NATIONAL INSTITUTE FOR SMART GOVERNMENT
ON BEHALF OF
THE GOVERNMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

Ministry of Digital Economy

BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS

Volume 02 of 03 - Annexure 11: Overview of Technology

Two Stage Bidding Procedure

FOR THE

APPOINTMENT OF A MASTER SYSTEM INTEGRATOR (MSI) FOR DEVELOPMENT, IMPLEMENTATION AND MAINTENANCE OF THE "UNIQUE DIGITAL IDENTITY (SL-UDI) PROJECT" OF GOVERNMENT OF SRI LANKA

INVITATION FOR BIDS No: NISG/SLUDI-2025

June, 2025

Table of Contents

Table of Tables

Table of Figures

1. Introduction

The following diagram illustrates the overall logical design of the SL-UDI System.

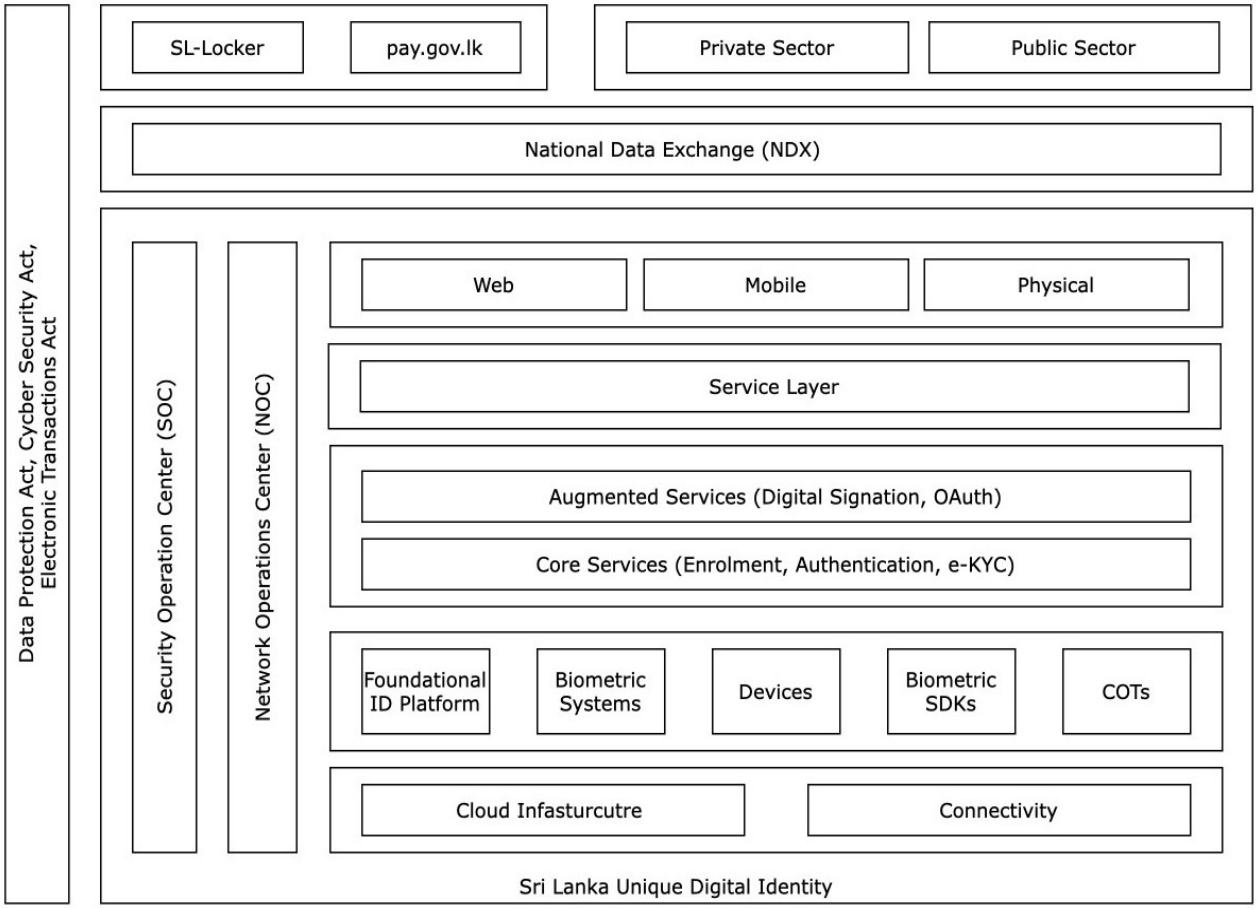


Figure 1: Overall SL-UDI

2. Solution Overview

2.1. Reference Functional Architecture

The reference functional architecture for SL-UDI is provided in the figure given below:

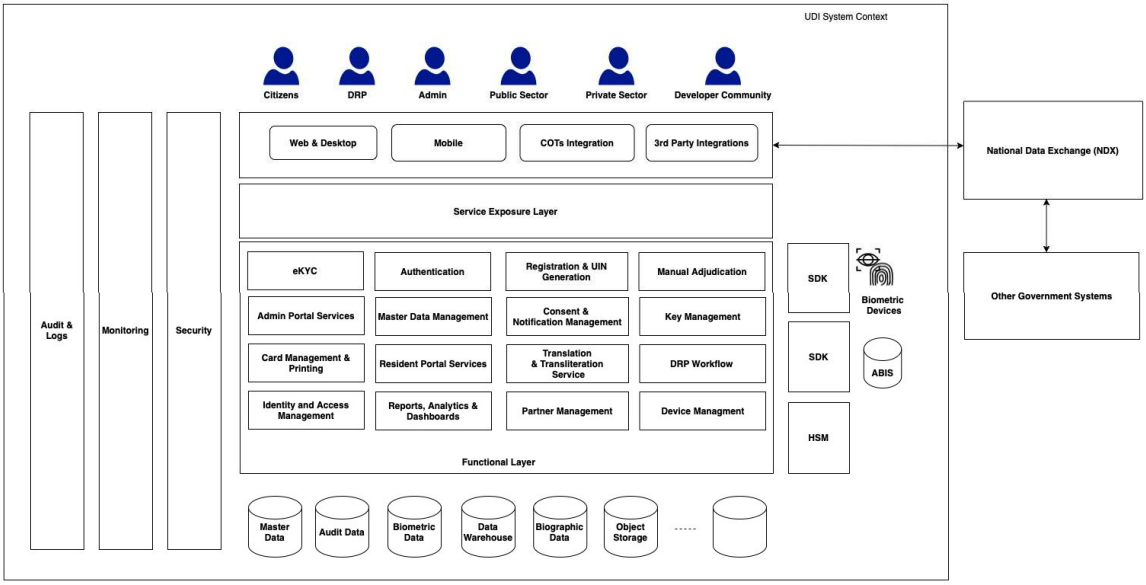


Figure 2: Reference Functional Architecture

2.2. Design Principles

The design principles to be adopted for the SL-UDI system are as follows:

- **Scalability & Modularity:** The system should be scalable in-line with the rollout plan for all IT Infrastructure. It should be modular for each business service, catered by a separate module thus ensuring separation of transactions. As the system would increase the coverage, new authentication agencies would start using the system. Therefore, the system should be designed in such a way that required hardware can be augmented into the Data Center in an incremental manner on a need basis. Data partitioning/sharding should be leveraged to ensure that system can scale with growth in data. Application scalability should be ensured using Open API's and asynchronous design in logic allowing each resource to do its job, loosely coupled through a messaging layer. Use of Open API's also provide a layer to integrate application components from different partners addressing issues related to single MSI.

- **Security by Design:** The system should have the ability to secure data from thefts, tampering, unwanted modifications, network attacks, and other security threats. Use of Hardware Security Module (HSM) Technologies, Public Key Infrastructure (PKI) based encryption, hashing algorithms, strong physical security, access management, stringent audits, non-repudiation, 24x7 Network Operations Centre (NOC) and Security Operations Centre (SOC) monitoring, data encryption should be strongly enforced to make system robust and secure from any data thefts. Further, only necessary, and minimal information would be shared after the consent by the citizen for using the online authentication service of SL-UDI.

- **Vendor Neutrality:** The system should make use of open standards, open frameworks, and open-source software to avoid MSI/vendor locking, wherever possible. The open standards allow robustness, longevity, and continuous adoption of best-in-class technology by different technology vendors. To ensure openness and vendor neutrality, system should use open standards such as ISO based biometric standards, data standards like JSON, XML, open security standards for PKI, LDAP, open protocols like https, etc.

- **Interoperability:** The system should have the ability to interoperate with other systems / services using open interfaces, open data standards and ability to continually re-factor and/or replace specific components without affecting the rest of the system. Use of MSI neutral layers like open API's based on open data standards such as XML, JSON would provide the necessary loose coupling between different components allowing technologies from different partners to seamlessly integrate with each other and which can be changed easily.

- **Manageability & Upgradeability:** The system should have the ability for end-to-end management of the components to ensure health of the system and adherence to service levels. For complete lights out operation, all layers of the system such as application, infrastructure must be managed through automation and proactive alerts rather than manual management. The entire application must be architected in such a way that every component of the system is monitored in a non-intrusive fashion (without affecting the performance or functionality of that component) and business metrics are published in a near real-time fashion. This allows data center operators to be alerted proactively in the event of system issues at a granular level. Application architecture shall also allow specific components to be watched very closely through a component level debugging scheme. The system should have the ability to seamlessly upgrade services, components, and modules without affecting services.

- **Flexibility:** The system should be designed for extensibility for specific features using a Metadata based approach, Business Rules and/or SOA based open APIs. Open Architecture adopting open standards followed by multiple partners would mean that the system can work with hardware and software procured from different partners at different times. Open APIs would enable the applications to be developed in such a way that the applications can run from mobiles, smartphones, tablets, desktops, and laptops. Further, open APIs create a layer that is MSI neutral allowing multiple partners products and applications to co-exist also enabling change of partners whenever technology or scalability issues are encountered.

- **Cost Effective:** Low-cost technology would be used to maximize benefits, avoid MSI / vendor locking, etc. Use of scale out architecture through horizontal scaling capability of hardware and data, use of open API's allowing different partners to co-exist together would ensure low Total Cost of Ownership (TCO).

- **Use of Automation:** Automation would be adopted to minimize the cost of ownership especially in areas of testing, application & infrastructure monitoring, provisioning of new environments using virtualization technology and run book automation.

- **Performance & Availability:** Infrastructure and networks should be designed to support performance as per the agreed Service Levels (SLAs). Each application should be tested to

identify and mitigate performance issues. The potential performance bottlenecks need to be identified and cost-effective paths for performance improvements should be provided for these identified problem areas. The system infrastructure should be architected considering failover requirements, rack-awareness and ensure, a single server or network link failure does not bring down the entire system. The platform solution should support effective disaster recovery.

2.3. Solution Framework and Description of Building Blocks

2.3.1 SL-UDI Software System

SL-UDI Software system shall contain MOSIP applications as well as Support applications. In order to implement the SL-UDI Software System, certain components of the SL-UDI Software System like MOSIP application would be taken over from an agency of IIIT Bangalore, India, some would be developed afresh (bespoke development) while some other components will be implemented by customizing COTS products. A list of all such components is provided below:

Key Components	MOSIP	Biometric Solution Provider	MSI - Bespoke Application	MSI - COTS Application
1. Pre-enrolment Application	Y			
2. Enrolment Client Software	Y			
3. Identity Management System	Y			
4. Unique Identity Generator	Y			
5. Authentication Solution	Y			
6. Partner and Device Management	Y			
7. Integration Middleware	Y			
8. Biometric SDK		Y		
9. Automated Biometric Identification System		Y		
10. Web Portal and Mobile Application			Y	
11. Business Intelligence and Analytics				Y
12. Customer Relationship Management				Y
13. Document Management System				Y
14. Identity and Access Management				Y
15. Service Billing System			Y	Y
16. Knowledge Management				Y
17. Knowledge Management				Y
18. Learning Management				Y

Key Components	MOSIP	Biometric Solution Provider	MSI - Bespoke Application	MSI - COTS Application
19. TSP and UA Software (Three sample applications – two in JAVA and one in .Net)			Y	
20. Enterprise Management System				Y

Table 1:Components of SL-UDI Software System

For more details, please refer to the scope of work.

2.3.2 SL-UDI-Data Store (SL-UDI-DS)

The SL-UDI-DS would form the backend of the SL-UDI System and would consist of among others the following:

Category	Component	Sub-Component
Data Centre Infrastructure	Servers	• Blade Servers • Blade Chassis • Rack Servers • Server Racks
	Storage	• SAN Storage and Disks • Tape Library and Tapes • SAN Switch • Storage Racks
	Network	• Internet Router
Network and Security Infrastructure		• MPLS Router • Global Load Balancer • Application Load Controller • Data Center Inter Connect Router • Core Switches in DMZ Zone and MZ Zone • Data Center Access Switch • User Access Switch • KVM Switch • Network Access Control • Network Racks
	Security	• Firewall (External) • Firewall (Internal) • Web Application Firewall • HIPS/NIPS/NIDS • IPS/IDS • Security Racks • SSL / IPSec VPN Box • HSM • Access Control System & Directory Services • Anti-DDoS

Category	Component	Sub-Component
		• Anti-APT • Network Detection and Response
Software Systems	System Software	• Virtualization Software • Operating System • Databases
	Application Software	• Patch Management Solution • Antivirus • API Gateway • Identity & Access Management • Enterprise Service Bus + SOA Suite • BPM/Workflow tools • Business Rules Engine • Business Intelligence and Analytics • Performance testing tool • Backup Software and Agent Licenses • Application Container Platform • Web Servers • Messaging Platform-Publish/Subscribe Queues • Large-Scale Random-Access Storage • UI, Portal, etc. • Program / Project Management Tool • Distributed Caching • Customer Relationship Management • Document Management System • Enterprise Management System
	Security Software	• DLP Solution • Email Gateway (Security Solution) • Web Gateway with content Filtering & Proxy Solution • 2 Factor Authentication • SIEM solution (incl. UEBA features) • Security Orchestration and Automation and Response (SOAR) • PIM/PAM with TACACS • Virtual Desktop Infrastructure Solution • Database Activity Monitoring • Web Vulnerability Scanner • Code Review Tool • Network Vulnerability Scanner • Anti-APT • Endpoint / Extended Detection and Response Solutions

Table 2: Components of SL-UDI-Data Store

For more details, please refer to the scope of work.

2.3.3 SL-UDI-DS Operations

IT systems once live would be managed by SL-UDI-Operations team. Following would be some of the key areas for SL-UDI-DS:

Technology Management[1]	Incident Management
Change Management	Event Management and Correlation
Problem Management	Configuration and Asset Management
Application Support	Availability, Performance and Capacity Management
IT Helpdesk	Tools Management
Release Management	Partner onboarding
Procurement and Provisioning	Other components (e.g., asset management)

Table 3: SL-UDI DS

[1] DBA, Server, Virtualization, Storage and Backup, Network, Middleware Administration

For more details, please refer to the scope of work.

2.3.4 Software Lifecycle Management and Release Management

The implementation of SL-UDI Software System shall span across the following stages of software development lifecycle:

Requirements Gathering	Design
Development and Customization	Testing
Release (Including User Acceptance)	Operational Acceptance
Continuous Build	

Table 4: SL-UDI Software System

For more details, please refer to the scope of work.

