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

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

January, 2026

Table of Contents

1 Introduction 6
1.1 Background 6
1.2 Current Challenges and Need of This Project 6
1.3 Objectives of the Project 7
1.4 Stakeholders and their responsibilities 7
1.5 Adopted Standards (Demographic, Biometric, etc.) 8
1.6 Targeted Sizing and Design Consideration Performance Parameters (Throughput, Accuracy, Availability, Integration) 9
1.7 Components and their Procurement Strategy 9
1.8 Key Considerations (Summary of who does what as per MOSIP) 10

2 Functional Overview (As-Is System and proposed functional overview) 14

3 Project Scope 15
3.1 Introduction 15
3.2 SL-UDI Implementation, Operations, Support and Maintenance 15

4 Solution Overview 18

5 Scope of Services 19
5.1 Software Solutions 30
5.1.1 Phase-wise Implementation of SL-UDI Software System 30
5.1.2 MOSIP Application 31
5.1.3 COTS Application 33
5.1.4 Support Application 36
5.1.5 Biometric Solution Implementation 39
5.1.6 Solution Testing 42
5.1.7 Integration of MOSIP Applications with SL-UDI Information System 45
5.2 Hosting Infrastructure 48
5.2.1 Data Center Site Set-up 48
5.2.2 Hosting Environments 49
5.2.3 Installation, Configuration and Testing 50
5.2.4 Design and Commission 52
5.2.5 Server Services 52
5.2.6 Network Services 53
5.2.7 IT Infrastructure Requirements 55
5.2.8 Storage Services 56
5.2.9 Backup and Replication Services 56
5.2.10 Virtual Environment Services 57
5.2.11 Container & OS Environment Services 58
5.3 Field Infrastructure 58
5.3.1 Biometric Registration Kit – (As per the BOQ) 58
5.3.2 Supply, Installation and Commissioning of Enrolment Kits 60
5.3.3 Service Centers and Spares 62
5.4 Enrolment Centers 63
5.5 Identity Cards 63
5.6 Training and Capacity Building 63
5.6.1 Training Needs Assessment 63
5.6.2 Preparation of Training Plan 64
5.6.3 Impart Trainings (Refer Annexure-14-List of Indicative Trainings) 64
5.6.4 Ensure Training Effectiveness 64
5.7 Performance Testing, Security Compliance & Audit, Acceptance and Go-Live 65
5.7.1 Performance Testing 65
5.7.2 Acceptance 67
5.8 Information Security and Business Continuity 71
5.8.1 Information Security 71
5.8.2 Business Continuity and Disaster Recovery 82

5.8.3 Deliverables for Information Security and Business Continuity *88*
5.8.4 Support (Contact Center and Helpdesk) *94*
5.8.5 IT Helpdesk *98*
5.9 Security and Network Operations 102
5.9.1 Security Operations (Complying with SOC-2 standards) *102*
5.9.2 Network Operations *104*
5.10 Business and Technical services 106
5.10.1 Business Services *106*
5.10.2 Technical Services *112*
5.11 Operations and Maintenance 116
5.11.1 Support and Maintenance Services *116*
5.11.2 Hosting Infrastructure (SL-UDI-DS and its Operations, Maintenance and Administration Services) *117*
5.11.3 Software System (including MOSIP, Biometric, and all other components) *130*
5.12 Project Reporting 135
5.12.1 ABIS Reports *135*
5.12.2 Data Quality Monitoring & Reporting *135*
5.12.3 Incident and Issue Reporting *136*
5.12.4 SLA Reporting *137*
5.12.5 Other Reports *137*

6 Implementation Schedule 137
6.1 Project Duration 137
6.2 Implementation Schedule 138
6.3 Implementation Milestones 139
6.4 Transition to Managed Service Provider (MSP) – 152

~~7~~ Schedule of Requirements 152

8 Change Request 158

9 Compliance to Schedule of Requirements 159

List of Tables

Table 1: Stake Holder Responsibilities 8
Table 2: Standards Adopted 9
Table 3: Key Considerations 13
Table 4: Key Components 15
Table 5: Scope of Work of the MSI 30
Table 6: Implementation of SL-UDI Software System 31
Table 7: Solution Testing 45
Table 8: Data Center 49
Table 9: Hosting Environment 49
Table 10: Network Connectivity 54
Table 11: Biometric Registration Kit 59
Table 12: Mobile Kits 59
Table 13: Volume of Authentication Biometric Capturing Devices 60
Table 14: pre-supply activities 61
Table 15: Performance of the SL-UDI Information System 66
Table 16: Performance of the SL-UDI Information System 66
Table 17: Performance of the SL-UDI Information System 67
Table 18: Requirement of Solutions on Endpoints as well as Servers 75
Table 19: Security of SL-UDI data centers, data stores and administrative offices 82
Table 20: Indicative List of Recovery Strategy of Processes 84
Table 21: HSM Recovery 86
Table 22: Disaster Recovery Strategy and Procedures 87
Table 23: Deliverables for Information Security and Business Continuity 94
Table 24: key features of the proposed Contact Center 97
Table 25: Sample Queries at the Contact Center 98
Table 26: Level Definition 101
Table 27: Indicative Bill of Material for SOC 103
Table 28: part of SOC operations 104
Table 29: NOC operations 106
Table 30: Server and Virtual Services Operations Activities 121
Table 31: Storage Operations Activities 124
Table 32: Backup Operations Activities 125
Table 33: Implementation Schedule 139
Table 34: Implementation Milestones 152
Table 35: Bill of Martial 158
Table 36: Change Request 159
Table 37: Compliance Sheet 160

List of Tables

Figure 1: SL-UDI Support arrangement. 17
Figure 2: TSP and UA Applications 38
Figure 3: SL-UDI Project Duration 137

Disclaimer

1 Introduction

1.1 Background

The National Policy Framework (NPF) Vistas of Prosperity and Splendour is aimed at achieving a fourfold outcome of a productive citizenry, a contented family, a disciplined and just society, and a prosperous nation. A Technology Based Society (Smart Nation) is one of the 10 key goals of the NPF. In that, setting up a Citizen Centric Digital Government and digitally empowered economy have been identified as a strategy to achieve the government vision.

Governments worldwide are adopting the strategy of having a Unique Digital Identity (UDI) Framework and Architecture to empower citizens within a Digital Economy and Society. It is envisioned that it could enable dramatic leaps in service quality and massive efficiency gains for governments, as well as drive financial and social inclusion to a maximum extent by providing citizens access to citizen services and benefits of healthcare, education, and other government programs.

In view of the above, the Sri Lankan Government has also given priority for a national level program for the establishment of a Unique Digital Identity Framework for Sri Lanka (SL-UDI). Therefore, the SL-UDI Framework has been defined as a foundational component with the overall Digital Government Architecture for Sri Lanka as defined by the ICTA (Apex Institution of Government of Sri Lanka).

