myGov, selecting the appropriate technical solutions, and ensuring the successful implementation for long-term sustainability.
2.	Security Expert	1	i) Minimum graduate in Computer Science and Engineering / relevant subjects. ii) Minimum 5 years of experience in IT System security with a total of 7 years of experience in the ICT industry. iii) Firm Certification e.g (ISSP/CEH/ISO/CISA/CISM is expected) will get advantage.	Develop plans to safeguard computer files against unauthorized modification, destruction or disclosure. Choose, implement, monitor and upgrade computer anti-virus and malware protection systems Encrypt data transmissions and erect firewalls to conceal confidential information during transmit Modify security files to incorporate new software, correct errors, and change user access status Perform risk assessments and tests on running data processing activities and security measures

				Educate workers about computer security and promote security awareness and security protocols
3.	Infrastructure Expert	1	i) Minimum graduate in Computer Science and Engineering/ICT or any other relevant Science disciplines from any University. ii) Must have a minimum 05 years of profound experience in the field of system installation, configuration.	Infrastructure Administrator will be responsible for Supervising, Leading and Guiding the Infrastructure Team. Designing and Executing Strategic Plans to assure Infrastructure Capacity Attains Current and Future Needs.Defining and Managing IT Disaster Recovery Strategy. Reporting and Preparing Strategies to Maintain Server and Evaluating System's Performance. Determining Network and System Requirements. Maintaining Integrity of The Network, Server Deployment And Security
4.	Senior Developer	1	i)Minimum graduate in Computer Science and Engineering/ICT or any other relevant Science disciplines from any University. ii)Should have a minimum 7 years of profound experience in the field of web-based software	Conduct requirement analysis for a particular ICT for development solution Develop the necessary business and system specifications Provide assistance to develop system design for any technical solutions Develop URS, SRS for any outsourcing of project work. Carry out the technical evaluation for project development standardization Monitor execution of the outsourced project work programming/coding/scripting for ICT based application or Software development. Experience needs to focus on

				multiple development platforms including PHP
5.	Developer	5	i)Minimum graduate in Computer Science and Engineering/ICT or any other relevant Science disciplines from any University. ii)Should have a minimum 3 years of profound experience in the field of web-based software	The Developer will develop code accordingly to ensure the product's usability and stability based on requirements. Assist team members in critical areas of programming. programming/coding/scripting for ICT based application or Software development. Experience needs to focus on multiple development platforms including PHP
6.	AI/ML & Data Expert	1	i) Minimum graduate in Computer Science/CSE/Software Engineering or any other relevant disciplines from any University. ii) Should have a minimum 3 years of profound experience in the field of artificial intelligence (JAVA/C/ Python/R, JavaScript, SQL, machine learning and data science) with a total of 7 years of experience in the ICT industry.	Coordinate with data engineer to Collaborate with Data Scientists, Data Architects and Business Analyst to ensure alignment between the business objectives and the analytics back end as well as ensure the scalability security of the final product.
7.	AI/ML & Data Engineer	2	i)Minimum graduate in Computer Science/CSE/Software Engineering or any other relevant disciplines from any University. ii)Should have a minimum 02 years of profound experience in the field of artificial intelligence (JAVA/C/ Python/R, JavaScript, SQL, machine learning and data science) with a total of 05 years of experience in the ICT industry.	Collaborate with Data Scientists, Data Architects and Business Analysts to ensure alignment between the business objectives and the analytics back end as well as ensure the scalability security of the final product.

8.	Technical Document Expert	1	i) Minimum graduate in any Computer Science or any other relevant discipline. ii)Should have a minimum 02 years of profound experience in the field of technical documentation with a total of 05 years' industry experience.	Technical document expert will ensure Record Technical description of features, API, 3rd party integration. Guide technical writer to prepare user manual by describing the current flow of application. Also deliver the release notes to the team lead with proper explanation for the user.
9.	Technical Document Writer	1	i) Minimum graduate in any Computer Science or any other relevant discipline. ii)Should have a minimum 01 years of profound experience in the field of technical documentation with a total of 3 years' industry experience.	Technical document writers record technical description of features, API, 3rd party integration. prepare a user manual of the application. Create release notes with proper explanation for user
10	Senior DevOps Engineer	1	i) Minimum graduate in Computer Science and Engineering/ICT or any other relevant Science disciplines from any University. ii) Must have a minimum 05 years of profound experience in the field of system installation, configuration.	A Senior DevOps Engineer is responsible for assisting the senior DevOps Engineer in designing, automating, and maintaining the infrastructure, implementing CI/CD pipelines, and ensuring security and scalability in software development and deployment.
11.	DevOps Engineer	1	i) Minimum graduate in Computer Science and Engineering/ICT or any other relevant Science disciplines from any University. ii) Must have a minimum 03 years of profound experience in the field of system installation, configuration.	A DevOps Engineer is responsible for assisting the senior DevOps Engineer in designing, automating, and maintaining the infrastructure, implementing CI/CD pipelines, and ensuring security and scalability in software development and deployment.
12.	UI/UX Expert	1	i)Minimum graduate in Computer Science and Engineering/ICT or any other relevant Science disciplines from any University. ii)Should have a minimum 03 years of profound experience in the field of UI/UX.	This role is about designing the interface to ensure it delights the user.