2.3.5 Solution Integration

SL-UDI Software System will need to integrate with external systems. Within the SL-UDI Software System, there will also be a need to integrate different components. There are four major channels of integrations namely Open API's, ETLs, Secure transfer mechanism, and Integration Middleware. These are described below in detail:

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

   a. **Choice/Flexibility**: Users across the SL-UDI ecosystem gets the choice and flexibility of using their preferred application and user interface without having to depend on a single

portal.

b. **Innovation**: Application ecosystem can innovate in terms of providing all kinds of features such as offline capabilities, alerting capabilities, mobile/tablet interfaces, and so on as device and **user** interface technologies evolve without SL-UDI Information System to build all possible features into a single portal.

c. **Agility**: When entire system is loosely coupled via components exposing APIs, it allows individual API implementations to change without having to affect the rest of the system. Building the **entire** system as a monolithic application completely takes away the agility of SL-UDI to adapt to the changing policy decisions and rules. API driven approach allows encapsulation of components and data models without every other part of system knowing the details. API based design also allows automated testing of the entire system to ensure changes are quickly tested in a completely automated way to avoid regression.

d. **Manageability**: API based systems allow easy manageability in terms of monitoring, auditing, and performance analysis. In addition, individual APIs can be version controlled and deployed/upgraded/rolled-back instead of entire application being released, tested, and deployed.

e. **Scale**: For a national system like SL-UDI to scale, load has to be distributed across various systems. This is key **for** responsive user experience as well as core system scaling. Instead of entire application being monolithic and access via web portal, it should be built with stateless APIs that can be scaled horizontally. Most critically, user interface load is distributed to external applications making SL-UDI Information System truly a lean platform that can be scaled to country's need. Providing stateless APIs allow load balancing across Data Centers for scale and distributing user interface load to 3rd party applications.

f. **Data consistency**: Providing APIs to access all data models and functionality ensures data is not duplicated unnecessarily. This offers a single source of truth of data to be managed via common APIs. In addition, providing centralized data validation, digital signature, etc. ensures data is consistent and accurate across the system.

g. **Security**: Data security is paramount to SL-UDI Information System. Accessing data only via APIs ensure centralized management of security controls. Encapsulating access control, auditing, confidentiality (via encryption), and integrity (via signatures) is only possible via common APIs.

h. **Cost effective**: Most importantly, SL-UDI Information System can be kept simple, scalable, API driven, 3rd party application driven, and agile to meet the changing needs of residents, ecosystem partners, and policy makers which ensures that the cost of entire system is kept minimal while providing all core features and functionalities.

ii. **ETL** would be used **for** integration of all application data with the Data Warehouse, Business Intelligence, Analytics, , etc.

iii. **Secure transfer mechanism** would be used for secured transfer of enrolment packets from enrolment centers to IDMS.

iv. **Enterprise Service Bus / Integration Middleware:** For hosting all the web service/API endpoints for internal consumption and external consumption by Pre-enrolment and other

applications

2.4. Framework for MOSIP Solution

International Institute of Information Technology, Bangalore (IIIT Bangalore), India has constituted a MOSIP society with global experts. IIIT, Bangalore, India has entered into an agreement with DRP to provide MOSIP application suite (refer www.mosip.io), along with relevant documentation, which shall form a part of the SL-UDI Information System.

2.4.1 Guiding Principles

The MOSIP philosophy is to provide a "Good ID". As part of this MOSIP embraces a core set of design and architecture prin1ciples that allow the platform to offer best practices for a Good ID system. MOSIP is built on the following architecture principles

i. MOSIP must follow **platform-based approach** so that all common features are abstracted as reusable components and frameworks into a common layer

ii. MOSIP must follow **API first** approach and expose the business functions as RESTful services

iii. MOSIP must **not use proprietary** or commercial license frameworks. Where deemed essential, such components must be encapsulated to enable their replacement if necessary (to avoid MSI lock-in)

iv. MOSIP must use **open standards** to expose its functionality (to avoid technology lock- in)

v. Each MOSIP component must be independently **scalable** (scale out) to meet varying load requirements

vi. MOSIP must use **commodity computing** hardware & software to build the platform

vii. Data must be **encrypted** in-flight and at-rest. All requests must be authenticated and authorized. Privacy of Identity Data is an absolute must in MOSIP

viii. MOSIP must follow the following manageability principles – **Auditability** & monitor ability of every event in the system, testability of every feature of the platform & easy upgrade ability of the platform

ix. MOSIP must follow the principles of **Zero-Knowledge** which means that the services know nothing about the Personally Identifiable Information (PII) data stored.

x. MOSIP components must be **loosely coupled** so that they can be composed to build the identity solution as per the requirements of a country

xi. MOSIP should work with different locales so that that ID systems can be localized for languages and cultures easily.

xii. All modules of MOSIP should be resilient such that the solution as a whole is **fault tolerant**

xiii. The key sub-systems of MOSIP should be designed for **extensibility**. For example, if an external system has to be integrated for fingerprint data, it should be easy to do so.

2.4.2 Components of MOSIP

i. MOSIP application suite shall comprise of the following applications which will have to be customized and integrated with other components by the MSI:
   a. **Pre-Enrolment Application**: This application shall allow the residents to submit pre-

enrolment information through a web-based portal or mobile app interface and obtain appointment at enrolment centers.

b. **Enrolment Software:** This application shall be hosted on a Desktop/Laptop of the Enrolment Officer and will be used for enrolment of the citizen. The Enrolment Officers would login using the SL-UDI number and their own biometrics. With regard to citizen enrolment, through this software, the Enrolment Office will fetch the pre- enrolment information (wherever applicable), enter remaining demographic information, scan supporting documents, capture photograph and biometrics (all fingerprints and both iris), fetch the photograph taken from the Studios. Citizen information once captured would be stored in the desktop/laptop in an encrypted format for onward transmission to SL-UDI-DS in a secure format.
c. **Identity Management System**: This application shall receive the enrolment packet and process it in a sequential staged manner from the validation of the packet, Verification activities by the Department of Registration of Persons, to the generation of SL-UDI number and intimation of the SL-UDI to the citizen. This application shall contain a management and a core layer. The management layer will orchestrate requests, and the core layer will host the business logic.
d. **SL-UDI Generator:** The unique identity numbers to be allocated in the SL-UDI system would be sourced from the SL-UDI generator. Thus, every successful transaction confirmed from all stages will be assigned a unique number from this generator.
e. **Authentication Solution:** This software application shall provide online authentication and e-KYC services. **The** core functions of authentication solution shall include the following:
    i) An extractor which extracts the biometric templates for newly enrolled residents and stores in a citizen database. The citizen database would be used for biometric based authentications.
    ii) The biometric matcher shall compare on 1:1 matching the biometric templates received as part of a biometric authentication request with the biometric template of citizen stored in citizen database after enrolment.
    iii) A set of open APIs for different types of authentications (Demographic, Biometric and OTP).
    iv) A cached OTP retained and deemed valid for designated time period. Authentication requests would come to this application through an array of Trusted Service Providers (TSP) and User Agencies (UA).
f. **Partner and Device Management:** The Partner and Device management application would **cater** to the needs of the partner community, which includes the Trusted Service Providers, User Agencies and Enrolment Centers.
    i) Administration and User Management of Enrolment Community: The application would allow Administrators to setup new users as Enrolment officers by allotting them a unique Number. This application would also allow the setup of Enrolment centers and manage the lifecycle of these centers.
    ii) View Statistics and KPI's for Enrolment Community: This application would provide the **capability** to view statistics related to enrolment at various enrolment centers such as time taken for enrolment, number of enrolment packets that failed from an enrolment center/ enrolment officer, etc.

iii) **Administration and User Management of TSPs and UAs:** The application would allow **administrators** to setup new users as TSP/UAs along with their credentials etc. This would **allow** for registration of devices, services permitted (w.r.t. limited e-KYC).

iv) View **Statistics and KPI's for Authentication statistics:** This application would provide the **capability** to view statistics related to authentication Partners, such as number of authentications handled by a particular TSP.

v) **Drill into individual issues:** This application would have capability to provide insights into **individual** performance issues of TSP, UA, or Enrolment Officers to improve their performance.

g. **Integration Middleware:** Data exchange between the SL-UDI Information System and other **Internal**/External Systems will be carried out through APIs. The MSI, in consultation with GoSL, will also be required to set up a process for issuance of standards for the SL-UDI Information System APIs. The MSI needs to set up, operationalize and maintain system for APIs. As other systems may transmit data in CSV (or other) format; the MSI would build a converter/adapter to convert XML into the desired format or vice versa. The convertor/adapter will reside in the SL-UDI Information System environment and will parse the data as and when received. A utility will also need to be built to push or pull information to or from the other departmental systems based on event triggers. The exchange of information with other departments may be a batch exchange of data or live integration on a transactional basis. The utility may reside both in the department environment as well as in the SL-UDI's environment based on requirement for data exchange and feasibility to change in department side application. **The MSI shall be entirely responsible for customization of the solution which satisfies all features, functions and performance requirements as captured during requirements gathering stage and as described in RFP and relevant documents**.

ii. The MOSIP architecture decisions have been based on the defined charter. The design choices are in line with the need for modularity, loose coupling, and scalability of its components, and being API first.

- Micro-service-based architecture for all platform services for modularity and scalability.
- Staged Event Driven Architecture (SEDA) for processing Registration data for extensibility.
- Thick client architecture for the registration client to support offline operations as well as process security.

iii. The functional architecture of MOSIP is depicted in the diagram given below, for details please refer to MOSIP website ().

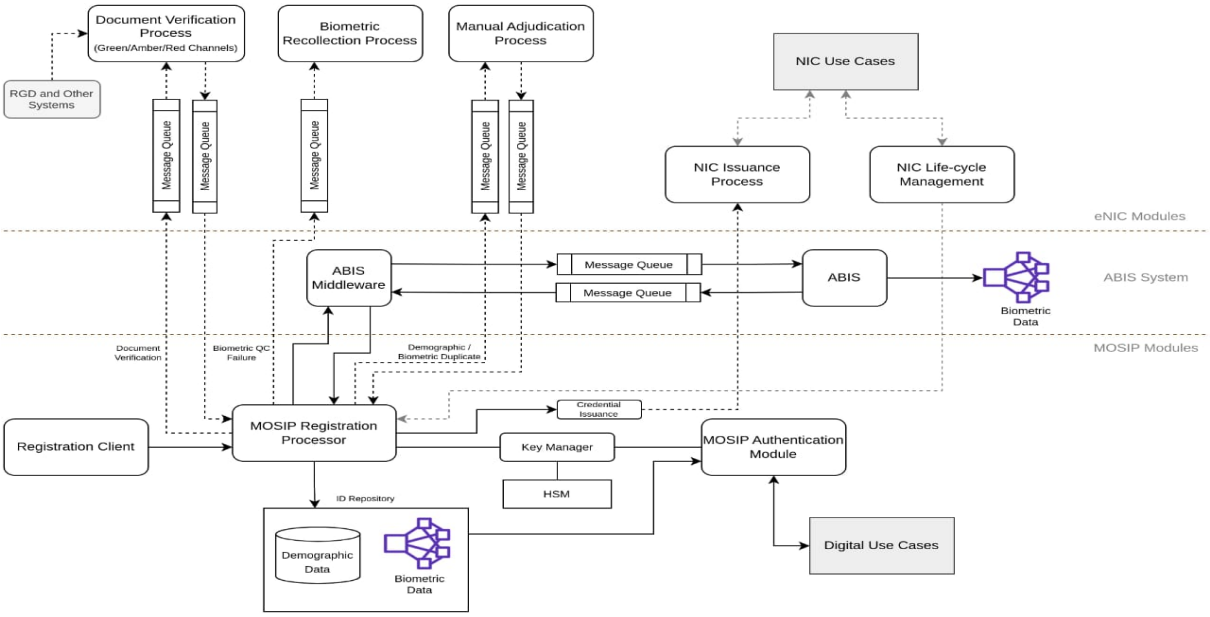


Figure 3: functional architecture of MOSIP

iv. The MOSIP, as far as possible, is built on free and open-source components. The Technology Stack of MOSIP is provided on its website (https://docs.mosip.io/platform/architecture/mosip-architecture/technology-stack).

v. International Institute of Information Technology, Bangalore (IIIT Bangalore), India, and its nominated agency shall provide the requirements, architecture, design specifications, drawings, performance benchmark, etc.

vi. MOSIP application suite shall be provided to the <Nominated Agency>by a nominated agency of IIIT Bangalore, India under a license like Mozilla Public License v2.0. The MOSIP software (long term version) can be downloaded from MOSIP website. This software needs to be customized as per the requirements of the Sri Lanka Unique Digital Identity program.

2.5. Framework for Biometric Solution

2.5.1 Guiding Principles

The administrative policies of <Nominated Agency>will impact the design and operation of both the ABIS and the enrolment software. In this section, we enumerate the current policies, which needs to be further detailed during the requirement gathering phase to include all improvements and additions where applicable:

1. With regard to slap fingerprints, search outcome should not be impacted by inversion of thumb placement.
2. Iris images will be automatically labelled by the capture device as left or right and therefore this label may be used to restrict iris searches for de-duplication.
3. ABIS system should not restrict the search on the basis of demographics (gender, age, location) initially, but this capability should be preserved for potential insertion at a later stage in the program.

4. Face photo image enhancement at the enrolment software may include cropping and rotation but must not include non-reversible grey-level alterations (i.e., pose and illumination normalization).
5. The ABIS system must create a record in the reference database whenever SL-UDI Application invokes INSERT method regardless of biometric image quality.
6. With the growth of the database, <Nominated agency> may require the BSP to enhance or replace algorithm. The ABIS should be structured to allow for replacement, enhancement, or insertion of new algorithm.
7. De-duplication flow over multiple modalities can be chosen by the BSP. However, <Nominated agency> may upon review of results, may require that MSI must perform de-duplication on all (fingerprint, iris, and face) modalities fully.
8. Authorizations for all requests will be verified at the SL-UDI application level. Therefore, all requests sent by the SL-UDI application to the ABIS can be assumed to be from an authorized source.
9. During enrolment as well as authentication, the biometric capture devices of various OEM's will be utilized. These biometric devices will be compliant to the defined biometric standards (Section 2.5.3). The biometric solution should be device agnostic i.e., should operate properly with biometric capture devices, of different OEMs, meeting the aforementioned biometric standards.

2.5.2 Biometric Solution Design Principles

Following are the key design principles for the biometric solutions that shall be developed by the BSP:

1. **Modularity**: The design must allow for replacement and updating of various components, from various partners, without any impact on the other components. The components in this context should be as fine grained as possible. For example, the enrolment server and authentication server are fully decoupled and will use separate database and could use different matcher.
2. **Standards**: Use of standards prescribed by <Nominated agency> is mandatory. All interfaces to the outside systems must be based on current industry standards adopted by <Nominated agency> for maximum interoperability. Use of open source also aids in standardization.
3. **Avoidance of MSI lock-in**: In the area of biometrics, proprietary algorithms and data representation are perhaps required to achieve performance and accuracy requirements of the <Nominated agency>. The system is designed such that these algorithms and data representation form a part of the black box, **and the entire box or a sub-system can be r**eplaced without any impact on the other biometrics black boxes. All proprietary data formats needed within each solution are not exposed outside of the black box.
4. **Resident Convenience**: The entire process of enrolment and authentication must be conducted with strict conformance to quality and precision. At the same time, the process will provide transparency, flexibility, and convenience to the residents. For example, the collection of biometric features will have user interface that is consistent with these requirements.
5. **Risk Mitigation**: Sri Lanka is proposing to undertake biometric collection of the entire

population and biometric authentication for service delivery. As the quality and availability of biometric measures across the population is currently not known, alternate methods for de-duplication and fallback strategy must be incorporated in the design to ensure quality.

6. **Universality:** To support scalability and inclusiveness of the solution, three biometric profiles will be collected fingerprint, face, and iris. Fingerprint will be all 10-fingerprints, Iris images will be collected in pairs and facial image will be full frontal.
7. **Security:** Biometric Solution must be secure and conform to Government of Sri Lanka's data security and DRP's security guidelines, including encryption and decryption. For example, all personal information stored on a permanent storage media must be encrypted.
8. **Enrolment data quality:** The quality of data depends on enrolment process and technology. DRP will use best practices for enrolment process and utilize optimum technology to capture best quality of data while ensuring that no one is denied enrolment due to poor biometric data. A number of techniques such as operator enrolment and verification of enrollee's biometric against all registered operators and supervisors will be performed at the enrolment station.
9. **Service Oriented Architecture:** The biometric components follow SOA principles. They provide specific services using well defined interfaces.
10. **Isolation -** ABIS will not have access and should not try to access any network resources except the resources referenced by the URLs provided through the API.
11. **DBMS –** The DBMS should be compatible with RDBMS of SL-UDI application and should be able to import/export data with ease
12. **Distributed Database** – Solution should provide distributed database for the purpose of authentication.

2.5.3 Biometric Standards

The biometric solution should be compliant with MOSIP standards mentioned at Biometric Specification | MOSIP Docs 1.1.5

2.5.4 Biometric Solution Architecture Requirements

Given below is the biometric architecture requirement.