Sri Lanka has a strong lineage in the (physical) registration and issuance of Identity Documents (including National Identity Cards). Further, the Department for Registration of Persons (DRP) has been vested with powers by the Registration of Persons Act No. 32 of 1968 to secure the identity of persons by ensuring timely registration of citizens of Sri Lanka. Therefore, the SL-UDI framework is being established in close collaboration with DRP and ICTA/Ministry of Digital Economy (MoDE) as the key stakeholder of the project.

By now, Government of Sri Lanka (GoSL) is in the process of carrying out detailed planning related to possible regulatory changes, process re-engineering, and solution implementation. Considering the SL-UDI framework is a vital element in delivering the National Policy Framework of the Government, Government of Sri Lanka (GoSL) intends to expedite the implementation of the SL-UDI through an accelerated time period.

Government of Sri Lanka (GoSL) will be leveraging Modular Open-Source Identity Platform (MOSIP) with the expectation that the foundational ID platform for SL-UDI be built using the MOSIP platform.

1.2 Current Challenges and Need of This Project

One of the main concerns of the government with regard to identity is that *there is a significant number of duplications among multiple departments where the exact number of citizens cannot be ascertained due to the lack of an efficient and accurate identity system*. As a result, government funds may be wasted or misused.

One of the key concepts that the proposed project intends to address is the issuance of a 'National Unique Digital Identifier.' Currently, there is no mechanism for identifying/authenticating an individual uniquely during digital interactions. As a result, most of the financial and important transactions are carried out manually, despite having cross-government solutions.

Should there be such a unique identifier, all government and private sector systems will be able to recognize each individual interacting with systems and would be able to communicate and transact securely. Currently, there are many inefficiencies in the way citizens interact with others and with institutions as a result of not having such a unique identifier.

Many government organizations are planning to issue their own digital transaction cards. Further, none of those cards carry a digital identifier. Such multiple projects are a waste of government funds. However, if the

government decides to issue a single digital card, incorporating among others, a unique digital identifier of the owner, then it may have a wide variety of uses.

1.3 Objectives of the Project

Cabinet Appointed Procurement Committee of Sri Lanka intends to initiate the procurement to obtain services of a Master Systems Integrator (MSI) in the SL-UDI supply, delivery, implementation, operations, and maintenance. The MSI is required to work closely with GoSL in order to ensure successful implementation of the Foundational ID platform envisioned by the SL-UDI.

Cabinet Appointed Procurement Committee of Sri Lanka is planning to hire the services of a local partner, being referred to as the Managed Service Provider (MSP). This MSP will take-over the components in a gradual manner from the MSI. For details on transition and support strategy, (**Refer Annexure 6:Exit-Management**). The MSI will be required to work collaboratively with the MSP to achieve the objectives of the project and to enable the MSP to operate and maintain the components transitioned to it by the MSI. The project will be governed and monitored by an independent project management consultant (IPMC) working collaboratively with all stakeholders.

The MSI will be required to provide following services:

i. Customization, Implementation and Maintaining the process, hardware systems, network systems, security systems, software systems, biometric systems, biometric capture devices, etc. required to implement Digital Identity in Sri Lanka.

ii. To facilitate and integrate with the components/systems necessary to implement Digital Identity and its use cases.

iii. To fine-tune, operate and maintain the solution for the contract period ensuring at SLA's are adhered to for a smooth operation of SL-UDI during and post implementation.

iv. To suggest and make improvements for smoother operation during the maintenance period.

v. Use of proper technologies to assure high availability, security, performance, and usability of the system.

vi. Provide required documentation and knowledge for gradual transition to the MSP to carry on the operations of SL-UDI.

1.4 Stakeholders and their responsibilities

The following departments and agencies are involved in the complete ecosystem of SL-UDI:

#	Department/Agency	Role
1.	Department of Registration of persons (GoSL)	• Data custodian of the SL-UDI project.
2.	ICT agency of Sri Lanka (ICTA) and Ministry of Digital Economy (MoDE)	• Technical stakeholder for SL-UDI project.
3.	Department of Immigration and Emigration	• Association of SL-UDI number for citizens obtaining citizenship by the respective DRP Act.
4.	Registrar General's Department	• Verification of Birth, Marriage and Death certificates (*Note: UIN will be issued to the Department of Registrar General from the details obtained from the database of Department of Registration of Persons at birth of a citizen*) • Association of SL-UDI number for citizens by birth based on the DRP Act.

5.	Department of Elections	• Verification of Voter Registry
6.	Ministry of Home Affairs	• Verification of Householder Registry
7.	Master System Integrator (MSI)	• For the provision of services as described in this document.
8.	Managed Service Provider	• Work collaboratively with MSI from the start of the project. • Take handover from the MSI for various components in a well-planned, gradual, and seamless manner. • Coordinate with parties (MOSIP, OEMs, etc.) on behalf of the GoSL after the UAT. • Operate and maintain the components transitioned to it by the MSI
9.	Relying parties (TSP)	• Organizations that are leveraging the authentication services of the SL-UDI program
10.	Registered Photo Studios	• To capture ICAO standard photographs of the citizen and share it with GoSL

Table 1: Stake Holder Responsibilities

1.5 Adopted Standards (Demographic, Biometric, etc.)

The following are the ***Standards Adopted***, but not limited to (MSI shall use the latest standard wherever applicable):

#	Description	Proposed Standard
Biometric Standards		
1.	Fingerprint Image	ISO/IEC 19794-4:2011
2.	Fingerprint Minutiae	ISO/IEC 19794-2:2005, or ISO/IEC 19794-2:2011
3.	Fingerprint Image Compression	JPEG 2000
4.	Iris Image Data	ISO/IEC 19794-6:2011
5.	Iris Image Compression	JPEG 2000
6.	Face Image Data	ICAO 9303 compliant (present) and ISO/IEC 19794-5:2011 (in future)
7.	Face Image Compression	JPEG 2000
8.	Biometric presentation attack detection	ISO/IEC 30107-2: 2017
9.	Information security – Criteria and methodology for security evaluation of biometric system	ISO/IEC 19989
Demographic Standards		
10.	Format for Title, Name, Gender, etc.	To be defined by MSI in consultation with GoSL
11.	Date Formats	
12.	Location Names and Codes	
13.	Address Formats	
PKI Infrastructure		
14.	Digital Signature Standard	FIPS 186-4

#	Description	Proposed Standard
15.	RSA—Digital Signature Algorithm	RFC 3447 RSA (PKCS #1)
16.	Secure Hash	FIPS PUB 180-4 (SHA-1 / SHA-256 / SHA – 512)
17.	Cryptographic Modules	FIPS 140-2 Level 3 or more
18.	Public Key certificates	ITU-T X-509, ISO 9594-8
19.	XML Digital Signature	W3C / ETSI XadES
20.	Type	Number
21.	Length (Tentative)	11 (Eleven) digits – inclusive of checksum (it may get finalized during implementation)
22.	Structure	Random Number
23.	Algorithm	To be decided at the time of implementation
24.	Exclusions	To be decided at the time of implementation
25.	Checksum	Yes
26.	Guess-ability	0.5%
Data Exchange		
27.	APIs	Open API
28.	Bar Code / QR Code	ISO/IEC 18004:2015— Quick Response (QR) code and PDF417 / QR code
Others		
29.	W3C verifiable credentials	Data Model 1.1

Table 2: Standards Adopted

1.6 Targeted Sizing and Design Consideration Performance Parameters (Throughput, Accuracy, Availability, Integration)

The SL-UDI should be designed considering as per the **Annexure 5: Demand Capacity**

For the purpose of integration with external systems, all such systems would be integrated using runtime plugin libraries, allowing for the reuse of official container images to facilitate simpler updates and maintenance processes.