13.	UI/UX Designer	2	i)Minimum graduate in Computer Science and Engineering/ICT or any other relevant Science disciplines from any University. ii)Should have a minimum 01 year of profound experience in the field of UI/UX.	This role is about designing the interface to ensure it delights the user. He/she will support the UI/UX Expert to ensure the proper design of the interface and user satisfaction.
14.	QA Lead	1	i) Minimum graduate in Computer Science and Engineering/ICT. ii) At least 5 years of progressive experience in Quality Assurance.	QA Lead will oversee the activity of the quality assurance, developing, implementing, and maintaining a system of quality and reliability testing for the System.
15.	QA Engineer	2	i)Minimum graduate in Computer Science and Engineering/ICT or any other relevant Science disciplines from any University. ii)Should have a minimum 03 years of profound experience in the field of software quality assurance in application.	QA Engineer is expected to designing and developing automated test procedures on the basis of requirements (S)he is expected to executing the test cases all across the system following the procedures This role is about designing the interface to ensure it delights the user.
16	Support Engineer	2	i)Minimum graduate in Computer Science and Engineering/ICT or any other relevant Science disciplines from any University. ii) At least 2 years experiences on providing software support services.	Support Executive will provide support to Users from different offices that need dedicated support to run the application smoothly.

6. Qualification Criteria & Eligibility criteria

following are defined as minimum eligibility criteria:

- **Legal and Business Status:**

  The consulting firm must be a registered company/entity with a minimum of 5 years of experience in the ICT business (please provide work completion certificate or RJSC certificate applicable)
- **Financial Eligibility:**

  Must have a minimum average annual turnover of BDT 3 crore in the last 2 years supported by audited financial statements.(Please submit the necessary Documents).
- **Tax and Regulatory Compliance:**
- *Must have a valid and up-to-date (2022-2023) trade license, VAT, certificate, TIN & BIN certificate, and updated income tax payment certificate*
- **System Scale**

  At least one developed system must have the User handling capacity of more than 100,000 with min 10,000 daily log-in. Please submit the necessary Documents.
- **System Complexity**

  At least one developed system must have integration with multiple internal/external stand-alone systems/components. Please submit the necessary Documents.

- **Conditions for Multiple Firms:**
  I. If multiple firms are collaborating, a consortium agreement or a clear delineation of roles and responsibilities between the firms must be provided where one company needs to be led. Lead company needs to fulfill all conditions mentioned in this TOR.
  II. Lead company needs to fulfill all conditions mentioned in this TOR.

8. Exit Process

During the contracted period, there will be a technical team at the procurement entity side who will be engaged to gather knowledge on both the technology and operation of the platform. Once the contract expires and the platform is delivered, that team will undertake the platform. A2i will work on that to take over the responsibility on behalf of Govt. of Bangladesh will handle this technology after expiry of the contract.

ANNEXURE 01

3.1 Scope of Work

Doptor Platform: It will contain foundation architecture, core data & applications, generic processes, primary standards, principles and core architectural artifacts etc.

Enhancement of Platform, Solution and Standards

Enhancement of Doptor where Single Sign on (SSO) and Single Logout (SLO) for web, Central Dashboard, Core Services and Shared services are the main components. Update the standard and guidelines and publish through standard portal.

1.1 Enhancement of existing Core service framework

3.1.1.1 Enhancement & restructure of existing core service framework. The core service framework provides office related common services like – GEO, Office, organogram, employee profile etc. So that it is capable of serving all perspectives along with retrospective eService requirements.