S. No.	Dimension	Requirement
1.	Scalability	Dynamic or rule-based ability to scale the system within servers, across servers without inherent bottlenecks and code changes, and ability to scale at data centers. ▪ The system shall have ability to scale dynamically within a server depending upon the load. ▪ The system shall have ability to add nodes dynamically without bringing the system down. ▪ The system shall have ability to utilize dynamically increased CPU, RAM, and storage. ▪ The system shall have ability to utilize network bandwidth provided through multiple interfaces. ▪ The system shall have ability to load balance across servers ▪ The system should not have a single point of failure and inherent design bottlenecks that stops it from scaling.
2.	Security	Ability to secure all data from thefts, tampering, unwanted modifications, network attacks, and other security threats using physical and logical measures as per DRP specified security and data protection policies. The solution shall support: • storing primary data in encrypted fashion • profile based encryption schemes • secure communication protocols while communicating with external components • communication with only the SL-UDI application. • only authorized users to access appropriate data • changing the encryption schemes dynamically periodically • integration with external security components • configuring Access Control Lists • running services without super user privileges • Auditing all access and modifications (by any user) to biometric data and make these audit trails available. Audit trail should be stored.

S. No.	Dimension	Requirement
3.	Interoperability	Ability to interoperate with other systems/services within and across any open interfaces and ability to continually re-factor and/or replace specific components without affecting rest of the system. The solution shall support: • the open standard protocol-based communication • command line-based interface for interaction • re-factor/replace individual services without bringing the whole system down. • all APIs and interfaces defined by GoSL as part of biometric MSI integration specifications. • automated integration from external management products such as systems management, network management, and other tools
4.	Manageability	Ability to manage end-to-end solution and its components to ensure solution health and SLAs using external data center management tools. The solution shall support: • monitoring of its services using management tools • ability to bring its services up and down • monitoring its CPU/network/storage utilization • monitoring the response time of individual services • maintenance of its services without affecting client access • continuous availability of its services even during regular management activities
5.	Availability	Ability of the solution to be up and running over long periods of time and ensure continuous availability. The solution shall support: • high availability of its services across servers and data centers • integration with technologies that provide application high availability • integration with technologies that provide data replication to have data high availability • continuous availability of its services even during regular management activities

S. No.	Dimension	Requirement
6.	Upgradeability	Ability to seamlessly upgrade services, components, and modules without affecting services and open interfaces. Ability to upgrade without bringing down the solution. The solution shall support: • upgrade of individual modules without bringing the solution down • backward compatibility • upgrading using third party software delivery systems • reverting back to original configuration in case of an upgrade failure • reverting back to old configuration after a successful upgrade
7.	Installation and Configuration	Ability to configure the solution using wizard and other end user tools. Ability to install the solution using install script. The solution shall support: • connectivity with IDMS • integration with change management system • integration with software delivery systems • installation and configuration without super user privileges
8.	Maintainability	The solution shall have the: • Ability to continuously maintain, enhance, re-factor solution without breaking other parts.
9.	Open Standards based	Technology choices should be based on open standards and widely adopted frameworks as long as they meet the needs of the system. The solution shall have: • technologies that are based on open standards • frameworks that are widely adopted
10.	Administration	Ability to administer ABIS during its operation. The solution should support: • ability to administer the solution with minimal user intervention with well-defined user interfaces and access policies • easy to use operator interface • command line for all administrative operations • role based administration • automation of administrative tasks
11.	Logging and Reporting	Ability to log and report at a sub-system level state, health of the solution. It shall also log different events encountered by the subsystem. The solution shall have:

S. No.	Dimension	Requirement
		• The ability to log and create reports to know the current state of the solution and improve the quality of different services offered by the solution • a mechanism to configure the logging level for different modules • a mechanism to rotate the logs based on polices • a mechanism to search through the logs with different filters • a mechanism to integrate with alert management tools • a mechanism to generate reports on various performance indicators • a mechanism to integrate with external reporting tools
12.	Storage Access	Ability to use heterogeneous storage environments. The solution should: • work in heterogeneous storage environments with data partitioned across servers • function with storage getting provisioned using heterogeneous storage technologies like NAS/SAN/DAS • access only the data to which it was given access • support data partitioned across different servers
13.	Backup / Restore	Ability to provide backup and restore of the persistent data. The solution should have: • capability to backup and restore the data generated in the solution • ability to backup of the data generated in the solution while continuing to process service requests. • allowance for incremental/differential/full backup methods • ability to take backup of application consistent data • proper functioning after a restore operation

Table 5: Guiding Factors for Biometric Solution

The key functionalities of biometric solution are as follows:

- **System Configuration and Management –** Configuration console to be provided for defining business rules
- **User Management – Ability** to manage user lifecycle authorized to access the ABIS module
- **Reporting –** Status **reporting** to be done for the enrolment packets processed with sufficient details on the rejection criteria
- **Transaction management –** The complete transaction lifecycle of a packet (from requesting a biometric deduplication in the request queue to generating a response-to- response queue) is

broken down into various stages having relevant checkpoints assigned to each stage maintained both in memory and persistent database.

- **Transaction Validation and Security –** This module offers the feature of validating the transactions originating from IDMS and sent to ABIS for further processing. New identity is generated under this module for referencing the package under processing. This identity is mapped to the IDMS request through a mapping table.

- **Middleware Synchronization –** This functionality enables synchronization of management layers across ABIS, **IDMS** and Authentication to ensure seamless processing of incoming enrolment/ authentication requests

- **Biometric Middleware –** The IDMS communicates asynchronously with the ABIS servers using standard API to insert into their galleries and to perform 1:N deduplication. The communication happens with ABIS servers using inbound and outbound message queues. The requests are tracked using unique enrolment request numbers. This Message Oriented Middleware pattern conforms to **industry** standards and ensures persistence apart from delinking both requestor (IDMS) and responder (ABIS) processes thus avoiding unnecessary problems and ensuring high scalability, distribution of servers and performance.

- **ABIS performance tuning for FPIR and FNIR**- A performance tuning of Biometric data can be carried out every quarter to ensure quality of deduplication especially for judging the false accept rates. The **threshold** settings for FPIR and FNIR can be adjusted to ensure there is a good balance between false accepts and false rejects.

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

- **Template Generation, Segmentation and Sequence Check –** Template generation is the process of generated **biometric templates** (minutiae) from the raw biometric images captured through enrolment software.

- **Quality Check –** The SDK provided by ABIS performs basic quality check before the package processing is taken up by ABIS

- **Biometric Matching Engine –** ABIS provides a biometric matching engine to compare the generated minutiae with the ones existing in the ABIS gallery

- **Multi-Modal Biometric Fusion –** ABIS has a capability to use the multimodal biometric authentication systems, which combine information from multiple modalities to arrive at a decision

- **Biometric De-duplication (1:N) – Biometric** deduplication is run against the gallery of biometric templates to arrive at dedupe decision

- **Internal Template Storage –** All **the** successfully deduped biometric templates are stored in the ABIS for dedupe requests of new minutiae.
- **Software Development Kit – ABIS** also provides SDK for performing quality on the incoming packets.
- **Software Development Strategy** – COTS on Proprietary ABIS

The GoSL wishes to emphasis that the remote access to biometric solution (including ABIS) will not be provided outside nominated SL-UDI operational premises except in the case of trouble shooting of L3 Service Request.

2.5.5 Biometric Solution Components

The SL-UDI solution utilizes the biometric solution which are explained below:

2.5.5.1. Automated Biometric Identification System (ABIS)

ABIS is an essential component within overall SL-UDI solution. The system shall have the functionality to de-duplicate any new biometric with the existing biometric gallery in the solution. ABIS is envisaged to be multi-modal biometric matching which shall use biometric features (Fingerprint, Iris and Face) captured during the enrolment. For every new record the solution shall perform 1:N matches to ensure that there are no duplicates in the SL-UDI system. The enrolment cases that are found to be duplicate shall be considered for manual adjudication. ABIS solution will have the capability to interact with the other SL-UDI systems using Biometric Middleware.

The ABIS will maintain its own reference database of fingerprint, iris, and facial templates for de-duplication. The ABIS should also maintain a synchronized disaster recovery database at a separate physical location. All information necessary for ABIS to perform its functions should be maintained by ABIS in the reference database.

In addition to the reference database, a separate citizen data store is to be created and updated which is outside of ABIS. This identity repository will be used by Authentication Solution to deliver authentication services. The citizen data store will be created using the biometric SDKs.

The enrolment software has a feature of quality check for captured biometrics. However, the enrolment software permits the forced capture in case the quality remains poor despite multiple attempts. For such packet, there is a possibility of improving the quality of the captured biometric using the tool provided as part of biometric solution. Thus, this feature should be available within the biometric solution and integrated with IDMS.

2.5.5.2. Multimodal SDKs for Server and Client

Software Development Kit (SDK) is a set of libraries that provide functions and should be supplied and updated with patches and upgrades. SDKs will be used in the enrolment software, manual adjudication (for duplicates), authentication solution, and analytics module.

SDK should be able to work agnostic of the enrolment or authentication devices used and provide consistent and biometric standard compliant images to the IDMS during enrolment and to Authentication Solution during authentication. The SDK should have a service-oriented MSI

independent API. For management of biometric devices, the Virtual Device Manager of device OEMs will be utilized.

The biometric data captured shall be as per biometric standards defined in Section 2.5.3. During the enrolment, it is envisaged that the biometric solution shall enable capturing of fingerprints, iris and a photograph which shall be subsequently used for de-duplication and authentication.

SDK may contain signal detection, quality analysis, image selection, image fusion, segmentation, image pre-processing, feature extraction and comparison score generation **for fingerprint, iris, and face modalities.**

The supplied licenses should be perpetual, universal, irrevocable server and personal computer (desktop and laptop) for Multimodal SDK. GoSL shall have unrestricted, unfettered right to uses the licenses and the right to deploy the solution anytime anywhere.

SDK Client Side	SDK Server Side
• GoSL wishes to inform the BSP that the MOSIP (client-side components) is being developed in Java 11. Thus, the SDK to be supplied by the BSP should have an interface in Java 11.	• GoSL wishes to inform that the MOSIP (server-side components) is being developed in Java-EE 11. Thus, the SDK to be supplied by the BSP should have an interface in Java-EE 11.
• SDK should be compatible with latest Windows operating system, particularly, Windows 10 or latest (32-bit and 64-bit) and operating system provided in the enrolment client	• SDK should be compatible with Linux (RHEL 6 - 8, 64-bit) and Linux (Ubuntu 20, 24, 64-bit) including operating systems being proposed by the MSI for the servers on which these SDKs are proposed to be deployed
• SDK activation should be offline, permanent (no renewals required), and would be done in phased manner	• SDK will be utilized for fingerprint, iris, face.
• SDK will be utilized for fingerprint, iris, face, modalities only	• SDK should be licensed to address the volumes mentioned in the RFP and should be perpetual
• SDK licensing should be capped at specified quantity (1.25 x Number of Enrolment Kits planned under this project), machine independent and should be perpetual	• SDK should be benchmarked for response time given in the RFP
• SDK (and its licenses) should be bundled together in such a manner that the enrolment software package can be utilized in any enrolment kit (subject to overall limit of number of machines mentioned in previous point) of the DRP	• SDK should be fine-tuned for accuracy requirements given in RFP
• SDK should not be provided in form of any hard-token (dongle, etc.)	• SDK (and its licenses) should be able to meet the given volumes and service levels

SDK Client Side	SDK Server Side
• SDK should be pre-activated and pre-registered	• SDK should not be provided in form of any hard-token (dongle, etc.)
• In case of repair or replacement of enrolment kit, the representative of the BSP will be informed about the identity of enrolment kits (original as well as new one). The BSP should provide updated license, if necessary, for SDK free of charge.	• SDK should be pre-activated and pre-registered • In case MSI wishes to add more servers to meet the volumes, the representative of the BSP will be informed about the details of additional servers. The BSP should provide updated license, if necessary, for SDK free of charge.

Table 6:licenses

2.5.5.3. Biometric Middleware

Biometric middleware will act as a standardized data exchange platform between ABIS and Non-ABIS components of the SL-UDI solution. This will help in increasing standardization, reducing dependence on a single type of biometric hardware and software, allowing users to plug new devices into the infrastructure as required. The key features of the middleware are as follows:

- Routing of request and response
- Guaranteed delivery of request and response
- Fault tolerance and load balancing
- Support of web based ABIS API
- Support of biometric data exchange format standards
- Encapsulation and isolation of biometric solution components
- Standardized connectivity to other components of SL-UDI solution
- Open Standard based Messaging
- Should support multiple ABISs, if required

2.5.5.4. Resident Data Store (Authentication Repository)

In order to provide authentication and e-KYC service at a high-performance level, the biometric data shall be extracted and stored in the citizen data store outside the ABIS. The database licenses and infrastructure (server, storage, etc.) of the citizen data store will be provided by the MSI. The MSI will also be responsible for commissioning and administration, operation and maintenance of the citizen data store.

The BSP shall provide the SDKs to the MSI. The BSP will support MSI in the extraction of the templates and ensuring that citizen data store is always in synchronization with the biometric records in the reference database (ABIS gallery). The citizen data store should be able to support the gallery size and performance levels mentioned in the RFP. The role of BSP shall include among others the following:

- provide SDKs for extraction of biometric features from the raw packets
- provide SDKs which meet functional and performance requirements, and
- provide integration support to MSI

To serve the biometric authentication request, the authentication solution will utilize the citizen data store to extract the relevant biometric and will utilize the Server-Side SDK for matching the stored biometric with the biometric received as part of the request.

The DRP wishes to clarify the following will be stored in citizen data store:

- Fingerprints: ISO / Proprietary Template
- **Iris**: Proprietary template (for high performance)

- **Face**: Proprietary template (for high performance)

The BSP should note that the guiding principle of the solution is to ensure the independent of BSP and biometric device. As such, the BSP shall make all efforts to ensure that the authentication is not restricted to limited set of device(s)/OEMs. In case, there are any such limitations, the BSP has to clarify it during the proposal submission stage itself.

2.5.5.5. Manual Adjudication Solution

The enrolment cases that do not clear enrolment processing steps (such as demographic validation, biometric deduplication, etc.) shall be considered for manual adjudication. To facilitate the manual adjudication process, ABIS should have its own manual adjudication solution.

The Manual Adjudication Solution be able to fetch the details regarding subject and matching record(s) and show it to the adjudicating officer(s) for their decision. The record shall contain demographic information as well as biometric information (fingerprint, facial and iris) which may enable the adjudicating officer(s) to take the decision. For the biometric information, the system should provide the exact details both qualitative (points of similarity and points of dissimilarity) and statistical (match score, etc.).

Once the decision has been taken by the adjudicating officer, the case should be forwarded to the second level for confirmation. After the confirmation, the system should communicate the same to IDMS.

- The thick-client based software is needed for manual adjudication
- The manual adjudication software should have the features of comparing the fingerprint, face, iris, and demographic data. After implementation, the DRP may wish to disable the demographic portion, and this should be a configurable parameter
- The workflow should be of two levels (marker and checker)
- The queue management should permit to hold necessary volumes of records
- The BSP should make its own estimation on the volume
- The BSP should provide necessary training on decision making (biometric aspects)
- The BSP should provide necessary training on various features of manual adjudication software

The manpower and workstations for manual adjudication will be provided by the DRP. The minimum technical specifications for this manual adjudication workstation has been provided in Annexure-3.

2.5.5.6. Role of Biometric Solution in SL-UDI Information System

The biometric solution components will be used in the SL-UDI solution for enrolment as well as authentication. The role of these components in the SL-UDI solution is mainly in below mentioned areas:

S. No.	Area	Biometric Component Used
1.	Enrolment Data Capture	Multimodal SDK (Client Side)

S. No.	Area	Biometric Component Used
2.	Biometric Deduplication and update of Resident Data Store	ABIS
3.	Authentication Solution	Resident Data Store and Multimodal SDK (Server Side)
4.	Biometric sub-system monitoring and analysis	ABIS
5.	Manual Adjudication	Manual Adjudication Software and Multimodal SDK (Server Side)

Table 7: Usage of Biometric Solution in SL-UDI Information System

The details about the role of biometric solution components in above mentioned areas is provided below.

2.5.5.7. Enrolment Data Capture

For the enrolment, two different type of enrolment kits are planned to be procured. The first type of kits are desktop-based kits which are planned to be permanently stationed in CSCs. The second type of kits are laptop-based kits which are planned to be mobile to cover population in remote areas. For the biometric capture devices (photograph, fingerprint, iris) ~~from different OEMs~~ are planned to be utilized. The enrolment software will operate on both type of kit and will integrate with biometric capture devices ~~from different OEMs~~. At the time of enrolment, the enrolment software will capture the biometrics through these devices.

The SDK should be self-sufficient i.e., contain all the necessary APIs, libraries, documentation, etc. and usable across major operating systems (windows, Linux, etc.) and technology platforms usable across compatible to Mosip JAVA Version.