1.7 Components and their Procurement Strategy

The selected bidder i.e., Master System Integrator (MSI) will play the following roles:

(i) The MSI will have end-to-end responsibility of system integration, and the MOSIP & Non-MOSIP software components. The MSI will also be responsible for the entire hosting infrastructure and security infrastructure.

(ii) The MSI will be responsible for procurement, supply and maintenance of biometric devices (enrolment and authentication devices) as well as biometric solutions (ABIS, SDK, Manual Adjudication, etc.) and

corresponding hosting infrastructure (server, storage, tape library, etc.)

(iii) The MSI will be responsible for registration kits (excluding the existing components available with GoSL).

(iv) The MSI will be responsible for hosting infrastructure in the Data Center as well as Disaster Recovery site.

Note: (1) At various places in this RFP, the responsibilities are specifically listed for the Master System Integrator i.e., the lead bidder under this RFP

(2) At various places in this RFP, the responsibilities are specifically listed for the Biometric Solution Partner (BSP) which is the provider of biometric solution and the consortium member of the lead bidder (if such consortium exists)

1.8 Key Considerations (Summary of who does what as per MOSIP)

For understanding, the roles and responsibilities of the various agencies are summarized in the table given below for reference purposes. In addition to this, please read the entire RFP to clearly understand their roles and responsibilities. It should be noted that MSI must engage MOSIP for training and technical support of its components.

#	Item	Responsibility
Knowledge Transfer and Support		
1.	MOSIP KT	MSI can access the relevant documentation from MOSIP's website. MSI shall coordinate with the MOSIP team and arrange detailed training for its project team. The MSP can also join the KT sessions along with MSI.
2.	Technical Support (MOSIP)	MSI shall ensure MOSIP provides technical support for its components. The MSI will be responsible for raising the ticket with MOSIP and coordinating with MOSIP for the resolution. As part of the ticket, the MSI may be required to provide logs of debugging, etc. For some issues, the MSI may have to grant access to MOSIP to their development and testing environment.
3.	MOSIP Tools and Technologies	MSI will be responsible for obtaining enterprise support, as available.
Enrolment (Field Aspects)		
4.	Biometric SDK	MSI will provide the Biometric SDK and will integrate the registration client and other components of MOSIP
5.	Registration Client	MSI shall obtain the MOSIP registration client software (customize and undertake necessary integrations and installation in the registration kits, maintain the software and provide technical support
6.	Biometric Capture Devices	The MSI will provide the biometric capturing devices, deploy them with biometric registration kit, integrate with MOSIP, provide its technical support & maintenance, provide replacement devices, and provide comprehensive onsite maintenance and

#	Item	Responsibility
		troubleshooting.
7.	Registration Kit (other than Biometric Capture Devices)	MSI will provide the registration kit hardware, provide maintenance for the corresponding components it supplies under this project. The staff at registration centers will be equipped with basic diagnosis (as per training by MSI) and thereafter they may raise the tickets with IT Helpdesk for repair/replacement of any faulty devices/components. MSI will provide IT Helpdesk (incl. tickets management), provide remote support, provide on-site troubleshooting, escalate, and monitor the tickets to the respective agencies, provide maintenance claim/replacement, etc. For the components provided by GoSL, the escalation will be done to the GoSL team who will in turn be responsible for maintenance claim or replacements.
8.	Queue Management Software and Hardware.	The GoSL will be responsible for providing the queue management software, providing television displays for tokens, etc. The GoSL will setup necessary network wiring at registration centers. The GoSL will be responsible for necessary civil and electrical aspects (including electricity connection, internet/wide-area-network connection, recurring bills for electricity and internet) at the registration centers.
9.	Registration Manpower	GoSL will provide the registration manpower (including supervisors). A comprehensive training will be provided by MSI to the manpower on the different aspects of enrolment including basic troubleshooting of issues.
10.	Training and certification of registration manpower	The MSI will be responsible for planning training, developing training content, conducting trainings, and providing certificates of training completion to the participants.
11.	Registration related issue identification and resolution	Self-Diagnosis: The staff at registration centers will be trained to conduct basic diagnosis (as per training by MSI) and thereafter they may raise the tickets on the MSI's technical helpdesk. The registration client should have a section which can be used by the registration manpower for basic checks (e.g., device connected, test device usability, network availability, etc.). The MSI will be responsible to work with other agencies (BSP, GoSL, etc.) to develop and maintain the Standard Operating Procedures for this self-diagnosis. Remote Support: Helpdesk personnel of the technical helpdesk will provide remote support to diagnose and resolve issues. The first level of remote diagnosis will be performed by MSI. In case of issues with biometric devices, the next level of remote diagnosis

#	Item	Responsibility
		will be performed by the BSP. In case of issues with registration kit (other than the biometric devices), the next level of remote diagnosis will be performed by the MSI/GoSL The necessary software for remote support should be provided by MSI. Onsite Troubleshooting: For issues unresolved through remote support, MSI will do the first level of on-site troubleshooting. If the issue remains unresolved, then escalate it to the concerned agencies. For issues concerning the biometric capture devices, the BSP will be responsible to resolve the issue by operationalizing the device at registration center (if feasible) or provide spare as replacement, picking up the device from registration center, repairing it in its service center, and dropping the operational device at the registration center and connecting it to the registration kit. A similar process will be followed for the other non-biometric components of registration kits by MSI. Management, Monitoring and Reporting: The MSI will be responsible for managing the tickets, monitoring their resolution (including timely escalations), and submitting necessary reports as agreed at the time of implementation.
Enrolment Packet Processing (Centralized)		
12.	Components based on MOSIP (Pre-registration, Identity Management, Unique Identity Generator, Authentication Solution, Partner and Device Management.	MSI will provide software (customize MOSIP and undertake necessary integrations), finalize requirements for central infrastructure, install it in the central infrastructure, operate & maintain the software, and provide technical support.
13.	Components based on COTS/OTS and Bespoke Components (refer Section 5.1.3)	MSI will provide software (customize COTS/OTS, develop the bespoke software and undertake necessary integrations), finalize hardware requirements for SL_UDI Project and install it in the data center/ locations mentioned by GoSL, operate & maintain the software, and provide technical support.
14.	Biometric Components (ABIS and Manual Adjudication)	BSP will provide ABIS software and MSI will integrate with MOSIP with assistance of BSP.
15.	Quality Assurance	The GoSL will provide the manpower for review and approval of the enrolment packet as per their processes. The MSI will be required to develop the necessary software-based workflow to support these requirements.
16.	Manual Adjudication	Refer ‘Components based on ABIS’
17.	Unique Number Generation and Allocation	MSI shall provide this feature based on MOSIP and integrate with SL-UDI system.
Personalization, Issuance and Activation of Card		