1.1.2 Capacity to have a change log with history (GEO, Office, Employee, Organogram etc.)

1.2 Core Service and Shared Service Management

For system-to-system communication need to maintain existing API Manager and adopt any other technologies to manage Data sharing services-

1.2.1. Develop new RestFul API as per the requirements of other services.
1.2.2. Publish APIs/Services through the API manager / ESB
1.2.3. Manage API/Services visibility and restrict access to specific agencies or systems
1.2.4. Ensure API/Services security by restricting API access tokens to domain/IPs, validating APIs payload contents against a schema, applying security policies to APIs authentication and authorization and provide threat protection, bot detection and token-fraud detection
1.2.5. Systems should have proper capabilities to manage and scale API/ Services traffic and enforce rate limiting and dynamic throttling based on usage quotas and bandwidth quotas.
1.2.6. System should be horizontally scalable with easy deployment into clusters.
1.2.7. System should provide a pluggable analytics framework for API/ Services usage, like, requests, responses, faults, throttling, subscriptions etc.
1.2.8. System should track consumer analytics per API/Services, per API/ Services version, per tiers and per consumers

1.2.9. System should have provision to do the proper/required integration with SSO System

1.3 Maintenance and Enhancement of SSO and Access Management

Single sign-on is a specialized form of e-authentication that enables a user to authenticate once and gain access to the resources of multiple applications. With this property, a user logs in once and gains access to all systems without being prompted to log in again at each of them.

1.3.1. Maintain OpenID Connect SSO implementation.
1.3.2. Maintain Single Logout (SLO).
1.3.3. Provide Federated SSO via OpenID with external identity providers as per a2i's need.
1.3.4. Introduce support for multi-option/multi-step authentication
1.3.5. 2-factor authentication (2-FA) (hardware based or soft OTP)
1.3.6. Time-based one-time password (OTP) based authentication
1.3.7. Enhancement of Users and Group Management
1.3.8. Introduce Account recovery with email and secret questions
1.3.9. Introduce Password history validation
1.3.10. Password pattern configuration
1.3.11. Introduce account locking in single and multi-tenant environments
1.3.12. Introduce account suspension reminders and locking of idle accounts

1.3.13. Should have proper monitoring, reporting and auditing support by providing login events and session monitoring, user session termination, forced password reset and real-time security alerting for suspicious login activities and abnormal sessions based on rules

1.3.14. System should provide flexible deployment mechanism by supporting clustering for high availability deployment and centralized configuration management across different development environment

1.3.15. Sign in facility Mobile apps for both Android & iOS.

1.4 Api Monitoring

The system should monitor the usage of all published API. The API services are mentioned below.

- Number of requests from consumer app
- Number of API published

1.5 Service scheduler

The vendor should develop a service scheduler to run the service on a predefined scheduled basis.

1.6 Service queueing

The vendor should develop a service queuing app to run all api / services.

1.7 Enhancement of Digital service standard portal

1.7.1. Enrich the portal with proper presentation of integration guidelines to minimize in-person knowledge sharing for integration works.

1.7.2. The Portal should have a standard and document uploading panel using HTML structure and also using proper DDL.

1.7.3. The Portal should have its own document/content management system from the admin panel where documents can be listed/uploaded using various filters. Users with proper permission will be able to modify/remove standard and guideline documents as needed. Also, for each revision, the system should track versioning properly.

1.7.4. The Portal should have management dashboard and usage analytics and shares the data to the stakeholders and administrators

1.7.5. The Portal should provide an efficient search mechanism to allow users explore their queries navigating through different standard catalogs or tools of interest allowing options like keywords, different types of filters.

1.8. eService Registration

Office/eService providers will register eServices to make them accessible.

1.9 Personalized login panel

The system should have the option to upload/setup a personalized login panel for each SSO consumer application.

1.10. Help & Support

- FAQ for most commonly asked questions and answers.
- AI integrated support service

2.0 Development of common services:

2.1. **Holiday Calendar:** Maintain Government Holiday Calendar and provide API service to other Applications.

2.2. **Task Manager:** Facilitate users to create, assign tasks and manage/maintain his/her regular task and view his/her own task at a glance in Calendar Dashboard.

2.3. **Doptor Dashboard:** One dashboard for all systems. It will be a configurable dashboard which will connect all of the authorized systems/platforms of the government officer.

2.4. **Personalized Calendar:** The following features can be added in personalized Doptor Calendar-

1. Single and Recurring Event setup with Notifications.
2. Calendar sharing mechanism: Facilitate users to set their meeting/event time in the calendar as well as sharing with the team/office/external offices.
3. Invitation: Send invitation other officers and ensure necessary notifications
4. Integration with Different eservices for event creation.

2.5. **Organogram Builder:** Organogram builder and Office configuration privilege to authorized admin user –

3.2.5.1. User should have option to create self-office organogram through using Existing template

3.2.5.2. Using Drag & drop tools facilities

3.2.5.3. Using verification and approval mechanism

2.6. **Distributed Architecture** – Other systems may use Doptor as a separate instance where data will be synced with the Central instance of Doptor.