The enrolment software will utilize the multi-modal SDK for the following:

1. All the biometrics (photograph, fingerprint, iris) will be checked for quality. In case the quality is not acceptable or there is any actionable feedback, the operator will be alerted by the enrolment software based on input from SDK.

2. The captured photograph may need to be enhanced to meet the biometric standard. The image enhancement can be done for auto rotation, auto cropping, sharpness, exposure correction, etc.

3. The captured iris image may be cropped to ensure only relevant details are retained. The image alteration will not be performed on gray-level image.

4. The biometric image may have to be converted from one format to another or may have to be compressed/decompressed prior to storage. The conversion and compression should be in formats defined in Biometric Standards.

5. The enrolment software may be configured to extract and generate the templates at a local level. This function may be useful, among others, in below mentioned scenarios:
   i) reduce enrolment packet size
   ii) verification of enrolment officer during login
   iii) verification of enrolment officer at the end of each enrolment

iv) verification/authentication of enrolment agency administrator/ supervisor for login

6. The enrolment software will be required to match the biometrics locally, among others, for below mentioned scenarios:
   i) verification of enrolment officer during login
   ii) verification of enrolment officer at the end of each enrolment
   iii) verification/authentication of enrolment agency administrator/ supervisor for login

2.5.5.8. Biometric Deduplication and update of Resident Data Store

For ensuring no person gets two UINs, the biometric deduplication of enrolment should be performed. The SL-UDI solution is planning to use the multi-modal biometrics for biometric deduplication.

The IDMS will do the following before sending the packet to ABIS for biometric deduplication:

1. For each deduplication request, the IDMS will provide a unique reference number (other than UIN)
2. Perform deduplication using the demographic information

After the above steps, the IDMS will send the enrolment information to ABIS for the following:

i) As a result of deduplication, the ABIS shall provide the 'Duplicate' or 'Not-Duplicate' response along with unique reference number.

ii) For first case i.e., 'Duplicate', the ABIS will also provide a set of score for each duplicate. The set of score will have a fusion score (combined for all biometric features) as well as individual score (for each biometric feature). These scores should be comparative scores indicating the similarity between two biometrics. The scores should be scaled to the range of 0 (zero) to 100 (hundred) where 0 indicates least or no similarity and 100 indicates perfect or highest similarity.

The citizen data store should be updated with the unique reference number, demographics, and biometrics as soon as the result is sent back to IDMS. The details should be updated in citizen data store during enrolment process as well as biometric update process.

For deduplication the following guidelines will be applicable:

i) For the deduplication two Iris image labelled "L" or "R" will be sent to ABIS, and

ii) ICAO image(s) of face without non reversible grey level alterations

iii) Fingerprints labelled (e.g. Left- or Right-hand index finger)

The deduplication flow over multiple modalities can be chosen by the BSP. However, the DRP may review results for accuracy and may require that the BSP perform deduplication on relevant modalities fully.

2.5.5.9. Authentication Solution

For delivering the authentication services, the SL-UDI solution will have an authentication solution. This solution will be responsible to perform the 1:1 comparison and sending responses as per the capacity, and performance requirements mentioned in the RFP.

For the purpose of 1:1 comparison, the authentication solution will utilize the server-side multi-modal SDK provided by the BSP. The 1:1 comparison will be done of already enrolled record with

the record received as part of authentication request. For obtaining the enrolled record, the authentication solution will integrate with reference database.

The authentication request can contain one or more factors (demographic, one-time pin, and/or biometric). The authentication requests containing biometric will be served internally by the authentication solution. In this case, the SDK will be used to extract the biometric (fingerprint, iris, facial) template from the biometric image and then will be used to match the biometric (fingerprint, iris, facial) templates against the biometric (fingerprint, iris, facial) template stored in the citizen data store.

As the quality and performance of authentication is dependent upon the multi-modal SDK, the BSP will be required to ensure that the SDK meet the performance benchmarks as levels in this RFP.

For authentication the following guidelines will be applicable:

i) For the authentication services one Iris image labelled "L" or "R" will be sent to Authentication Server,
ii) One Fingerprint unlabeled or labelled (Left- or Right-hand index finger),
iii) ICAO image(s) of face without non reversible grey level alterations

2.5.5.10. Biometric System Monitoring & Analysis

The system monitoring and analysis modules of SL-UDI application require information from the biometric solution to:

i) monitor comparison score distributions
ii) monitor quality of the input data
iii) compare performance and analyse de-duplication risk across parallel ABIS systems.
iv) create metrics helpful in analysis of possible enrolment/verification fraud and system intrusion

BSP is expected to assist MSI to design and implement above functionality and do troubleshooting and resolution of issues.

2.5.5.11. Manual Adjudication

In cases where a manual intervention is required to take a decision on enrolment packet, the enrolment record will be sent for manual adjudication. Some of the cases where manual adjudication may be performed are as follows:

- ABIS determines that the case is duplicate
- ABIS is not able to clearly determine whether the record is duplicate or not

The manual adjudication software should be able to fetch the details regarding subject and matching record(s) and show it to the adjudicating officer(s) for their decision. The record may contain demographic information as well as biometric information (photograph, fingerprint, and iris) which may enable the adjudicating officer(s) to take the decision. For the biometric information, the system should provide the exact details both qualitative (points of similarity and points of dissimilarity) and statistical (match score, etc.). Once the decision has been taken by the adjudicating officer, the case should be forwarded to the second level for confirmation. After the confirmation, the system should communicate the same to IDMS.

2.6. Data Retention and Encryption

2.6.1 Data Retention

DRP has a policy of permanent archival of data including logs for this project. For at least one year, the MSI is required to manage the logs in online storage and thereafter the logs can be stored in online/offline storage. The MSI should consider this while designing the solution.

In view of the above, the solution shall not be permitted to delete any data or logs, even in case of biometric updates. In case of biometric updates, the existing record may be either deactivated or retained in the gallery as per the specific requirement of ABIS. The supplied licenses should also be sufficient to handle multiple biometric updates by the same individual without treating them as additional volume.

2.6.2 Data Encryption

Backup data shall be stored in encrypted format using the key(s) available to the DRP.

- **HSM Key(s)**: The BSP should provision its HSM and the BSP should ensure availability of key to the DRP from the time of installation of hardware
- **Storage OEM Key(s)**: The BSP should ensure availability of key to the DRP from the time of installation of hardware
- **Proprietary Key(s) of BSP**: The BSP should ensure availability of key to the DRP from the time of installation.

2.7. Authentication

From the biometrics perspective, the flow during the authentication stage is described separately for more clarity. SL-UDI system shall allow the citizen to use the UDI generated by SL-UDI for online real-time authentication at the point of service delivery of various agencies that subscribe to SL-UDI services. For ensuring privacy, the citizen would need to provide consent (among other options, the citizen can also provide consent through mobile) for using these services. The authentication service can be Demographic, Biometric and OTP based and would provide only a YES or NO response. In case of KYC service, the SL-UDI system would return the demographic details and the photograph of the citizens.

A large volume of service requests is expected, each request should be self-sufficient and stateless. The service requesting application may maintain its state to cater to errors and user experience. To protect against the replay of biometrics (stored biometrics), the analytics engine may be utilized.

For enrolment data, please refer to MOSIP website. The additional details are provided below:

- **Fingerprint Minutiae Record (FMR)**
  - Number of fingers: 1 or 2
  - Quality: NFIQ v1.0 (value of 1, 2 and 3 is acceptable)
  - Transmission format: minutiae
  - Storage: minutiae
- **Iris Image Record (IIR)**
  - Number of eyes: 1 or 2
  - Transmission format: JPEG2000 (lossy) or WSQ
  - Storage: JPEG2000 (lossy) or WSQ

- **Face Data**
  - Transmission format: JPEG2000 (lossy)
  - Storage: JPEG2000 (lossy)

3. Software Solution Requirements

The details of some of the solutions required in the SL-UDI system is provided below:

- MOSIP
- Business Intelligence and Analytics
- Customer Relationship Management
- Document Management System
- Identity and Access Management
- Mobile Application

The description of these solutions is provided below:

3.1. MOSIP

The IDMS sends the biometric data to ABIS for biometric de-duplication. The IDMS is being developed by MOSIP and the specification of biometric data during data acquisition and verification are provided below:

(i). MOSIP will use CBEFF ISO 19795-1 format to store and transfer biometrics data

(ii). MOSIP will use XML data format of CBEFF to store the biometrics data

(iii). MOSIP will use OASIS patron format ISO/IEC JTC 1 SC 37 – biometrics, Patron identified [257, patron format identifier 7 (Please refer https://www.ibia.org/cbeff/iso/bir-headeridentifiers for details)]

(iv). MOSIP will use OASIS Binary Data Block Format Identifiers for Format Type ISO/IEC JTC 1

(v). SC 37-biometrics, Patron identified -257, BDB patron format identifier such as 7-finger image, 8-face image, and 9-iris image (Please refer https://www.ibia.org/cbeff/iso/bdbformat-identifiers for details)

(vi). All the biometrics data captured for an individual is stored in a single XML file

(vii). The biometrics data itself inside the CBEFF file will be in the respective ISO format encoded as base 64 binary

(viii). Please refer to http://docs.oasis-open.org/bias/soap-profile/v1.0/errata02/os/cbeff.xsd for the XML schema of CBEFF XML format (sample XML is given in Annexure-III)

(ix). For enrolment data, please refer to MOSIP website (). The additional details are provided below:

a) Enrolment Data (Fingerprints)
   - Number of Fingers - maximum 10; minimum 1
   - Quality – NFIQ v2.0 value of 1, 2 and 3 is acceptable
   - Transmission format - JPEG2000 (lossless)
   - Storage - JPEG2000 (lossless)

b) Enrolment Data (Iris Image)

- Number of Eyes: maximum 2, minimum 1
- Transmission format: JPEG2000 (lossless)
- Storage: JPEG2000 (lossless)

c) Enrolment Data (Face Image)

- Image specification: ICAO 9303
- Transmission format: JPEG2000 (lossless)
- Storage: JPEG2000 (lossless)

3.2. Business Intelligence and Analytics

DRP is seeking the capability to analyse large quantities of SL-UDI data, transform the data into intelligence and insight, and deliver this intelligence and insight to the DRP's processes and users. In a move aimed towards digital economy in Sri Lanka, the DRP has taken up a Data Analytics and Business Intelligence initiative for SL-UDI Information System. SL-UDI Information System would help increase efficiency and improve savings in resources and availability of reliable data in a timely manner. DRP desires to build an enterprise-level DA and BI system with definition of Key Performance Indicators (KPI) for SL-UDI Information System. The KPIs need to be viewed from a Division, Function, Process, and user's perspective. The DRP believes that data mining and statistical analysis is a key requirement for Planning and Scorecard/Dashboard for SL-UDI Information System.

(i) The proposed product should preferably be an open-source solution along with Enterprise support.

(ii) The solution must have dashboards, analytics, and dynamic reporting. Reports should allow for exportable formats such as pdf, excel etc.

(iii) The solution should allow customizable and ad-hoc reports, the generation of the report shall not impair the System performance.

(iv) GoSL shall prescribe reports to be developed which will be identified at requirements stage as well as operations phase.

(v) The Data Analytics system should allow GoSL to customize notification of certain indicator that GoSL is interested to trigger activities/actions. The Data Analytics module should have a user interface to extract data based on the data required for self-analytics and report generation. The Data Analytics module should also allow for ad-hoc queries pertaining to the module for quick access to real time information and allow users to put in parameter to view the data from different perspectives.

(vi) The scheduled (weekly, fortnightly, monthly, quarterly, yearly) reports need to be extracted based on the agreed format and submitted to GoSL for KPI tracking purposes.

(vii) A key feature envisaged as the part of Data Analytics and Business Intelligence Solution for SL-UDI Information System is fraud analysis.

The key functionalities of the application are provided below:

(i) **Integration with other Components:** Execution of various business processes in the UDI

system would generate a lot of data which would be transformed into useful insights by BI.

(ii) **Enrolment Status Reports:** BI **solution would** provide enrolment status reports on a periodic basis for review to internal users.

(iii) **Enrolment Performance Reports:** The BI Solution would provide performance of different enrolment **centers**, enrolment officers and **overall** enrolment process to continuously evaluate if there are no bottlenecks from a system, process and people perspective and take mitigation steps when needed.

(iv) **Authentication Status Reports:** BI **Solution** would provide authentication status reporting on periodic basis for analysis and review by internal users.

(v) **Authentication Performance Reports:** BI Solution would provide authentication performance for different types of **authentications** carried out **to** point out any performance issues in any of the authentications.

(vi) **Data Quality Management:** Data before **being** fed into the BI tool would be evaluated for cleanliness and any **aberrations** would be filtered out by a Data Quality tool.

(vii) **Metadata Repository:** The BI Tool would **have** a metadata repository to contain business metadata.

(viii) **ETL/Data Acquisition System:** This would include tools that would extract data from all the source systems **into** the BI Tool. This **ensures** data in BI is integrated with other parts of the system to ensure data is consistent with the rest of the system.

(ix) **Visualization System:** This is responsible for **presentation** of data to end users in form of rich graphical **reports**, dashboards, KPIs, GIS based reports, etc.

(x) **Integration with Web Portal/Mobile App: The** portal and mobile application would show dashboard and many reports. For this purpose, the **Business** Intelligence and Analytics tool would require integration with UDI Portal / Mobile Application.

(xi) **Public Dashboards: Some** of the aggregated statistics like Enrolment, KYC, Authentication trends would be available for public view on the Web Portal.

(xii) **Other Analytics: The** Business Intelligence **and** Analytics tool would analyze the information generated as a **result** of enrolment, authentication and operations.

The proposed solution should meet the minimum technical specifications given in the RFP. Proposed BI and Data Analytics system must allow for the Design and distribution of dynamic, interactive reports and dashboards using a drag-and-drop designer environment which includes but not limited to:

a. Auto-charting automatically chooses the best graph suited to display the selected data.

b. Variety of analytical visualization such as line, bar and pie graphs, box plots, animated bubble plots, correlation matrices, forecast reports, etc.

c. Embeds Artificial Intelligence/Machine Learning into the platform and allow for automated analysis of available variables.

d. Use predictive analytics to analyses the data and predict the possible outcomes, forecasts etc.

e. Includes geospatial analysis, network diagrams, ability to create calculated, aggregated or derived data items

f. Able to allow for the reuse and sharing of reports, including filters, calculations, hierarchies and report element formatting

g. Must be scalable and include the handling of ever-growing numbers of users, data types, data volumes, and the evolving range of BI and analytical work loads

h. Ability to create alerts for a report object so that subscribers are notified via email or a text message when the threshold condition is met

i. Ability to provide self-service analytics that includes the creation of drillable hierarchies in a self-service manner without the need to predefine user paths and network diagrams to determine data links

j. Availability of a unified platform that allows users to customize its whole analytical journey. Ability to perform powerful analytic insights without writing any code or choosing to use the graphical user interface or choosing to integrate other technologies into the platform, like open-source coding and APIs

k. Availability of a collaborative platform that allows different users to perform different tasks in one platform such as managing and preparing data, visualize and create dashboards, build models, performing AI and other tasks in one application under one unified and collaborative platform without leaving the browser.

l. The tool should provide role-based access to various users of the system

m. All access to be system shall be via a secure web-based portal

   a. The middleware, data stores used by the tool should be a standard COTS/Open-Source product – should not use any proprietary components

   b. The tools should be deployed as virtual machines or containers on the proposed hardware platform (x86 based).

3.3. Customer Relationship Management

GoSL intends to create and maintain a common CRM platform to act as a citizen and partner helpdesk and provide redressal of queries of Residents and Ecosystem Partners regarding SL- UDI services, Enrolment services, Authentication services, TSP and UA related queries, etc.

The MSI's scope of work includes:

1) Procuring, commissioning, configuration, implementation, integration, deployment, and maintenance of an enterprise level Customer Relationship Management (CRM) Solution/Product.

2) The MSI shall carry out a detailed requirement phase upon award of the contract to review the CRM requirements.

3) The CRM solution should be used to log all incidents and queries in the system for generating id and track the logged query.

4) The CRM solution should be a single window to record and address queries of citizens and

partners. MSI shall be responsible for undertaking any customizations of the CRM solution as per GoSL's requirements, SRS, and associated Software Lifecycle Services.

5) MSI shall be responsible for operations, maintenance, and support of CRM solution as part of the Application Maintenance and Annual Technical Support from OEM including associated updates and upgrades.