#	Item	Responsibility
18.	Card Personalization and Issuance	GoSL will provide the 100% polycarbonate pre- printed blank cards, personalize them (incl. internal QA, etc.) and issue the same through the channels (registered post, self-pickup from DRP headquarters, registered courier) preferred by the citizen. The necessary software, hardware and manpower for card personalization, quality check, issuance, etc. is available with GoSL. The information to be personalized on the card may have to be provided by MSI through APIs. The MSI would assist the technology service provider of GoSL to undertake necessary customization in the card personalization software for integration with the aforementioned APIs.
19.	Card Management and Workflow	The GoSL will provide the software for management of cards (inventory management, workflow-based monitoring of card personalization and issuance, integration with issuance applications of registered post & couriers) and provide necessary reports.
Authentication		
20.	TSP and UA Software	Online Authentication and e-KYC will work in a federated structure of trust-based model. The MSI will develop and maintain the TSP and UA (3 sample protype) applications. The MSI will provide necessary documentation and technical support for the TSPs and UAs to deploy this software at their end.
21.	Onboarding of Authentication Partners	MSI will extend necessary technical support to the Authentication Partners for onboarding them as TSPs, and/or UAs.
Grievances		
22.	Grievance Management	MSI will provide CRM solution for grievance management.

Table 3: Key Considerations

[2]MOSIP Technology Stack
(https://docs.mosip.io/platform/architecture/mosiparchitecture/technology-stack)

2 Functional Overview (As-Is System and proposed functional overview)

The functional overview of the SL-UDI system is available in Annexure 1 and 1A.

3 Project Scope

3.1 Introduction

SL-UDI consist of the following high-level components which is elaborated in detail within this volume. In order to understand the project overall design aspect, it is important to understand how each component is aligned with all stake holders.

	Key components as detailed in the Requirement Schedule	Comments
1.	Supply, Implementation and maintenance of Information Technology Infrastructure, for the Data Center and Disaster Recovery Sites Includes connectivity to and between DC/DR sites.	Provisioning of the bandwidth and its commissioning and recurring charges shall be borne by GoSL during implementation and post-implementation phase. MSI will assist in establishing the connectivity between DC and DRC.
2.	Leverage the MOSIP platform to design and implement a foundational Identity platform solution for GoSL, in order to carry out citizen enrolment and issuance of digital identity.	
3.	Supply and maintain enrolment devices for fingerprint, dual iris scanner, face including device management server.	Manpower for enrolment, physical infrastructure (building, furniture, electricity, physical security etc.) for enrolment will be provided by GoSL
4.	Supply, Implement and maintain Commercial off-the-shelf (COTs) Products	
5.	Supply, Implement and maintain the ABIS solution, the Manual Adjudication solution and related integrations.	Manual adjudication manpower will be provided by GoSL
6.	Implement and operationalize the operations and support centers – Contact Center, IT Help Desk, Network Operations Center, Security Operations Center.	All non-IT infrastructure will be provided and maintained by GoSL.
7.	Operational support, Support and maintain the above solution for 3-years.	

Table 4: Key Components

3.2 SL-UDI Implementation, Operations, Support and Maintenance

1. Citizen's Demographic and biometric information, would be securely collected during the citizen registration process by the Departments of Registration of Persons for the issuance of the new National ID, which signifies the Digital ID.

2. Therefore, it is of critical importance that the citizens' data are securely managed. Key considerations for the implementation of the SL-UDI include following: -

   a) Privacy by design and Security by design consideration for the implementation of the SL-UDI framework.

   b) The SL-UDI was designed in accordance with the guidelines of the Personal Data Protection Act No. 9 of 2022.

   c) The SL-UDI data ownership is clearly defined.

   d) The SL-UDI design demands data being encrypted wherever possible.

   e) User Access to SL-UDI is confined within the Country.

   f) The SL-UDI framework has been designed leveraging the Modular Open-Source Identity Platform (MOSIP) framework to enable GoSL to administer, access control and operationally manage the SL-UDI project.

      (i) Service providers are responsible for implementing and operationally managing the SL-UDI framework.

a.	The Master Systems Integrator (MSI) – An Indian firm procured through competitive procurement funded through the GoI grant assistance.	1. Responsible for Implementing (1 year) the SL-UDI Solution, support and maintaining for 3-years.
b.	The Managed Service Provider (MSP) – Sri Lankan firm procured through competitive procurement by GoSL	1. Managed Service Provider for GoSL, responsible for the overall operations, audit, and governance of the SL-UDI as per agreed transition plan from MSI to MSP. 2. Responsible for administration, access control and operations management of the SL-UDI Framework. 3. Responsible for taking over the SL-UDI MOSIP ID Framework and its associated workflow including related COTS from the MSI at the end of the 1st year support time period. 4. Providing Level 01 support for selected key components.

      (ii) The responsibility matrix of MSP and MSI can be seen in the RACI framework attached as Annexure 16.

SL-UDI Support arrangement

SL-UDI Components	Citizen Service	Duration	Supporting Levels		
			L1	L2	L3
SL-UDI SI Component (including MOSIP ID Framework and its associated workflow)	GoSL	1st Year	MSI/MSP	MSI	MSI + OEM
		2nd, 3rd Year	MSP	MSP	MSP + OEM

ALL other components	GoSL	All 3-years	MSI	MSI	MSI + OEM

Figure 1: SL-UDI Support arrangement.

g) The Citizen Service Center (Contact Center) will be the initial point of contact for all queries and issue reporting. The contact center will be managed by the GoSL.

h) Support Levels for SL-UDI components

- During the 1st year Support and maintenance time period, after Go-Live, the MSP / MSI will provide the L1 support and the MSI is responsible for L2 and L3 support.
- At the end of 1st year Support and maintenance, the MSP will be taking over the SL-UDI MOSIP, Associated MOSIP workflow and related COTS from MSI. Therefore from 2nd year onwards, the MSP will be responsible for L2 and L3 support.

i) Support Levels for all other components of the SL-UDI:

- MSI is required to provide L1, L2 and L3 support.

4 Solution Overview

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 OTS/COTS products. The governing design principal and solution overview is provided in **Annexure 11: Overview of Technology**.

5 Scope of Services

The following sections provide an overview of the scope of work of the MSI.