2.7. **Horizontally deployment architecture** – System should have capacity to ensure deployment of maximum 3 instances with real time synchronization with central instance. Also Staging, sandbox and live environment should be available to ensure smooth operation.

3.0 Integration

Integrating e-government solutions with Doptor through the establishment of the integration among all stakeholders (i.e., Government/non government agencies, ICT industry, academia etc.) where feasible.

1. Must provide system integration service with the various e-service streams within the government sector and business sector to ensure that the solution is properly architected end to end to deliver a successful implementation.
2. Provide required coordination between internal and external agencies for service delivery/Integration Activities;
3. Integration with Template Builder.
4. Integration with Document Signer/e-Signer.
5. Integration with the BBS system for GEO information.
6. Integration with IBAS++/PDS/PIMS may be considered for data population if these are feasible.

3.4 System integration

1. Define integration scope of the system and prepare documentation
2. Define integration process and develop necessary documentation with diagram
3. Coordination with service providers and relevant stakeholders
4. Execution of the integration as per defined scope
5. Develop necessary API for System Integration
6. Integration testing and implementation

3.5 Maintenance and Change Management of Platform, Solution

3.5.1 Maintenance, Change management and support for Enterprise Service Bus/ any other similar platform.

3.5.2 Continuous health check of Database, tuning database, tuning codes & queries and mitigating the issues.

3.5.2 Fixing all bugs in the system irrespective of its nature and complexities.

3.5.4 Developing, recording and reporting change documents, source code management and version management.
3.5.3 The Service Desk team should efficiently implement changes approved by Concern Authority.
3.5.4 The Service Desk team should implement changes ensuring no risks to the existing and integrated Services.
3.5.5 Adjust and update system in compliance with any Security test or Load test and both parties responsible for the test execution.

3.5.6 Incorporating and streamlining the system in compliance with updated versions of development tools/language/DB and ensuring availability of APIs as required for integration with other services.
3.5.7 Ensure all levels of testing prior to executing changes in the production environment.

3.6 Multi-layered Support System

3.6.1 Deploying dedicated Support Engineers for 24/7 [Including Holidays] to address support issues. This is estimated that the consulting firm will have to have three (03) dedicated Support Engineers for contract period.
3.6.2. Recording, managing reporting issues and user level application related technical problems received through the method prescribed by a2i
3.6.3. Provide active operational support to update the system in compliance with respective changes by the stakeholder.
3.6.4. Ensure a structural support management system to scrutinize the raised issue
3.6.5. Provide approval-based issue fixing facilities at LIVE environment by providing highest level of data security
3.6.6. Provide Post development support service under structured SLA and Change Management Architecture.

3.7 DPG standards:

There should be at least one component of this assignment which will maintain the DPG standards to register the product as a DPG Eligible product. The following standards are explained which should be maintained by the vendor during development.

The digital solution should define the relevant to one of the sustainable development goals.

- The solution should use an approved open-source license.
- The solution ownership should be defined clearly.
- The solution should be plant form independent.
- The functional requirement document, source code document, use case document should be available for the solution.
- The solution should collect or use non-personally identifiable information (non-Pll) data and/on content.
- The Digital solution should maintain the policy of adhering to privacy and other applicable international and domestic laws.
- The solution should adhere to standards and best practices.
- The solution should take steps to anticipate, prevent and do not harm.

3.8 Quality Assurance and testing activities

3.8.1. The Consulting firm will set up a Sandbox for system tests.
3.8.2. Unit Testing, Integration Testing, System Testing, Load Testing and Acceptance testing at every phase of the project.

3.8.3. Ensure Security testing of the system at a regular interval not more than six months by a third-party organization.
3.8.4. Fix the necessary security holes.
3.8.5. Provide the relevant testing and its resolution report.
(Note: Software Testing detailed plan is explained in section 7.9 and 7.10)

3.9 Post-Hosting Support

3.9.1. Regular performance monitoring of the server, database, application etc.
3.9.2. Providing active and operation support to Data Center as well as a2i's nominated infrastructure experts in application/DB sizing the product reconciling and adjusting with user-base and number of offices.
3.9.3. Regular database tuning and application configuration support to the hosted environment as required.
3.9.4. On-demand accountable consultancy support to Data Center in terms of Data Backup Scheduling and Back-end service execution.

3.10 Capacity Management and Knowledge Transfer by the Consulting:

3.10.1. Facilitate monthly workshops with client teams for knowledge transfer.
3.10.2. Provide authentic access to client experts to source code and documents.