6) The MSI shall be responsible for integrating the CRM with the entire SL-UDI Information System.

7) MSI shall analyse the requirements of IT infrastructure for hosting the CRM software to meet the availability, performance and response times required to meet the Contact Centre service levels.

8) MSI shall generate and provide CRM Reports on daily, weekly, monthly, quarterly, and yearly basis.

9) MSI shall also be responsible for analysis of the CRM reports to continuously identify improvements in the CRM operations.

10) GoSL shall provide the MSI with a toll-free number(s) for contact center. MSI shall be responsible for integrating and manage the toll-free number.

11) The proposed product should be an enterprise level solution along with Enterprise support.

12) The license of the proposed/ deployed Solution should be an enterprise level on a perpetual basis in name of GoSL including ATS post for entire project duration.

13) The CRM solution should support at least Sinhala, Tamil, and English Languages.

14) A single view of the customer experience and history (customer data integration). The system shall be designed to give a single view of all interactions with a citizen for the past 3 months.

15) CRM shall be capable of taking caller satisfaction feedback on SMS. CRM shall be capable of generating SMS in respect of a sample of callers (such as 5th caller who spoke to agent) to get feedback about quality of response and satisfaction level. The criteria for defining select callers will be as decided by GoSL from time to time.

16) The CRM solution shall support relevant screen pop-ups, to the contact center agent along with the details of the previous calls during the last 30 days, on the agent' desktop on the basis of DNIS (Dialed Number Identification Sequence) etc.

17) The CRM solution shall maintain history regarding complaints/grievances.

18) The CRM solution shall support IVR, Voice, Email, ~~FAX, let~~ter and Web based complaint lodging, resolution, and response features using channels such as Voice, SMS, Email, ~~FAX~~, and Web.

19) The CRM solution should provide special functionality of handling handwritten letters as a

part of grievance redressal. The letters shall be scanned and maintained in the CRM solution.

20) The CRM system should provide extensive analytics and reporting capability on important KPIs concerning all types of users.

21) The solution should support call routing functionalities.

22) Real-time decision-making support (analytics) to understand customer intentions and customize services and interactions accordingly.

23) The CRM system shall be integrated with the Knowledge Management System and Document Management System of SL-UDI Information System through suitable APIs.

24) The proposed solution should meet the minimum technical specifications given in the RFP. The MSI will be required to gather detailed features, functionalities and requirements during the requirement gathering stage.

25) CRM should be integrated with Citizen Portal and mobile application to display and track incident reported by individual citizens.

26) The CRM should centralize all incidents and complaints from both members of the public and SL-UDI partners and track them using dedicated unique identifiers.

27) The CRM should include a web application including a set of GUIs and tools for SL-UDI operators to efficiently process incoming requests.

28) The MSI should integrate the CRM with all relevant SL-UDI Information System such as the IDMS, the IAM (operators' login) and the notification services (for sending updates to claimants via SMS).

29) The CRM should support complaints by members of the public as well as PSA partners through the following communication channels:
    a. SL-UDI help desks
    b. SL-UDI Fixed Registration Centers
    c. SL-UDI Mobile Application
    d. SMS gateway
    e. Official SL-UDI website(s) and email address(s)
    f. Letters sent via postal services (including handwritten ones)

30) The CRM Should timestamp all transactions and automatically prioritize them based on the distance with the relevant KPIs of the SLA.

31) The CRM should keep a history of all transactions not limited to metadata, but including identifiers, timestamps and content of all exchanges.

32) MSI MUST include all data processed and generated by the CRM into the SL-UDI backup scope and policies.

33) The CRM should produce and disseminate activity reports on a daily, weekly, monthly, quarterly and yearly basis.

The key functionalities of the application are provided below:

(i) **Single point of customer experience:** The system would be designed in such a way to give a single view of all the interactions with the resident for at least the given time period.

(ii) **Customer Feedback:** The CRM Solution would be capable of taking caller feedback on SMS, IVRS, UDI-Portal, and Mobile App going forward or through a KIOSK in the CSC. CRM shall be capable of generating SMS in respect of a sample of callers (such as 5th caller who spoke to agent) to get a feedback about quality of response and satisfaction level or for landline users caller satisfaction feedback can be taken over IVRS.

(iii) **Web Interface:** The CRM solution should be able to allow the field officials to directly log a call using CRM web interface

(iv) **Integration with UDI:** CRM would be integrated with other systems using an API based approach where API's of other systems like BI would be available for consumption or API's exposed by CRM would be available for consumption by BI and Analytics software to derive insights and trends of the resident behavior.

(v) **Multilingual Support:** CRM would be capable of multilingual support in French and Arabic language.

(vi) **Customer Analysis:** CRM would help in analysis of service to the resident by aggregating of statistics related to each resident experience while enrolment.

(vii) **Software Development Strategy –** Open Source Platform/COTS

3.4. Document Management System (DMS)

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

(i) Documents would be indexed using various unique numbers (internal and external)

(ii) The proposed solution should meet the minimum technical specifications given in the RFP. The MSI will be required to gather detailed features, functionalities and requirements during the requirement gathering stage.

(iii) The MSI MUST develop or customize, test, install and maintain the DMS.

(iv) For this particular system, the SI can either purchase and customize a COTS software product

(v) The DMS MUST support all functions listed in Sections Registration Procedure and updating Process. Notably, the DMS MUST allow for the storage of all scanned documents submitted by applicants during pre-Registration, Registration and personal data update.

(vi) Document management system should be interoperable and follow open standards to facilitate smooth takeover by any other vendor appointed by PSA.

(vii) The DMS should be integrated with pre-registration applications, registration, IDMS, KMS and LMS.

(viii) In addition, the SI shall allow at least ten (10) internal users to connect directly to the DMS application.

3.5. Identity and Access Management

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

(i) **Single Sign on access:** To avoid multiple access credentials Identity and Access management would be used which will be used across the different applications of SL-UDI Software System. A Single Sign-on (SSO) would be required to access multiple application in the SL-UDI landscape.

(ii) **Role Based Access:** Access to different applications from the SL-UDI Portal would be based on Role based access where after login to portal using SSO, the ability to invoke a particular application would depend on if the role is authorized to access the application.

(iii) **Provisioning of internal and partner users:** Access and identity management would help provision users depending on their roles into different applications such as Enrolment Software Administrators, Enrolment officers, CRM Users, Partner Admins, Partner users, BI Admins, Database admins etc. Administrator can be allowed access on the basis of multi-factor authentication devices.

The proposed solution should meet the minimum technical specifications given in the RFP. The MSI will be required to gather detailed features, functionalities and requirements during the requirement gathering stage.

3.6. Automated Biometric Identification System

The key functionalities of the application are provided below:

1. **System Configuration and Management –** Configuration console would be available for defining business rules

2. **User Management –** Ability **to** manage user lifecycle authorized to access the ABIS module

3. **Reporting –** Status reporting would be done for the enrolment packets processed with sufficient details on the rejection criteria

4. **Transaction management –** Complete transaction lifecycle of a packet would be broken down into various stages having relevant checkpoints assigned to each stage maintained both in memory and persistent DB. The journey starts from requesting a biometric duplication in the request queue and ends at submission of a reply to response queue

5. **Transaction Validation and Security –** This module would offer the feature of validating the transactions originating from Identity Management and sent to ABIS for further processing. New Identity is generated under this module for referencing the package under processing. This Identity is mapped to the IDMS request through a mapping table.

6. **Template Generation, Segmentation and Sequence Check –** Template generation is the

process of generated biometric templates from the raw biometric images captured through enrolment software.

7. **Quality Check –** The SDK provided by ABIS would perform basic quality check before the package processing is taken up by ABIS.

8. **Biometric Matching Engine –** ABIS would provide a biometric matching engine to compare the generated biometric templates with the ones existing in the ABIS gallery.

9. **Multi-Modal Biometric Fusion –** ABIS would have a capability to use the multimodal biometric authentication systems, which combine information from multiple modalities to arrive at a decision.

10. **Biometric De-duplication (1:N) –** Biometric de-duplication would run against the gallery of biometric templates to arrive at de-duplication decision.

11. **Internal Template Storage –** All the successfully de-duplicated biometric templates would be stored in the ABIS for dedupe requests of new packets.

12. **Software Development Kit –** Biometric solution should also have SDKs for performing quality on the incoming packets. SDK may contain signal detection, quality analysis, image selection, image fusion, segmentation, image pre-processing, feature extraction and comparison score generation for fingerprint, iris and face modalities.

13. **Middleware Synchronization –** This functionality enables synchronization of management layers across ABIS, IDMS and Authentication to ensure seamless processing of incoming enrolment/ authentication requests.

14. **ABIS Middleware –** ABIS has a response / request queue mechanism to receive messages from IDMS and allow adjudications application to subscribe for potential duplicate messages for manual adjudication.

15. **Biometric Template derived from Multimodal Fusion:** The biometric template that would be used for 1: N match for a deduplication would be not based on a biometric template of a single biometric but would be a full multimodal biometric template. A multimodal biometric would be a fusion of all the biometrics, which means a single template derived after concatenation of all the individual biometric images or templates.

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

17. **Fine tuning of ABIS for False Positive and False Negative Rates:** ABIS would have provision to analyse and report the false positive and false negative rates along with a provision to carry out detailed analysis for reasons thereof. ABIS would also have features to fine-tune thresholds and other settings for improving False Positive and False Negative Rates while ensuring there is a good balance between them. In addition to the tuning of thresholds, ABIS should have the provision to utilize / add appropriate biometric algorithms.

a) **"False Positive Identification Rate (FPIR)" -** A term applying to de-duplication transactions only. The ratio of number of false positive identification decisions to the total number of enrolment transactions by unenrolled individuals

b) **"False Negative Identification Rate (FNIR)" -** A term applying to de-duplication transactions only. The ratio of number of false negative identification decisions to the total number of enrolment transactions by enrolled individuals.

3.7. Web Portal

The SL-UDI Web Portal refers to various independent portals i.e., Enrolment Partner Portal, Authentication Partner Portal, Public Portal, Private Portal, Citizen Services Portal and Developer Portal (incl. documents, starter packs, SDKs). The key functionalities of the application, among others, are provided below:

a) Partner Services: UDI portal would contain catalogue for the various available partner services, including details of processes to enroll/onboard TSPs, required documentation, fees, if applicable, etc.

b) Citizen Services (Pre-enrolment, UDI status, UDI Card / Letter Download, etc.): Citizen portal/Mobile App would enable residents the to check status of their UDI under processing, to download a UDI number digital card (if required in future) for printing, to submit grievance and check its status, update of certain demographic information such as mobile number.

c) Public Portal: The public portal shall contain a lot of information for public or general consumption, among others, it will contain the following:

a) **Public and Internal Dashboards:** The resident portal would show dashboard from the perspectives of enrolment and identity services. These dashboards will have drill down facility to provide more details to the user, whenever necessary. The internal dashboard will be more comprehensive and may also contain the performance measures against predefined KPIs published on a periodic basis in the Business Intelligence and Analytics application. The private dashboards will be accessible by login using SSO feature.

a. Legal and Governance Framework: The web portal would have details on the legal and governance framework.

b. Resources and Public Relations: The web portal would have complete information on the resources and public relations.

c. Grievance Management: The internal UDI portal would allow the CRM user to login to the CRM application using SSO and perform all call center and grievance redressal activities. Residents would be given an interface where they would be able to file grievances online.

d. Events, Notices and Circulars: Web portals would contain relevant public notices, events, and circulars for viewing.

e. Other Application Interfaces: The internal web portal would allow the application users to login into respective user applications as per their roles and credentials. For example, adjudication users would login to the adjudication application using SSO and perform all quality check activities.

d) Mobile Application

The high-level functional requirement for mobile application are provided below:

S. No.	Functions	Requirements
1.	**Access to SL-UDI Mobile Portal**	SL-UDI Mobile application will be access through common government application. That mean SL UDI application will be embedded into the government Application. And also, it should be possible behave independently if required (downloading application directly from the apps stores)
2.	**Loading Page**	Once the user accesses the specific mobile app the application page will be loaded with the government emblem and this need to be customizable.
3.	**Binding Device with the Mobile Application**	• Binding Process: In order to bind the device with the mobile application, the user will have to scan at least one biometric scan of the physical UDI card and capture the mobile number along with the Email address to receive the OTP.
		• Application reinstall (new device): In case of changing the device, the user is obligated to reinstall the app which requires the re-binding process. This, however, exempts the app-update process. In case of re-installing the app in the existing device, the rebinding process can be exempted.
		• Application reinstall (existing): the app-update process. In case of re-installing the app in the existing device, the rebinding process can be exempted.
		• Change mobile number: The user has the capability to change their existing mobile number through biometric and by scanning Physical ID.
		• User Validation against UDI Database: The user should be validated through the UDI database.
		• Capturing all possible device biometrics: During the binding process, enable attachment of all available device biometrics to the access profile. This will be device-dependent. The objective of this is to allow a post-binding user to login into the app with device biometrics. Since the mobile number is collected during the enrolment process, the device and the mobile number will be interlinked.
		• Device and Mobile number Bonding: The user device and the mobile number will be bonded against the user and the UDI.
		• Anonymous User access: In the presence of an anonymous user, the binding process can be skipped which will restrict

S. No.	Functions	Requirements
		several services for the user.
		• 2FA enabled authentication: 2FA will be executed through the OTP.
		• Language Selection: The user should be able to define the app language to a preferred language. At the initial device binding.
4.	**Access to Application (Sign in and Sign Out)**	• Biometrics data that was collected in the binding process will be used to log in to the app.
		• A registered user will be able to use device biometrics to log in to the application.
		• The user can provide the UDI with the pin and the OTP to access the application.
		• The user can use the facial biometric and the OTP to login.
		• Iris biometric can be provided with the OTP to access the app.
		• The fingerprint of the user and the generated OTP to the Email or mobile number can be used to log in.
		• If the user fails to enter the correct details at a defined number of attempts the app will be locked and unlock procedure by forget credential options
		• An option will be provided to configure other biometrics which was not provided during the binding process.
		• If the user is inactive for a defined time period, the user will be automatically signed out from the app.
5.	**Simple and User-Friendly Landing Page**	• Once the user signs in to the app, the app will display the ID photo of the user along with the user details. (name, ID Photo, received authentication requests)
		• The authentication requests the user received will be displayed along with the navigation options.
6.	**Basic Application Component**	• At the bottom of the application, a quick access bar will be available. However, the available tools will vary based on if the user is registered or a non-registered user.
		• At the top of the application, the photo of the user should be displayed that will navigate the user to the user's profile.
		• Notifications should be displayed the number of notifications the user received which will navigate the user to the message inbox

S. No.	Functions	Requirements
		• On the top middle of the screen, the citizen's name and the ID number should be displayed.
7.	**My Profile View**	• User View - Users are able to define their own views by selecting necessary data elements. Also, the user has the option to select which user view to be displayed.
		• My View - My view option will allow the user to switch between different views.
		• Profile Services - Users can access Profile services through his/her profile
8.	**My Profile-Edit My Profile**	• In order to edit the user profile, under the user profile services the user will be able to access the profile edit services to make the desired changes.
		• The user has the ability to edit the defined fields. Some of the fields can be directly updated. However, some of the editing needs might need prior approval from the necessary authorities.
9.	**My Profile (Virtual ID generation) Mean generating user defined virtual IDs that mask the general ID details.**	• Profile View - The user will be able to define their own data set and by selecting the data fields that appear on the screen and create own virtual ID
		• Virtual ID (download/ share options) - Different options such as downloading and sharing are available for the Virtual ID
		• Virtual ID request - User should be able to request Virtual ID which will mask the original UDI and this need to be define the validity period
		• Define validity period for the Virtual ID.
10.	**My Profile - Display e- UDI**	• If the user currently doesn't have a mobile ID, the user will have the ability to request one.
		• Should have the capability to display both sides of the mobile ID.
		• The new information updates by the user should be reflected in the Mobile ID. in order to facilitate this the Mobile ID and the UDI data should always be in sync.
11.	**My Profile - QR code generation**	• The user is able to select the relevant data and generate the QR code.
		• The generated QR code can be either downloaded or shared.