1. The MSI is responsible for the design, develop, validate, update, support, and maintain the foundation ID platform.
2. The MSI's scope of work includes procuring, commissioning, configuration, implementation, integration, deployment, and maintenance of the entire SL-UDI system and its components.
3. The MSI should conduct a functional requirement study of the processes and review & understand the scope and functionalities required to implement the SL-UDI application. Changes which are identified before the sign off the System Requirement Specification should be accommodated by the MSI without a change request and at no additional cost.
4. The MSI shall prepare and submit a detailed design and solution architectures such as server architecture, network architecture, database architecture, security architecture, deployment architecture.
5. If any COTS components are proposed as a part of the proposed solution, the MSI shall conduct a detailed requirements study and produce functional design specifications and deployment design etc.
6. MSI shall be responsible for operations, maintenance, and support of COTS solution as part of the Application Maintenance and Annual Technical Support from OEM including associated updates and upgrades.
7. All patches and upgrades from OEMs shall be implemented by the MSI and the MSI shall conduct comprehensive and integrated testing by the MSI in order to ensure that the changes implemented in the system meet the specified requirements and do not impact any other existing functions of the system.
8. The implementation shall span across the following stages of software development lifecycle.
   a) Requirement verification and Development and customization
   b) Unit Testing, System Testing, Integration Testing, Performance Testing
   c) UAT
   d) Release management and Patch management.
   e) Deploy
   f) Change and version control.
   g) Documentation
9. The MSI shall use MOSIP to satisfy the requirements for the core modules. The MSI shall be responsible for configuring, customizing, and modifying, deploying and maintaining the MOSIP application suite to comply with given requirements. The MSI is required to provide enterprise licenses for MOSIP tools and technologies, wherever available.
10. The MSI shall re-assess the requirement of MOSIP components and suggest customization of the application as per the GoSL requirement, if any.
11. Other than MOSIP, the MSI is encouraged to use open-source applications with enterprise support/license in all possible scenarios, wherever available, for the SL-UDI system. The MSI is expected to estimate the number of licenses required and all the licenses/subscriptions purchased should be under the name of GoSL.
12. The MSI should submit all deliverables (an iterative/phased manner) as specified in the below **Section 6: 'Implementation Schedule'**.
13. The MSI should implement all non-functional requirements (security, governance including role-based

security, user lifecycle management, and complete audit-trails, etc.) mentioned in **Annexure 2: Non-Functional Requirements**.

14. The MSI should integrate the foundation ID platform with Automated Biometric Identification Systems (ABIS), Card Printing Services, Biometric-SDK, Biometric devices, Device Management Services, HSM, Studio Application (ICAO Pics) , and COTS, etc.
15. The MSI should study and implement a mobile application that facilitates digital ID services to the stakeholders.
16. The MSI should study and implement a Citizen portal to facilitate digital ID services to the stakeholders.
17. The MSI should study and build ID platform APIs that are required to integrate with external systems to facilitate Digital ID life cycle.
18. The MSI should propose the most suitable solution to securely exchange data using APIs primarily for the authentication and e-KYC use-cases.
19. The MSI may leverage its own environments for development and end-user application training in order to achieve the delivery timelines.
20. The proposed platform (citizen portal, mobile application, etc.) shall be able to integrate with multiple payment gateways and bank wallets proposed by the GoSL to facilitate online payments.
21. The proposed services/modules offered/interfaced to/with the public (eService interfaces) should be available in tri-languages (Sinhala, Tamil, and English).
22. An issue management system should be established for SL-UDI. An issue log shall be maintained by MSI for the errors and bugs identified in the Foundational ID platform as well as any changes implemented in the Foundational ID platform. The issue log shall be submitted to the GoSL monthly.
23. The MSI should understand the existing data volume and data complexity and provide a data migration strategy accordingly. Moreover, the data transformation strategy should follow the proper industry standards and proper control mechanisms in migrating these data to the new solution.
24. The Foundational ID platform should adhere to open standards and micro service architecture and industry standards.
25. The proposed Foundational ID platform should be browser independent and able to access with less configuration in the client workstation.
26. The MSI should carry out end-to-end security assessments prior to the Go Live of the Foundational ID platform launch and fix any issues found. Further, the GoSL / a GoSL nominated party will conduct security assessments periodically post implementation phase, and the MSI should fix any vulnerability issues identified during assessments.
27. The MSI should derive the UAT test cases in collaboration with the GoSL.
28. Obtain User Acceptance for the implemented the Foundational ID platform collaboratively with the committee appointed by the GoSL.
29. The MSI shall be responsible for ensuring information security including:
    a) Development of security processes and procedures
    b) Development, documentation, implementation, and maintenance of minimum baseline security

standards

c) Design, documentation, implementation, and maintenance of security design requirements.

d) Supply, Procurement, deployment, and commissioning as well as operations of all security tools and technologies.

30. The MSI shall provide necessary support and cooperation for the audit and close the findings of an audit.

31. The proposed Foundational ID platform should have a proper data backup plan and be equipped with a high availability and fault tolerance plan as per the project requirements.

32. The MSI should provide support and maintenance services from the date of Go-Live. Moreover, the MSI should adhere to the Service Level Agreement (SLA), during the support and maintenance (S&M) phase (**Refer Annexure 9 – Service Level)**.

33. The MSI should implement an SLA Management and Monitoring solution, configure the SLAs in the tool and enable automated monitoring and reporting of adherence to Service Levels. Manual intervention in computation of service levels should be avoided, and all monitoring and measurement should be automated. The MSI is expected to identify and implement RPOs and RTOs for backup and replication between DC and DR.

34. The MSI shall develop a proper alerting mechanism to monitor system performance issues, exceptions, and system downtimes. Moreover, the proposed alerting mechanism should send an alert via SMS to designated offices of the GoSL.

35. During the support and maintenance period, the MSI shall attend to any issue reported and carry out configuration changes (if required) and apply relevant security patches to ensure the security of the Foundational ID platform and apply updates and tuning of performance, etc.

36. The MSI shall accommodate change requests (CR) after obtaining approval from the Change Control Board and as per the CR rate agreed in the contract.

37. Any emergency changes to any component of the system shall be carried out through the approved Change Control Management process by the GoSL. The MSI shall always follow standard industry processes.

38. The MSI shall provide proper application training and knowledge transfer for all designated offices of the GoSL regarding technical aspects.

39. The MSI shall provide a training plan, considering different users, different functionalities, and the number of days, training approach, required language, etc.

40. The MSI is responsible for imparting the identified training in accordance with the training plan. The MSI shall also be responsible for the preparation of training materials, certificates, training aids (document, audio, or video). The GoSL shall arrange the venue and meals. During the training, the MSI needs to provide copies of the relevant training material.

41. The MSI has to ensure that the training sessions held are effective and that the attendees will be able to carry on with their work efficiently. For this purpose, it is necessary that the effectiveness of training sessions is measured. The MSI shall prepare a feedback form that will capture necessary parameters on measuring effectiveness of the training sessions. This form will be discussed and finalized with the GoSL.

42. The MSI should provide both soft and hard copies of user manuals (e.g., Printed documents). All manuals should be in tri-languages (Sinhala, Tamil, and English).

43. Adhering to the project management practices (**Refer Annexure *7:Project Management and Governance)***.
44. Participate in Project Review Committee meetings and Project management committee Meetings as a member and present the status of the project when necessary.
45. The MSI who gets engaged for the assignment should sign a Non-Disclosure Agreement (NDA) where applicable.
46. The MSI to adhere to the data protection act of 2022 in all components of SL-UDI.
47. The MSI to collaboratively work with the project stakeholders (i.e., GoSL's team, Project Management Consultant (PMC), MSP (Managed Service Provider), suppliers, departments, certification bodies, etc.) designated or proposed by the GoSL.
48. The MSI to work with the Project Management Consultant (PMC) of the SL-UDI project and accommodate the policies, procedures, recommendations, and the practices proposed.
49. The MSI to facilitate & provide technical guidance to set up the registration centers.
50. The MSI to suggest and make improvements for a smoother operation during the maintenance period including, not limited to, system administration, storage administration, database administration, backup/replication/restore/archival, monitoring of components, security management, event correlation, incident management, configuration management, management of license agreements and system manuals and documentation, etc. Further, the GoSL reserves the right to deploy its own team including the Managed Service Provider (MSP) for operations and maintenance alongside the MSI team after completion of 1st year of Operations.
51. The MSI to carry out a risk assessment in collaboration with the GoSL and PMC and take necessary precautions to manage the risk as instructed by the GoSL.
52. The MSI facilitates a smooth transition without disruption of operations to the GoSL designated team upon completing the maintenance period where the GoSL team is able to self-sufficient in managing the operations.
53. The following items (not limited to) should be reviewed, improved, and implemented by the MSI under the guidance of the Project Management Consultant (PMC) and the GoSL.
    a) Access Control Policy and Procedure
    b) Business Continuity Management Plan
    c) Development and Maintenance Policy and Procedure
    d) Incident Management Policy and Procedure
    e) Backup Management Policy and Procedure
    f) Security Policy and Procedure
    g) Risk Management Policy & Plan
54. The following items are out of scope for the MSI:
    a) Identity Card (NIC Card)
    b) Card personalization systems
    c) Card delivery/shipping

d) Enrolment Center Site / Citizen Services Centers (CSC) – (Except setting up and operationally supporting biometric capturing and other related devices procured from the MSI)

e) Costs associated with SMS alerts.

f) Local payment service provider fees (IPG)

g) Setting up the Contact Center

*** Refer "Services and Facilities provided by the Employer" – Section 10**

55. MSI shall use latest version of all the technology stacks wherever possible

56. The following items are part of the scope for the MSI:

Annexure 1A: As-Is Functional System

Annexure 1: Functional Overview

Annexure 2: Non-Functional Requirements

Annexure 3: Minimum Technical Specifications

Annexure 4: Software Engineering

Annexure 5: Demand Capacity

Annexure 6: Exit Management

Annexure 7: Project Management and Governance

~~Annexure 8: Biometric Device Certification~~ **(Not Required)**

Annexure 9: Service Levels

Annexure 10: Manpower Requirements

Annexure 11: Overview of Technology

Annexure 12: Project Sites and Sites

Annexure 13: Card Printing and Personalization Solution

Annexure 14: List of Indicative Trainings

Annexure 15: Transition Framework

Annexure 16: RACI Matrix

The scope of work of the MSI, spans the validation, upgrading, implementation and maintenance of the SL-UDI platform at the Primary Data Center, and Disaster Recovery sites.

S. No.	Scope	Sections	Brief Scope Description
1.	Overview of the Scope of Implementation	Not applicable	Implementation of SL-UDI Information System shall be undertaken and MSI will be responsible for undertaking various activities in each of phases including not limited to: • Demand and Capacity Planning (**Refer Annexure 5: Demand Capacity**) • Create a database schema of Register and Pre- Register • Commence the following services: o Pre-Enrolment o Enrolment o Authorization, Unique Identity Generation o Authentication and e-KYC services o Lifecycle Update Services o Ecosystem Partner Management etc. • Impact Assessment • Undertake activities for roll-out after completion.
2.	Software Solution	Section 5.1	**MOSIP Components / MOSIP Application (Section 5.1.2)** The application team of MSI shall take over and undertake knowledge transfer of MOSIP. MSI team shall also take over the necessary documentation (detailed features, functions, processes, and product specifications) from the MOSIP team. MSI shall re-assess the requirement of MOSIP components and suggest customization of the application as per the country requirements. MOSIP comprises of the following applications: • Pre-Enrolment • Enrolment Software Application • Identity Management System • Authentication Solution • Unique Number Generator • Partner and Device Management **Indicative COTS Components (Section 5.1.3)** MSI shall be responsible for procurement, integration and customization of following COTS applications: • Business Intelligence and Data Analytics • Customer Relationship Management • Document Management System • Identity and Access Management • Knowledge Management Solution • Learning Management Solution • Fraud Management Solution

S. No.	Scope	Sections	Brief Scope Description
			Support Applications (Section 5.1.4) MSI shall be responsible for application design, development, and implementation of following applications: • Citizen Portal • Mobile Application • TSP and UA Application (3 samples) **Biometric Solution (Section 5.1.5 Biometric Solution Implementation)** BSP shall be responsible for biometric solution customization, integration, and implementation of following applications: • Automated Biometric Identification System • Biometric SDK • Manual Adjudication **Integration of MOSIP with SL-UDI Information System (Section 5.1.7)** MSI shall be responsible for providing API gateway and its integration with MOSIP. MSI shall be required to integrate the MOSIP components. **Phased Implementation of Solution (Section 5.1.1)** Release_1 and Release_2 of implementation of Software System shall span across the following stages of software development lifecycle i.e., Requirements Gathering, Design, Development and Customization, Testing, Release and Continuous Build. **Software Lifecyle Management (Refer Annexure 4: Software Engineering)**

S. No.	Scope	Sections	Brief Scope Description
3.	Supply, installation, commissioning of hosting infrastructure	Section 5.2	The MSI is responsible for supply, installation and commissioning of the IT hardware, software systems and peripherals required for the Primary Data Center and Disaster Recovery for implementation. Accordingly, MSI shall prepare detailed design and solution architectures, among others server architecture, network architecture, virtualization architecture, container application platform architecture, database architecture, security architecture, deployment architecture migration & transition plan etc. MSI shall Design, Supply, Installation, Commission, and Acceptance, and perform the following services: • Server Services • Network Services • Storage Services • Backup and Replication Services • Virtual Environment Services • Container and OS environment services
4.	Field Infrastructure (Supply, installation, commissioning of Enrolment Kits)	Section 5.3	MSI shall perform the following activities: • Porting of enrolment software in the kits • Supply and Commission of Enrolment Kits at enrolment centers. • Creation of content and training of Master Trainers for Enrolment Software • Creation of content and training of Master Trainers for Authentication Solution • Operationalization of enrolment kits and extend support in GoSL provided network at Enrolment Centre for enrolment. • Spares and Maintenance of Enrolment Kits
5.	Enrolment Centers	Section 5.4	MSI is responsible for establishing, operating, and maintaining the enrolment kits.
6.	Identity Cards	Section 5.5	GoSL issues the identity cards at its own cost i.e., card procurement, card personalization, and card issuance.
7.	Training and Capacity Building	Section 5.6	During implementation and operation of SL-UDI Information System, MSI shall be required to train key resources to ensure successful implementation and operations of SL-UDI Information System. The MSI is responsible for the following: • Training Need Assessment • Preparation of Training Plan • Imparting Training (including preparation of training content)