S. No.	Functions	Requirements
		• Predefined QR Code option also need to be in place
		• Consent popup to the citizen when the client read the QR code for request information. utilize a predefined QR code that can be scanned by the client. To get the consent of the user in sharing data, a popup will be appearing.
		• This predefined QR code can be utilized as login credentials to acquire other necessary government services.
12.	**My Profile - Track My Request**	• The option will allow the users to track their requests which were made through the application.
		• An option to create a new request which directs the user to the e-services section.
13.	**My Profile - Settings**	• The users will be able to update their preferred languages. (Sinhala, English)
		• Settings will provide the option to enable and disable authentication modes.
14.	**My Profile - Digi Locker**	• Pointers to necessary approved documents so that application does not required to store locally this information.
		• Users have the facility to upload new documents which will be reviewed later and added to the Digi locker.
15.	**My Profile - My History**	• Users will have the ability to access all the historical transactions made through the application.
16.	**E-Services Section**	• Two separate sections will be available for Government Services and Private Sector Services
		• Integrated Private or Government Services will be listed under each tile
		• The users are able to search necessary government departments and add them as a tile
		• Based on the security sensitivity of the services, user Authentication with UDI is required. (example: if the user request service for police report, re authentication is popup)
17.	**My Requests**	• This option will display all the services which require the user to act upon.
		• User authentication with the UDI is required based on the security sensitivity of the services. o Simple authentication request

S. No.	Functions	Requirements
		○ Request digitally stored documents (Digi locker)
		• In a scenario where the user wants to submit information along with documents in the Digi locker, the users will have to enter their UDI in the necessary website. After the UDI is entered a popup will be displayed to take the consent to share this information.
		• Open requests tab: The tab will display all the open requests. Which user wants to take actions on
		• Rejected requests tab: Tab to display rejected requests.
		• Approved requests: This will display all the approved requests.
18.	**Support Center**	• Chatbot tab: The chatbot option is available for the user to communicate with the system virtually.
		• FAQ tab: In order to find solutions for the frequently raised questions, the user can refer to this.
		• Email Option: The user is able to send mails through this option when needed.

Table 8: Mobile Application

e) Knowledge Management System (KMS)

The main capabilities that would be delivered by the KMS are as follows:

a) Search Capabilities: This allows users to ask questions and search for knowledge in the underlying repositories – DMS, Portals, Emails, or other document repositories.

b) Collaboration Capabilities: This allows collaboration among the users through use of collaboration tools such as Blogs, Wikis, Discussion forums, chats etc.

c) Share: This allows for automatic notifications to users to keep them aware of any news and changes especially in areas the person is interested in knowing.

d) Knowledge Storage: It includes preserving existing and acquired knowledge in the knowledge repositories.

e) Workflows: KMS would entail workflows for creation, approval and sharing of knowledge contents.

f) Navigation System: A KMS system would provide navigation features to browse through the knowledge base using folder-based system with a well- defined hierarchy.

g) Reporting: A reporting system for reports to indicate trends related to the access pattern of knowledge assets would be available for review by knowledge management officers.

f) Learning Management System (LMS)

The main capabilities that would be delivered by LMS should include the following:

(i) **Curriculum Management:** With LMS, the administrator would be able to upload new trainings, which could be video trainings, document manuals. LMS would also allow new versions of existing trainings, retiring obsolete trainings, setting up passing criteria for trainings, setting up business rules for automatic creation of training plans whenever a new user is provisioned in some application. LMS would allow administrators to schedule trainings in the case of instructor lead trainings.

(ii) **Assessment & Test Management:** LMS would have an assessment engine, which would allow users who **have** completed a training to take tests/assessments/quiz etc. In certain cases, the course would require a mandatory pass before a user can take up a particular role.

(iii) **Learning Plan Management:** LMS would enable creation of Learning Plans for employees and partners such as enrolment officers, TSPs etc. These plans would consist of a set of trainings that the users would need to undergo as part of a mandatory or a suggested annual learning plan for their career progression & development etc.

(iv) **Certification Management:** LMS would allow maintaining certificates of users who have successfully completed their learnings.

(v) **Learning Registration and Plans:** LMS would allow users to register for trainings that are planned for them by LMS either automatically or by LMS admin or by self-request.

(vi) **Workflows:** LMS would allow workflows with human approvals, to allow trainings request to be evaluated by the LMS admin and approve/reject request.

(vii) **Social Integration:** LMS would integrate with different social engines to include learnings, articles of interests etc.

(viii) **Surveys and Reporting:** LMS would allow the users to take surveys so that courses and trainings can be continuously improved. LMS would also have the capability for reporting

(ix) **Classroom Management:** LMS would allow the admins to allocate classroom facilities to Instructor led trainings.

(x) **Instructor Management:** LMS would allow admins to allocate instructors to trainings.

(xi) **Learning catalogue Management:** LMS would allow admins to create Learning catalogue where users can self-register.

(xii) **Platform Compatibility:** All capabilities would be available on a web application accessible on desktops/laptops.

g) Mobile Application

The mobile application should be a comprehensive application for citizens to perform various activities, including but not limited to Enrolment Centers information, Pre-enrolment, UDI Status, Download UDI softcopy, Get UDI on mobile, Retrieve Lost ERN/UDI, UDI information update, Verify UDI, Verify Mobile/Email Address, Lock / Unlock Biometrics, UDI Authentication

History, Grievance Logging and Status, Generate Virtual Identity (VID), Retrieve VID, Replace VID, etc.

Some of the key requirements related to Mobile application, but not limited to, are mentioned below:

(i) The Mobile Application should provide an intuitive and user-friendly GUI that enables users to navigate and apply actions with ease. The GUI should be responsive with very little or no delays or time lag at launch or whilst navigating through screens.

(ii) It should enable ease of configuration and changes to existing GUIs and support the introduction of new screens.

(iii) It should provide on screen tips and online help to aid users while interacting with it.

(iv) Should make use of data available in the existing database and reduce duplicate data entry.

(v) Apps should be easily customizable and easy to Administer data in the database.

(vi) Network level security and traffic should be encrypted using secured connectivity.

(vii) Should structure overall content with proper tagging to make them screen reader friendly.

(viii) Application should ensure compatibility with all major platforms such as Android and iOS etc.

(ix) Solution should develop resolution independent design structure i.e., Mobile Application should adjust itself automatically as per the screen resolution, form factor and size of the mobile.

(x) Mobile Apps should work flawlessly across different platforms.

(xi) There should be minimum use flash contents so that home page should be loaded quickly.

(xii) Should provide Role Based Access control.

(xiii) Should come with mobile threat prevention and recovery system.

(xiv) Should support in-device authentication

The below mentioned requirements for the mobile application is for initial understanding of the bidder. The successful bidder is required to do a detailed requirement gathering in consultation with stakeholders and design the system accordingly.

1. Access to SL-UDI Mobile Portal

SL-UDI Mobile application will be access through common government application. That mean SL UDI application will be embedded into the government Application. And also, it should be possible behave independently if required (downloading application directly from the apps stores)

2. Loading Page

Once the user accesses the specific mobile app the application page will be loaded with the government emblem and this need to be customizable.

3. Binding Device with the Mobile Application

3.1. **Binding Process:** In order to bind the device with the mobile application, the user will have to scan at least one biometric scan of the physical UDI card and capture the mobile number along

with the Email address to receive the OTP.

3.2. **Application reinstall (new device):** In case of changing the device, the user is obligated to reinstall the app which requires the re- binding process. This, however, exempts the app-update process. In case of re-installing the app in the existing device, the rebinding process can be exempted.

3.3. **Application reinstall (existing):** the app-update process. In case of re-installing the app in the existing device, the rebinding process can be exempted.

3.4. **Change mobile number:** The user has the capability to change their existing mobile number through biometric and by scanning Physical ID.

3.5. **User Validation against UDI Database:** The user should be validated through the UDI database.

3.6. **Capturing all possible device biometrics:** During the binding process, enable attachment of all available device biometrics to the access profile. This will be device-dependent. The objective of this is to allow a post-binding user to login into the app with device biometrics. Since the mobile number is collected during the enrolment process, the device and the mobile number will be interlinked.

3.7. **Device and Mobile number Bonding:** The user device and the mobile number will be bonded against the user and the UDI.

3.8. **Anonymous User access:** In the presence of an anonymous user, the binding process can be skipped which will restrict several services for the user.

3.9. **2FA enabled authentication:** 2FA will be executed through the OTP.

3.10. **Language Selection:** The user should be able to define the app language to a preferred language. At the initial device binding.

4. Access to Application (Sign in and Sign Out)

4.1. Biometrics data that was collected in the binding process will be used to log in to the app.

4.2. A registered user will be able to use device biometrics to log in to the application.

4.3. The user can provide the UDI with the pin and the OTP to access the application.

4.4. The user can use the facial biometric and the OTP to login.

4.5. Iris biometric can be provided with the OTP to access the app.

4.6. The fingerprint of the user and the generated OTP to the Email or mobile number can be used to log in.

4.7. If the user fails to enter the correct details at a defined number of attempts the app will be locked and unlock procedure by forget credential options

4.8. An option will be provided to configure other biometrics which was not provided during the binding process.

4.9. If the user is inactive for a defined time period, the user will be automatically signed out from the app.

5. Simple and User-Friendly Landing Page

5.1. Once the user signs in to the app, the app will display the ID photo of the user along with the user details. (name, ID Photo, received authentication requests)

5.2. The authentication requests the user received will be displayed along with the navigation options.

6. Basic application Component

6.1. At the bottom of the application, a quick access bar will be available. However, the available tools will vary based on if the user is registered or a non-registered user.

6.2. At the top of the application, the photo of the user should be displayed that will navigate the user to the user's profile.

6.3. Notifications should be displayed the number of notifications the user received which will navigate the user to the message inbox

6.4. On the top middle of the screen, the citizen's name and the ID number should be displayed.

7. My Profile View

7.1. User View - Users are able to define their own views by selecting necessary data elements. Also, the user has the option to select which user view to be displayed.

7.2. My View - My view option will allow the user to switch between different views.

7.3. Profile Services - Users can access Profile services through his/her profile

8. My Profile - Edit My Profile

8.1. In order to edit the user profile, under the user profile services the user will be able to access the profile edit services to make the desired changes.

8.2. The user has the ability to edit the defined fields. Some of the fields can be directly updated. However, some of the editing needs might need prior approval from the necessary authorities.

9. My Profile (Virtual ID generation) Mean generating user defined virtual IDs that mask the general ID details.

9.1. Profile View - The user will be able to define their own data set and by selecting the data fields that appear on the screen and create own virtual ID

9.2. Virtual ID (download/ share options) - Different options such as downloading and sharing are available for the Virtual ID

9.3. Virtual ID request - User should be able to request Virtual ID which will mask the original UDI and this need to be define the validity period

9.4. Define validity period for the Virtual ID.

10. My Profile - Display e-UDI

10.1. If the user currently doesn't have a mobile ID, the user will have the ability to request one.

10.2. Should have the capability to display both sides of the mobile ID.

10.3. The new information updates by the user should be reflected in the Mobile ID. in order to facilitate this the Mobile ID and the UDI data should always be in sync.

11. My Profile - QR code generation

11.1. The user is able to select the relevant data and generate the QR code.

11.2. The generated QR code can be either downloaded or shared.

11.3. Predefined QR Code option also need to be in place

11.4. Consent popup to the citizen when the client read the QR code for request information. utilize a predefined QR code that can be scanned by the client. To get the consent of the user in sharing data, a popup will be appearing.

11.5. This predefined QR code can be utilized as login credentials to acquire other necessary government services.

12. My Profile - Track My Request

12.1. The option will allow the users to track their requests which were made through the application.

12.2. An option to create a new request which directs the user to the e-services section.

13. My Profile - Settings

13.1. The users will be able to update their preferred languages. (Sinhala, English)

13.2. Settings will provide the option to enable and disable authentication modes.

14. My Profile - Digi Locker

14.1. Pointers to necessary approved documents so that application does not required to store locally this information.

14.2. Users have the facility to upload new documents which will be reviewed later and added to the Digi locker.

15. My Profile - My History

15.1. Users will have the ability to access all the historical transactions made through the application.

16. E-Services Section

16.1. Two separate sections will be available for Government Services and Private Sector Services

16.2. Integrated Private or Government Services will be listed under each tile

16.3. The users are able to search necessary government departments and add them as a tile

16.4. Based on the security sensitivity of the services, user Authentication with UDI is required. (example: if the user request service for police report, re authentication is popup)

17. My Requests

17.1. This option will display all the services which require the user to act upon.

17.2. User authentication with the UDI is required based on the security sensitivity of the services.

- Simple authentication request
- Request digitally stored documents (Digi locker)

17.3. In a scenario where the user wants to submit information along with documents in the Digi locker, the users will have to enter their UDI in the necessary website. After the UDI is entered a popup will be displayed to take the consent to share this information.

17.4. Open requests tab: The tab will display all the open requests. Which user wants to take actions on

17.5. Rejected requests tab: Tab to display rejected requests.

17.6. Approved requests: This will display all the approved requests.

18. Support Center

18.1. Chatbot tab: The chatbot option is available for the user to communicate with the system virtually.

18.2. FAQ tab: In order to find solutions for the frequently raised questions, the user can refer to this.

19. Email Option: The user is able to send mails through this option when needed.

h) Citizen Portal

A web portal shall be implemented as part of SL-UDI Information System. The SL-UDI Web

Portal would be available to all stakeholders (residents, internal users, contact center agents, TSPs, Administrators, etc.) to perform various functions under the digital identity ecosystem. The residents will be able to use applications such as pre-enrolment, public dashboard, enrolment status, etc. The internal users will be able to access applications like manual quality check, adjudication. The contact center will be able to use applications such as CRM, Partner Management. The TSPs will be able to use the applications such as Partner Management. MSI shall be responsible for the following:

(i) Gather requirements and design the SL-UDI Web Portal.

(ii) Development of the SL-UDI Web Portal.

(iii) Hosting and subsequent maintenance of the portal in accordance with the service levels.

(iv) Implementation of a robust portal security solution and its continuous improvement on an ongoing basis.

(v) Develop the portal's initial content in consultation with GoSL. Train the GoSL's officials to update the content based on requirements.

(vi) Implement a "Content Management" framework and solution to allow authorized users of GoSL to manage publication of new content on the portal. The proposed content management solution should meet the minimum technical specifications given in the RFP. As part of this, MSI shall provide training to users identified by GoSL on the following:

   a. Overview of the GoSL's Portal Content Management Framework.

   b. Portal operations such as upload of content, managing publication, archival, etc.

(vii) Re-design/enhance the portals whenever required on GoSL's request. Some of the key requirements of such re-design/enhancement shall be:

   a. Leverage technological advancements for portal applications as they emerge and implement the same.

   b. Implement basic design principles in portal design including use of consistent, unified common themes including a consistent unique stylesheet including fonts, colours, etc. and implement consistent look and feel and navigation.

   c. Provide universal accessibility: The portal shall be accessible to all irrespective of technology, platform, devices, or disabilities of any kind. The portal shall adhere to the W3C web content accessibility latest guidelines.

(viii) The MSI is expected to position appropriate qualified and trained manpower to manage the portals.

(ix) The portals should support Sinhalese, Tamil, and English languages.

Note: The SL-UDI Web Portal refers to various independent portals i.e., Enrolment Partner Portal, Authentication Partner Portal, Public Portal, Private Portal, Citizen Services Portal and Developer Portal (incl. documents, starter packs, SDKs).

i) Service Billing System

The Service Billing System (SBS) is designed to allow various stakeholders and citizen to make payments for services. The SBS captures the purpose of payment, details of the user and calculates fees based on configurable business rules. The SBS will be used for transactions such as Card Replacement and other services involving payments.

The MSI shall be responsible for design, develop and maintain the SBS. The MSI can choose to utilize a COTS or develop a bespoke application for this component. The SBS should have following features:

a. Should be integrated with the payment gateway provided by GoSL to enable various types of payments, their reconciliation, and their refund

b. Support billing for G2C and G2B scenarios

c. Manage customer profile, metering and pricing configurations, invoicing and receivables, collections, notifications, reporting, etc.

d. Should be integrated with Authentication Solution, Pre-Enrolment Application, Enrolment Software, Web Portal, Mobile Application, BI & Analytics Solution, etc.

e. Should support create payment transaction records, record an audit trail of all actions, payment refund, payment status tracking, etc.

4. Infrastructure Functional Requirements

4.1. Indicative Architecture for Virtualized platform

MSI to ensure the proposed virtualization and container platforms shall support a secure, enterprise-grade orchestration that provides policy-based control and automation to the infrastructure.