S. No.	Scope	Sections	Brief Scope Description
			• Ensuring Training Effectiveness • Managing Continuous Learning
8.	Performance Testing, Acceptance and Go-Live	Section 5.7	• Undertake performance testing exercise before Go- live. • Validate the Application and Infrastructure performance testing and undertake enhancement/augmentation, if required • Performance testing should be done in both the Primary Data Center and Disaster Recovery Data Centre.
9.	Information Security and Business Continuity	Section 5.8	**Information Security (Section 5.8.1)** MSI shall be responsible to ensure information security including: • Development of security processes and procedures • Development, documentation, implementation, and maintenance of minimum baseline security standards • Design, documentation, implementation, and maintenance of security design requirements. • Procurement, deployment as well as daily operations of all security tools and technologies • Documenting, implementing, as well as obtaining certifications. • Provisioning of security controls (enrolment, authentication, and overall security aspects) **Business Continuity (Section 5.8.3)** The MSI is required to conduct the end-to-end Business Continuity and Disaster Recovery Planning and carry out the related BCP operations.
10.	Support (Contact Center and IT Helpdesk)	Section 5.8	**Contact Center (Section 5.8.5.1)** The MSI is responsible for: • Provisioning and integration of CRM solution • Reporting and Monitoring **IT Helpdesk (Section 5.8.6)** The MSI is responsible for setup, operations, and administration of IT helpdesk. As part of contact center MSI is responsible for: • Helpdesk setup and operations • Training to helpdesk manpower • Deployment of IT and Non-IT Infrastructure • Reporting and Monitoring • Conducting IT helpdesk operators

S. No.	Scope	Sections	Brief Scope Description
11.	Security and Network Operations	Section 5.9	**Security Operations Center (Section 5.9.1)** The MSI is responsible to SOC Setup, SOC Integration and running the SOC services. **Network Operations Center (Section 5.9.1)** The MSI is responsible to NOC Setup, NOC Integration and running the NOC services
12.	Business and Technical Services	Section 5.10	**Business Services (Section 5.10.1)** • Authentication Services (Partner Onboarding and Device Management) • Ecosystem Partner Management • Authentication Services Management • Manual Adjudication Services **Technical Services (Section 5.10.3)** • IT Asset Management • Field Network Assessment • IP Address Management • ATS and AMC management • Software Management • SMS Services Integration • Biometric Solution Management
13.	Operations and Maintenance	Section 5.11	**Support & Maintenance Services (Section 5.11.1)** The MSI is required to provide the support & maintenance services for the hardware, software, network, security, field infrastructure, and other components. **Operations, Maintenance and Administration (Section 5.11.3)** The MSI is required to do the following: • Management of Primary Data Center and Disaster Recovery site • Server and Virtual Services Operations • System Maintenance and Management • DC/DR/SOC/NOC/IT Helpdesk Network Connectivity Management and Operations • System Administration • Storage Administration • Database Administration • Backup / Replication / Restore / Archival

S. No.	Scope	Sections	Brief Scope Description
			• Network Monitoring • Security Management • Event Correlation • Incident Management • Configuration Management • Patch Management • Change request Implementation Management of license agreements and system manuals and documentation. **Note:** GoSL reserves the right to deploy its team for the operations and maintenance period with the team of System Integrator. **Software Systems** **(Section 5.11.4)** The MSI will be responsible for maintenance and management of the Software System. Key activities to be performed by the MSI shall include: • Annual Technical Support • Application Software Support • MOSIP Support • Issue Identification and Resolution • Change and Version Control • Release Management • Maintain System Documentation • Patch Management **Field Infrastructure** **(Section 5.3)** The MSI is required to do the following: • Issue Identification and Resolution • Repair services through service center. • Spares for timely resolution of issues • Software Updates

14.	Exit Management	**Annexure 6**	**Exit Management**
			• MSI shall be responsible for carryout end-to-end transition activities, including SL-UDI implementation and operations to the MSP.
			• MSI shall be responsible for, but not limited to, the following activities:
			  • Preparation and execution of the transition management plan, in cooperation with GoSL
			  • Transfer of Deliverables and Documents
			  • Transfer of Agreement and Licenses
			  • Knowledge Transfer
			
			Exit Management

S. No.	Scope	Sections	Brief Scope Description
			MSI shall be responsible for, but not limited to, the following activities: • Preparation of exit management plan • Transfer of Deliverables and Documents • Transfer of Agreement and Licenses • Knowledge Transfer • Sub-contractor(s) Transition Management

Table 5: Scope of Work of the MSI

5.1 Software Solutions

(i) MSI shall be responsible for implementation and maintenance of the SL-UDI Software System's support applications.

(ii) The MSI will follow the offshore development model wherein a dedicated core team shall be stationed at the GoSL's premises while the development shall happen in an offshore location.

(iii) Provision of the offshore application development and testing environment along with all the necessary tools, artifacts, sub-systems required for development, testing and maintenance of the SL-UDI software system would be the responsibility of MSI. In case MSI has not considered any component/service which is necessary for implementation of the SL-UDI Software System, the same shall be brought by the MSI at no additional cost to the GoSL.

(iv) Implementation of SL-UDI software system is envisaged to be undertaken in the following manner:

- Application development as Release_1 of the SL-UDI Software System.
- Application development as Release_2 of the SL-UDI Software System.
- Maintenance and management of the SL-UDI Software System (refer to section 5.11.4 for detailed scope for this phase).

5.1.1 Phase-wise Implementation of SL-UDI Software System

(i) The scope of work for the MSI spans the complete Software Development Life Cycle from designing, developing, testing, maintaining, and supporting the SL-UDI Software System. MSI shall work closely with GoSL during the software implementation, maintenance, and enhancement phase to ensure successful implementation and operations of the SL-UDI Software System. Implementation of SL-UDI Software System is envisaged to be rolled out in the following two versions:

Release_1(MVP): An integrated and fully tested initial release of SL-UDI software system called 'Release_1' is planned to be released in T+12 months (where T = month of signing of MSI contract) for commencement of enrolment locations established island-wide and other operational areas specified in project sites/sites (**Refer Annexure 12: Project-Sites-and-Sites**). Release_1 of the SL-UDI Software System is proposed to primarily consist of the Pre-enrolment Software, Enrolment Software, Identity Management System (IDMS), ABIS, Identity Services (Authentication and KYC) and a few support applications such as CRM, SL-UDI Portal, Partner and Device Management, Document management System etc. as given in the table below.

Release_2: Subsequent version of the SL-UDI Software System i.e., 'Release_2' is planned in T+15 months. Release_2 shall consist of 'Release_1' applications and the rest of the support applications such as Fraud Management, Business intelligence and analytics, etc.