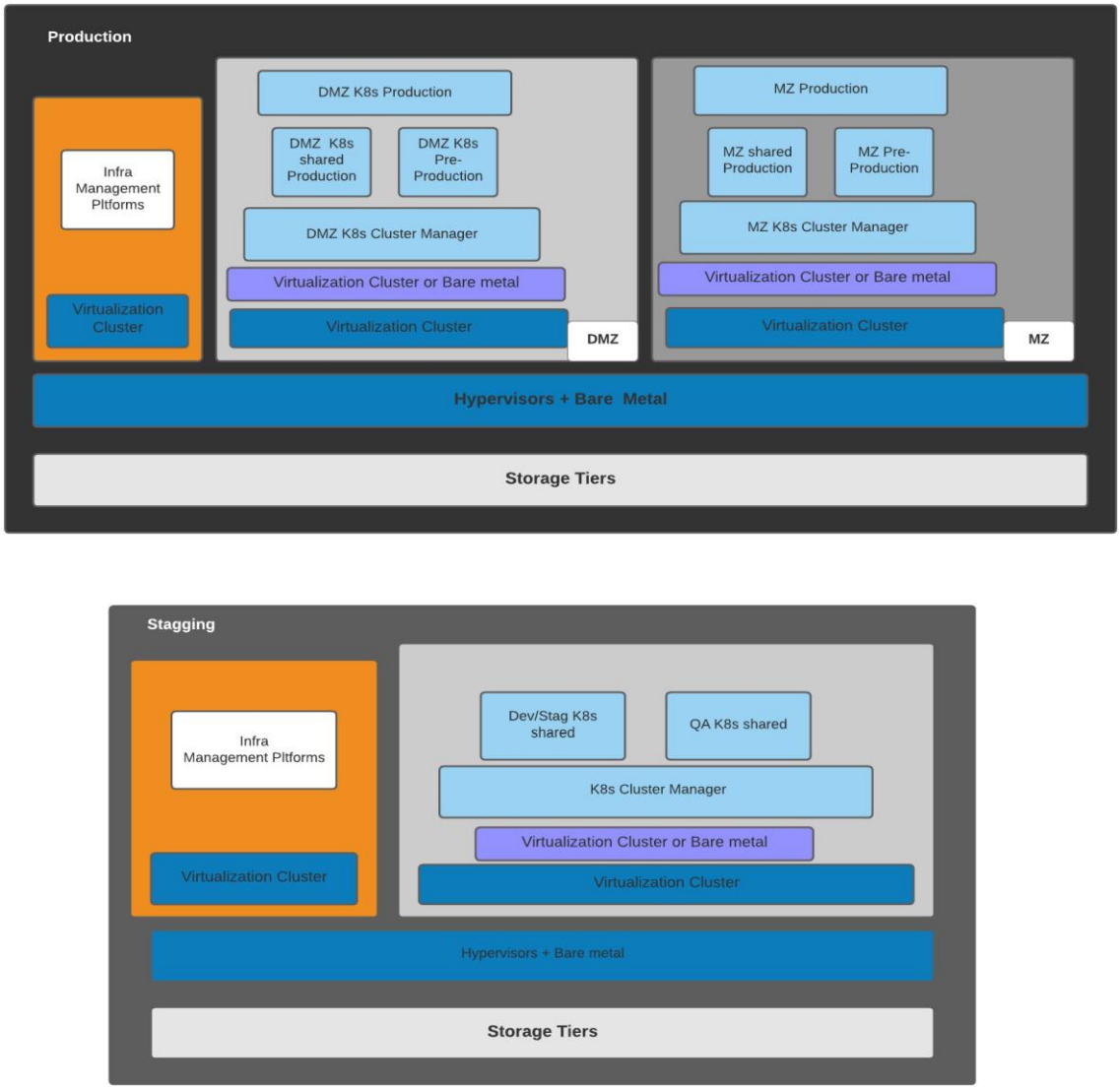


Figure 4: Indicative Architecture for Virtualized platform

This is only an indicative illustration, the bidder may propose better arrangement if any shall implement infrastructure stag environment with required capacities and capabilities, the MSI shall calculate and estimate a required number of nodes and capacities for staging environment and production environments. The MSI will be responsible for setting up all test environments required for the acceptance tests, and should ensure that all environments, hardware, software, and other related configurations are setup as required.

Multi storage tiers to be used in underline storage infrastructure in order to cater to general IOPS and higher IOPS workload requirements. Separate management cluster to be deployed and production

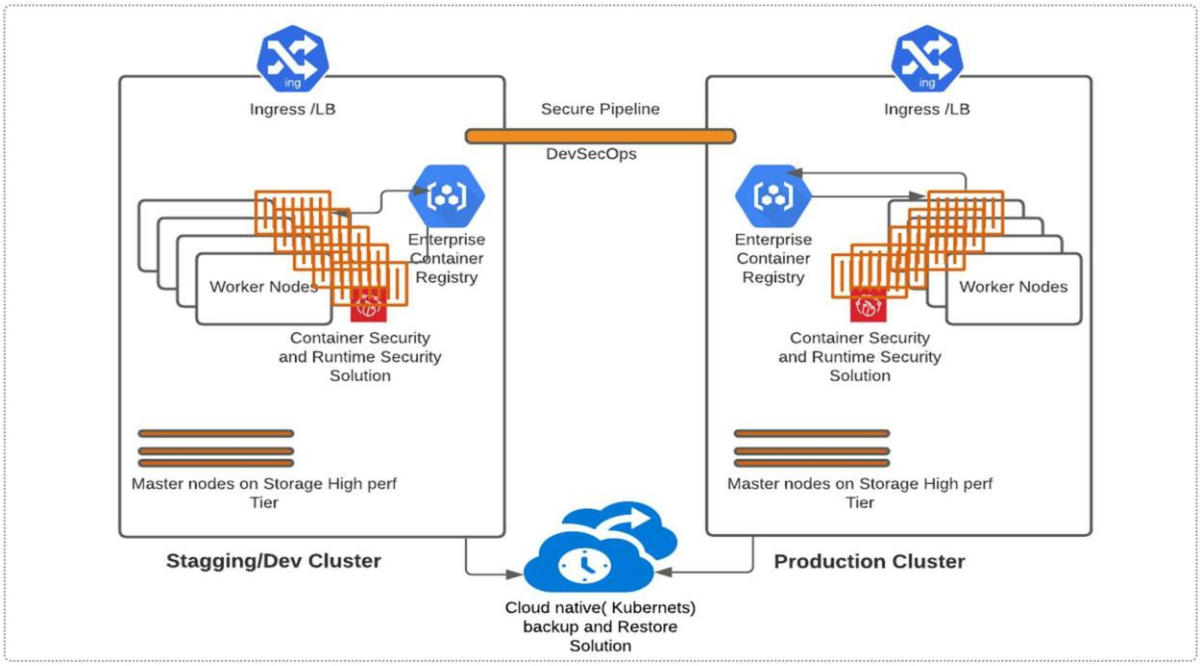
MZ and DMZ zones to be segregated. Inter-zone workload communications shall strictly through firewall cluster. This should also include a highly- available administrative console for management of the virtual data center platform to conduct activities such as onboarding/managing/updating hosts, virtual machines, storage, and networks. Provide the ability to hot-add CPU and memory and hot-plug disks and NICs (provided the same is supported by the guest operating system).

Refer to Annex 3: Virtualization Platform and subsections of specification

Enterprise-grade container platform to be implemented on top of the virtualization platform or on top of bare-metal servers, a bidder may decide and propose considering SLUDI to meet optimum performance level. Platform shall be able to define security policies and controls for each workload based on dynamic security groups, which ensures immediate responses to threats inside the environment and enforcement down to the individual virtual machine.

The Platform should have the ability to deliver end-to-end security for all applications by delivering network-level micro-segmentation, distributed firewalls, load balancers, virtual routers, virtual switches and VPN, compute-level encryption for VM, hypervisor, and live migration.

4.2. Indicative Container platform and Security Solution Architecture



DC Site

Figure 5: DC Site

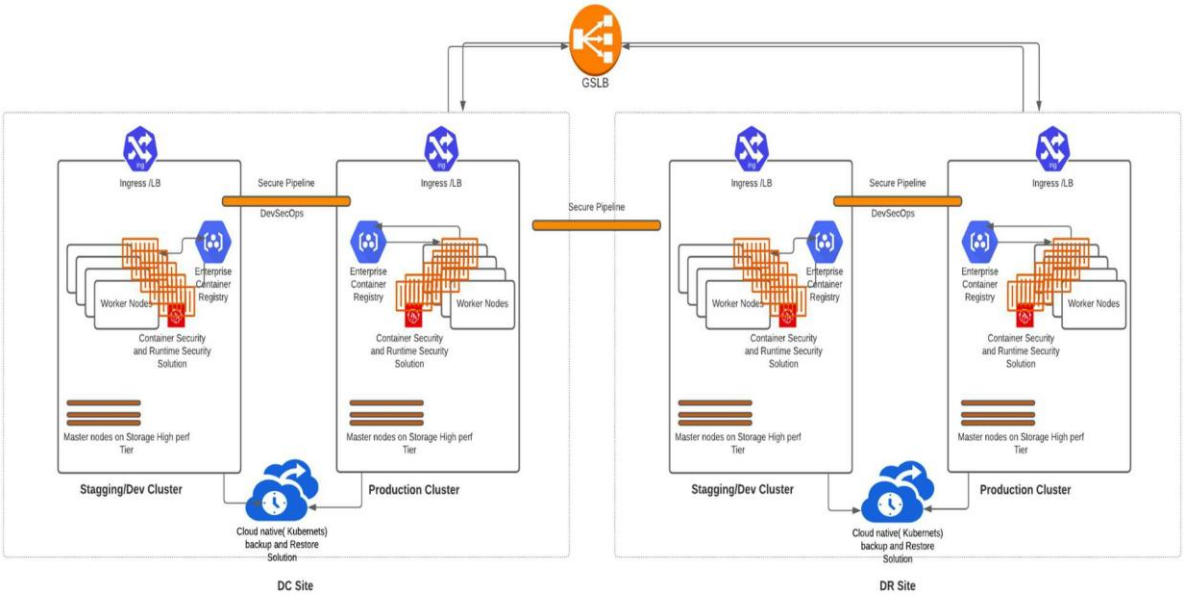


Figure 6: Indicative Container platform and Security Solution Architecture Diagram

MSI to ensure the proposed container platform shall support a secure, enterprise-grade orchestration that provides policy-based control and automation for applications. Enterprise- grade container platform master nodes may deploy on a high-performance storage tier for better performance. Enterprise-grade container registry should be used, and each environment shall integrate via secure DevSecOps pipelines. Security shall be built into the DevSecOps process and the containerized environment throughout its lifecycle. This includes the development and build process, testing, and deployment to production.

Refer Annexure 3:Minimum Technical Specification (3.4.3.8. Enterprise Container Application Platform)

The MSI shall provide Cloud-native applications (k8s) backup and restore Solution and support in place restore and restore into a separate namespace.

Refer Annexure 3:Minimum Technical Specification (3.4.3.6. Cloud Native Backup and Restore)

Use a defense-in-depth approach to protect the containers across their lifecycle by using continuous vulnerability management, compliance checking, and enforcement, runtime defense, and a cloud-native firewall.

Refer Annexure 3:Minimum Technical Specification (3.4.3.10. Container Runtime Security and East-west Traffic Inspection and Attack Mitigation Solution)

4.3. Indicative Security framework/Architecture

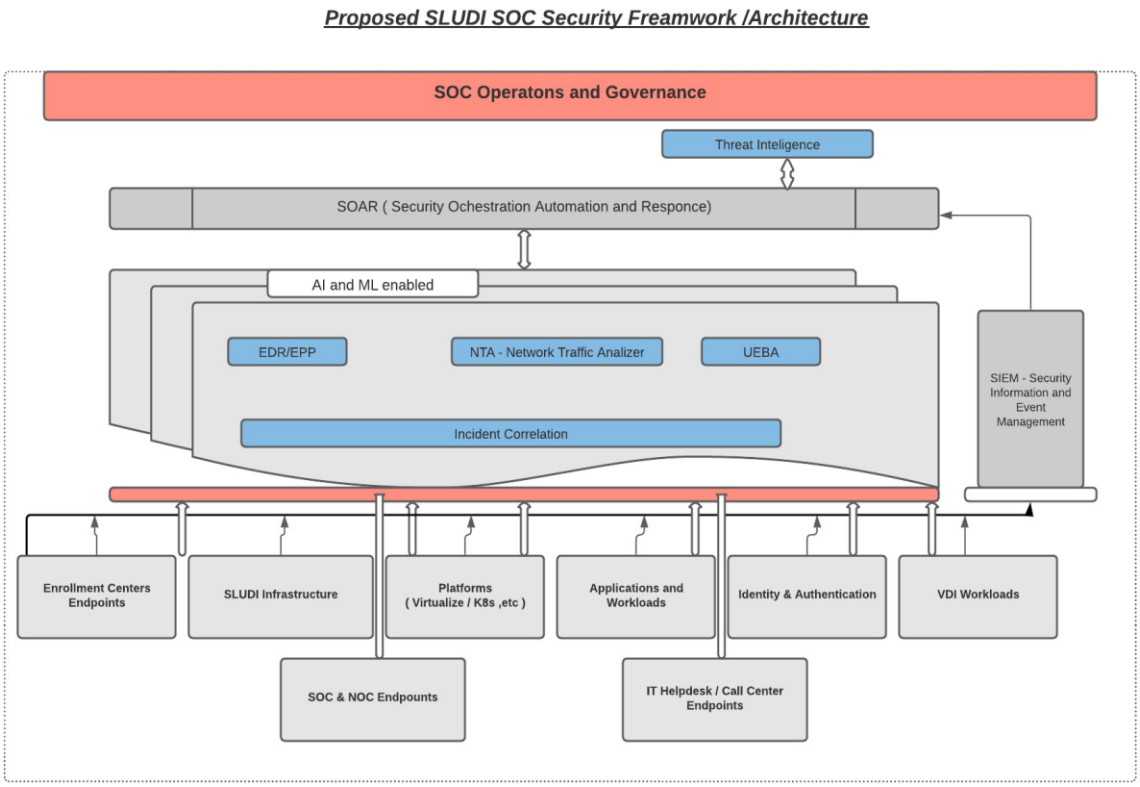


Figure 7: Indicative Security framework/Architecture

SOC setup and framework shall comprise all mentioned security tools and solutions (e.g.- EDR, SIEM, UEBA, Threat Intel, NTA/NDR, etc.) in RFP. *Refer Volume2: 1.1.1.1. SOC Setup and Annex 3: Infrastructure and Security sections.*

As above depicted Schematic shall protect and monitor all enrolment centers endpoints, SLUID infrastructures (DC-DR), platforms, applications and workloads, VDI workloads, SOC/NOC endpoints, and IT help desk and call center endpoints.

4.4. Latest and Proven Technologies by MSI

MSI should offer the latest and proven technologies that are available for items including but not limited following: *(Refer Annex 3 : Minimum Technical Specification)*

a) **Endpoint Detection and Response (EDR)**: Real-time monitoring and detection of threats, and automated remediation. This solution must include both antivirus and HIPS capabilities as well. The solution shall be deployed as per the specifications, industry best practices, program requirements etc.

b) **Security Orchestration Automation and Response (SOAR)**: A solution stack of compatible software programs that allow an organization to collect data about security threats from multiple sources and respond to low-level security events without human assistance. The solution shall be configured as per specifications, industry best practices, program requirements etc.

c) **Security Information and Event Monitoring (SIEM)**: To get full visibility of the infrastructure via logs. Provides enterprises with network security intelligence and real- time monitoring for network devices, systems, and applications. SIEM shall be deployed and

integrated with all systems in the SL-UDI program such as servers, databases, network devices, applications etc. Monitoring rules and correlation rules shall be developed to ensure that real time alerts are generated and shall be monitored. Solution deployment shall be capable of developing correlation rules across sites such as between DC and DR. Configuration, integration and rule review shall be performed as per the defined SLA.

d) Web Vulnerability Scanner: Tool used for web application security. Scans and identifies vulnerabilities in web applications. All applications in the program shall be scanned for vulnerabilities using a standard vulnerability scanner to scan against OWASP top 10, SANS top 25, etc. Any new application or change in an existing application must be scanned for vulnerabilities and all vulnerabilities must be addressed and re-scanned for closures before deployment in production. These vulnerabilities shall be fixed promptly upon identification as per the defined SLAs.

e) Code Review Tool: To conduct security code review of an application's source code in order to ensure that the application has been developed so as to be "self- defending" in its given environment. The source code review tool shall be deployed, and all applications and codes shall be scanned as per the SLAs. Any new application, codes or any changes in existing applications shall be scanned for vulnerabilities and gaps shall be addressed and rescanned for closures before deployment in production as per the SLAs.

f) Patch Management Tool: Tool for managing patches or upgrades for software applications and technologies. Patch management solution shall be deployed for all operating systems, software's, solutions that are deployed in the program/project. Patches shall be deployed promptly as per the software vendor requirements and alerts sent by these vendors. The vendor shall subscribe for automated alerts with all such software OEMs. Critical patches shall be deployed promptly upon release.

g) Network Vulnerability Scanner: Vulnerability management tool to find security loopholes in the networks. All live hosts and IPs on the network and all zones shall be scanned for vulnerabilities as per the SLAs. Any new infrastructure or change in an existing infrastructure must be scanned for vulnerabilities and all vulnerabilities must be addressed and re-scanned for closures before deployment in production. All vulnerabilities shall be fixed promptly as per the SLAs.

h) Network Detection and Response (NDR): A network detection and response solution to monitor network traffic for malicious actors and suspicious behaviour to detect cyber threats to the network.

4.5. Indicative Overall DC/DR Architecture - Bird's Eye View

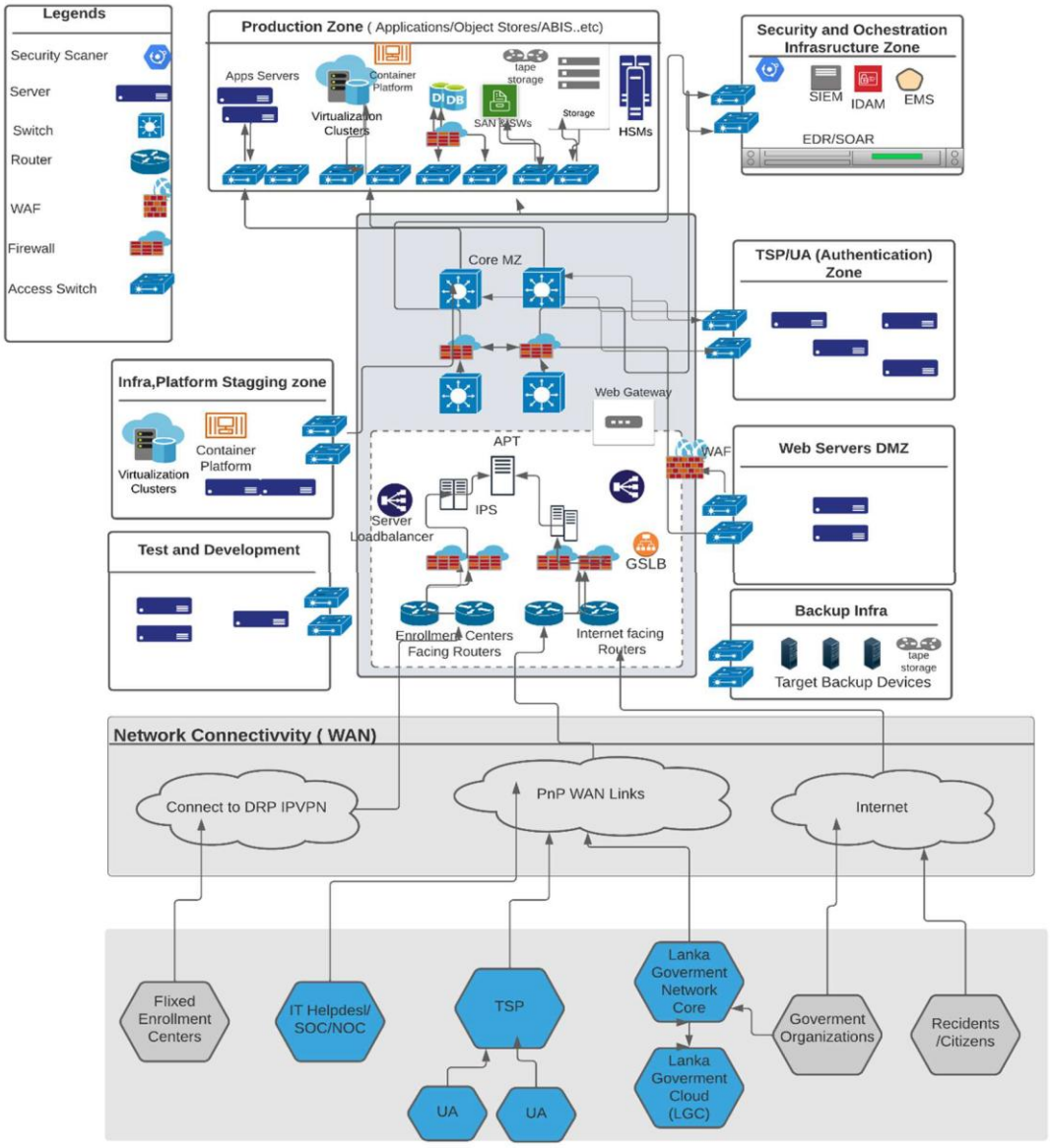


Figure 8:Indicative Overall DC Architecture - Bird's Eye View

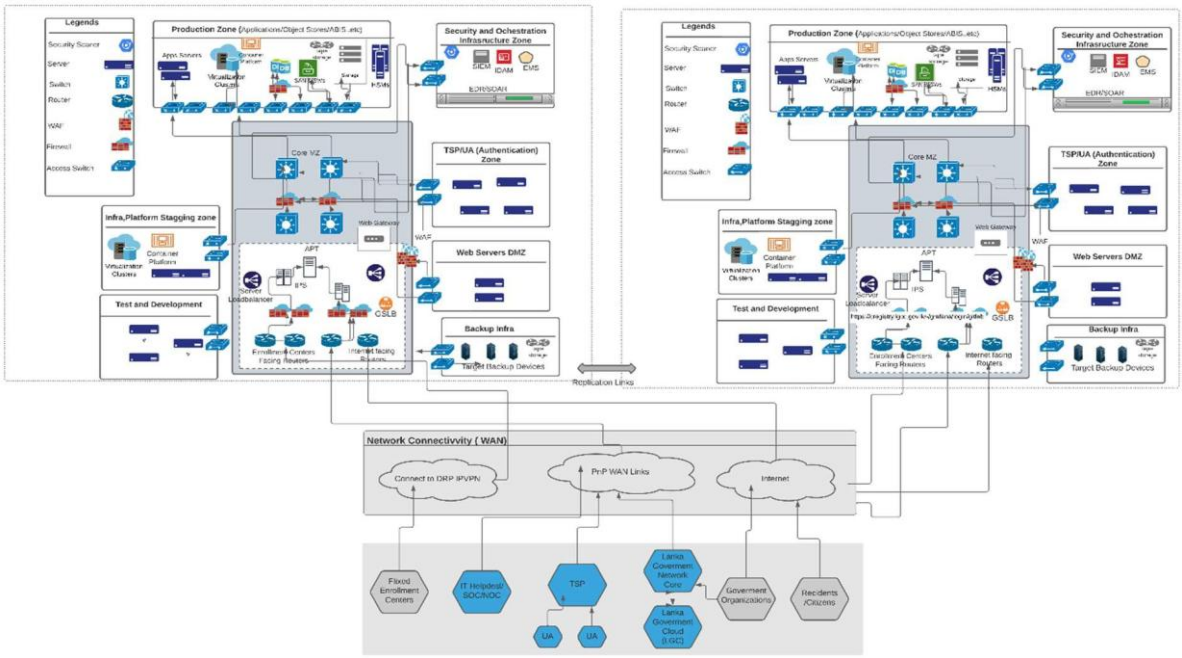


Figure 9: Indicative Overall DC/DR Architecture - Bird's Eye View

*(*Refer *Volume 2 and all annexures, these are only an indicative architectures)*

Fixed enrolment centers to be connected via DRP IPVPN network, DRP will extend exiting IPVPN network to DC, DR and NOC/SOC/IT helpdesk building, Bidder shall facilitate required interfaces and devices to terminate the connections in respective locations. IT Helpdesk, SOC, NOC to be connected to DC and DR via p2p WAN links, bandwidth to be decided by MSI. Shall provide an optimum way of separate HA devices clusters for connectivity at data canter level. Lanka government network(LGN) and Lanka government cloud(LGC) will connect to DC and DR with redundancy, DRP will provide required connectivity(layer2 MPLS) from LGN/LGC to SLUDI DC and DR, MSI shall facilitate required termination devices and interfaces at data centers(DC/DR). DC/DR Replication link to be implemented considering the RTT/latency requirement of applications.

Perimeter level shall comprise of NGFW, IPS/IDS, SSL/IPSEC VPN concentrators, Anti APT, Secure email gateway, secure web gateway. etc.) Each zone is to be segregated physically and/or logically in an optimum way. [Refer 4.6 Indicative Zoning]

MSI should offer the latest and proven technologies that are available for items including but not limited following:

(Refer Annex 3 : Minimum Technical Specification)

a) Virtualization Platform: Virtualization uses software that simulates hardware functionality to create a virtual system in SLUDI. This allows SLUDI to operate multiple operating systems, more than one virtual system, and various applications on a single server with greater efficiencies and economies of scale.

b) Automation and Orchestration: MSI should automate the infra provisioning requirement, Monitoring and DR automation for SLUDI.

c) Enterprise Container Application platform: Enterprise Container platform: provide a container runtime environment, that allows to create containers, manage container images, and

perform operations while allowing to manage, govern and automate containers at scale. Container-compatible storage platforms. Container orchestrators can connect to storage and dynamically provision storage volumes. Ensure SLUDI storage infrastructure integrates with the development life cycle and can support the required performance and availability of containerized workloads. When running SLUDI applications containers at scale, eliminate manual network configuration, and leverage network automation capabilities of container orchestrator.

d) **Container and runtime security and Attack mitigation solution:** SLUDI Containers need to ensure have, full-stack security to address vulnerability management, compliance, runtime protection, and network security requirements of containerized applications running on SLUDI DS.

e) **NextGen Firewall (Internal and External)**: To provide a barrier to control network traffic both into and out of an organization's Internet-connected network, or between different segments of an internal network. Firewalls also provide protection against threats including denial of service (DOS) attacks. All traffic between the zones shall pass through firewalls and firewalls shall be configured appropriately as per the best practices, least privilege requirement, program requirement, architecture and any other specifications provided. Segmentation and zones shall be proposed by the vendor as part of the solution. Firewall configuration and policies shall be reviewed as per the SLAs.

f) **Web Application Firewall (WAF):** Filters, monitors, and blocks HTTP/HTTPS traffic to and from a web application. By inspecting HTTP/HTTPS traffic, it can prevent attacks stemming from web application security flaws, such as SQL injection, cross-site scripting (XSS), file inclusion, and security misconfigurations. WAF shall be deployed for all web applications (internet and intranet). Any access to a web application (internet or intranet web application) whether from outside the network or inside the network shall pass through a web application firewall. Web application firewall shall be configured as per specifications, industry best practices such as OWASP top 10, program requirement etc. WAF configuration and policies shall be reviewed as per the SLAs.

g) **Host Intrusion Prevention System (HIPS):** To protect hosts against local, application and network-based attacks. HIPS shall be installed on all endpoints (servers etc.) to protect the endpoints. The solution shall be deployed as per the specifications, industry best practices, program requirement etc.

h) **Intrusion Prevention System/Intrusion Detection System (IPS/IDS):** To inspect network traffic to identify signs of malicious activity and policy violations, enabling organizations to respond before a threat actor causes significant harm to IT systems. IPS/IDS solution shall be configured and deployed as per the provided specifications.

i) **Data Loss Prevention (DLP):** To identify, monitor and protect data in use, data in motion on network, and data at rest in data storage area or on endpoints. The DLP solution shall be deployed for all endpoints (desktop, laptop, etc.) wherever data may be stored, all network gateways, all email gateways etc. from where data may go out and servers (data at rest module) where data may be stored. The deployment, configuration, rules etc. shall be reviewed on a periodic basis as per the SLA.

j) **Email Gateway:** To prevent data loss, perform email encryption, protect against malware. By detecting and blocking malware, spam, phishing attempts, and other malicious content, can significantly reduce the no. of attempted and successful attacks against an organization. Email gateway solution shall be deployed as per the specifications. Solution shall be

configured to monitor emails for unwanted content, phishing emails, scan for malwares, prevent malicious files etc.

k) **Web Gateway:** To filter unwanted software/malware from user-initiated Web/Internet traffic. Used for black box testing or dynamic testing of the web applications. Web gateway solution shall be deployed on the network at the gateways which provide access to the internet. Content filtering shall be configured to ensure that there is restricted access to the internet as per a defined and approved internet access matrix. The solution shall be configured as per specifications, industry best practices, program requirements etc.

l) **SSL VPN:** SSL VPN solution for Internet users to security access applications. SSL VPN solution shall be deployed for access to infrastructure from a remote location in a secure manner.

m) **2 Factor Authentication (2FA):** Combination of password and OTP/ Biometrics to ensure secure login and avoid unauthorized access. 2 factor access control shall be deployed across all systems and solutions for the entire program. Solution deployment and configuration shall be reviewed on a periodic basis as per the SLA and shall be updated on a prompt basis.

n) **Hardware Security Module (HSM):** Dedicated crypto processor that is specifically designed for protection of the crypto key lifecycle. It protects cryptographic infrastructure of organizations by securely managing, processing, and storing cryptographic keys inside a hardened, tamper-resistant device. HSM modules shall be configured and deployed as per the provided specifications.

o) **Privileged Access Management (PAM) / Privileged Identity Management (PIM):** To secure, manage and track administrative access to privileged accounts. PAM/ PIM solution shall be deployed to manage the user lifecycle in the program and to manage privilege access to the servers, network devices, and databases etc. as per the specifications. The privilege access solution shall support all systems for privilege management such as server OS privileges, database privileges, application privileges, network devices privileges etc. The deployment, configuration etc. shall be reviewed on a periodic basis as per the SLAs.

p) **Virtual Desktop Infrastructure (VDI):** Virtualization technology that hosts a desktop operating system on a centralized server in the datacenter. The VDI solution shall be configured and deployed as per the provided specifications.

q) **Access Control System and Directory Services:** Centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories. Centralized and standardized access control system and directory services shall be deployed to automate network management of user data, security, and distributed resources, and to enable interoperation with other directories as per the specifications.

r) **Database Activity Monitoring (DAM):** To independently monitor and audit all database activity, including administrator activities. To generate alerts on policy violations, provide real-time monitoring and rule-based alerting. DAM shall be deployed for all databases to ensure that all databases are protected by the solution and help in improving database security by detecting unusual database read and update activities etc. from the application layer. Database event aggregation, correlation and reporting shall be done to improve database audit capability without the need to enable native database audit functions. Solution shall be deployed in such a manner that it does not adversely affect the performance of the databases.

s) **Anti-Advanced Persistent Threats (Anti-APT)**: Advanced Persistent Threat Protection solution. Anti-APT solution shall be deployed for the network, endpoints etc. as per

specifications. All network traffic shall go through the Anti-APT solution and shall be analyzed for malwares/malicious software etc. The deployment, configuration etc. shall be reviewed on a periodic basis as per the SLAs.

t) Anti-DDoS: To prevent DDoS attacks. Anti-DDoS solution shall be deployed on the network perimeter for internet and MPLS traffic to protect against DDoS attacks. The deployment, configuration etc. shall be reviewed on a periodic basis as per the SLA.

u) GSLB: Web traffic management and application delivery over SLUDI DC and DR data centers. All RTO/RPO=0 services may wire through the GSLB.

4.6. Indicative Zoning

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

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

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

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

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

   Access to infrastructure hosted in this zone: Only from Zone-2 (Users room Infrastructure

   Management zone only) after Firewall and other security measures.

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

   Access to infrastructure hosted in this zone:

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

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

   Access to infrastructure hosted in this zone

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

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

   Access to infrastructure hosted in this zone

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

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

   Access to infrastructure hosted in this zone

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

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

   Access to infrastructure hosted in this zone

   - *WAN: None*
   - *Within DC: Zone-2, Zone-3 and internal applications require communication with this zone.*

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

   Access to infrastructure hosted in this zone

   - *WAN: None*
   - *Within DC: Zone- 2, Zone-3 and internal applications require communication with this zone*

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

   Access to infrastructure hosted in this zone

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

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