(ii) The SL-UDI Information System should be designed for scalability and should be able to handle a capacity given in Section 5.8.

(iii) The table below provides a break-up of applications which shall be a part of Release_1 and Release_2 of the SL-UDI Software System.

Implementation of SL-UDI Software System	
Release_1 (T + 12 Months) (MVP)	**Release_2 (T + 15 Months)**
MOSIP Applications** • Pre-Enrolment Application • Enrolment Software • Identity Management System (IDMS) • Authentication Solution Unique Identity Generator • Partner and Device Management • Biometric Software Development Kit (SDK) • Automated Biometric Identification System (ABIS) • Manual Adjudication	• SL-UDI Portal • Business Intelligence and Data Analytics • SL-UDI Mobile Application • Knowledge Management System • Service Billing System
Support Applications and Other Applications • SL-UDI Portal (basic aspects for pre-enrolment and enrolment) • Business Intelligence and Data Analytics (basic reporting) • Customer Relationship Management (CRM) • Document Management System • Identity and Access Management • Sample TSP and UA Software (3 samples) • Project Management Tool	

Table 6: Implementation of SL-UDI Software System

** Where T is the date of signing of contract with the MSI*

** The applications are available on https://github.com/mosip and the documentation is available on docs.mosip.io and training on MOSIP is available on https://academy.mosip.io/

**** A key component of the SL-UDI information system is the multi-modal ABIS solution. The MSI will be responsible for integration of ABIS solution with rest of SL-UDI Information System. MSI shall work closely with the biometric solution provider to undertake the integration.*

Note: The above timelines include the time till user acceptance testing.

5.1.2 MOSIP Application

(i) MOSIP comprises of various components which are planned to be utilized:

- Pre-Registration (Pre-enrolment Application)
- Registration (Enrolment Client Software)
- Registration Processor (Identity Management System and Unique Identity Generator)
- ID Authentication and ID Repository (Authentication Solution)
- Partner Management (Partner and Device Management)
- Administration
- Kernel
- Resident Services

(ii) MOSIP team will invest about 4 to 6 weeks, approximately, on training the MSI. The training would be on the following topics roughly:

- Deployment
- Configuration
- Customization
- Integration (Device integration, application integration, use case integration)
- Troubleshooting
- Administration and Monitoring
- Security, Privacy and Auditing
- Best Practices

(iii) The functional architecture of MOSIP is available on their website.

(iv) The MSI shall be responsible for using the MOSIP application suite from IIIT Bangalore, India. The adaptation shall happen through IIIT Bangalore, India for a required period through online medium.

a. Define a detailed adaptation plan including scope of the transition, day wise activity schedule etc. in coordination with IIIT Bangalore, India.

b. Execute the adaptation plan including, but not limited to, the following activities:

- Study the existing architecture and design.
- Obtain Detailed knowledge transfer of the source code and its documentation.
- Obtain the necessary documentation.

c. The MSI shall also identify and document potential risks along with their mitigation strategies. MSI should present the risks to the GoSL as part of the review meetings.

d. After taking a knowledge transfer of the MOSIP application suite and its documentation from IIIT Bangalore, India, MSI will undergo reverse transition where the MSI shall take lead in providing a knowledge transfer of the MOSIP applications.

(v) The MSI needs to capture the customizations requirements (w.r.t. the employer specific requirements) as part of the requirement gathering. After takeover, MSI shall be responsible for customization of the MOSIP application as per the SL-UDI Information System requirements gathered by the MSI. The cost of this customization needs to be included by the MSI in its

commercial proposal and there will not be any additional payment from GoSL on the account of MOSIP customization related to country requirements.

(vi) The authentication solution should provide virtual identities, tokens, etc.

(vii) MSI has to provide support related to MOSIP as per Section 5.11.4.3.

5.1.3 COTS Application

The COTS components of the SL-UDI Information System comprise of the following applications:

5.1.3.1 Business Intelligence and Analytics

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

(ii) The MSI's scope of work includes procuring, commissioning, configuration, implementation, integration, deployment, and maintenance of Data Analytics and Business Intelligence Solution for SL-UDI Information System. The MSI shall enable the system to provide comprehensive monitoring of enrolment and authentication through Business Intelligence (Dashboards and reports) and Analytics.

(iii) The MSI shall carry out a detailed requirement phase upon award of the contract to review the data analytics requirements for the Data Analytics module.

(iv) The MSI shall produce a detailed functional specifications and design specifications, including detailing the data analytics module to be developed, system architecture design, design principles/considerations, etc.

(v) Regarding BI and Data Analytics system, the MSI shall also perform the following among others,

- Propose, design, and implement an integrated BI and Data Analytics system.
- Quality assurance test for BI and Data Analytics system
- Provide documentation for BI and Data Analytics system.
- Perform integration with internal SL-UDI data sources for BI and Data Analytics system.
- Master Data Management for all applications

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

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

(viii) The MSI should propose tools that allow customizable reports. The generation of the report shall not impair the System performance.

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

(x) The Data Analytics system should allow GoSL to customize notification of certain indicator that GoSL is interested in 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 limited users (5) to put in parameters to view the data from different perspectives.

(xi) MSI has to prepare detailed requirements around reports and also study SL-UDI KPIs to define required reports, analytics capability to meet the SL-UDI Information System's needs.

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

(xiii) The proposed solution should meet the minimum technical specifications (**Refer Annexure 3: Minimum Technical Specification**) given in the RFP. The MSI will be required to gather detailed features, functionalities and requirements during the requirement gathering stage.

5.1.3.2 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 CRM solution should cover the entire SL-UDI stakeholders, such as Citizens, CSC, Partner Management, TSPs, User Agencies etc. which includes integrations and other components.

The MSI's scope of work includes:

1. Procuring, commissioning, configuration, implementation, integration, deployment, and maintenance of Customer Relationship Management (CRM) Solution. The CRM solution should be used to log all incidents and queries in the system for generating id and track the logged query.
2. 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.
3. 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.
4. The MSI shall be responsible for integrating the CRM with the technical Help Desk.
5. MSI shall analyze the requirements of IT infrastructure for hosting CRM software to meet the availability, performance and response times required to meet the Contact Center service levels.
6. MSI shall generate and provide CRM Reports on a daily, weekly, monthly, quarterly, and yearly basis.
7. MSI shall also be responsible for the analysis of the CRM reports to continuously identify improvements in the CRM operations.

8. GoSL shall provide the MSI with a toll-free number(s) for contact center.
9. The license of the proposed / deployed Solution should be at an enterprise level on a perpetual basis in name of GoSL including ATS post for entire project duration.
10. The CRM solution should support at least Sinhala, Tamil, and English Languages.
11. 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.
12. 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 decided by GoSL from time to time.
13. 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.
14. The CRM solution shall maintain a history regarding complaints/grievances.
15. The CRM solution shall support IVR, Voice, Email, and Web based complaint lodging, resolution, and response features using channels such as SMS, Email, and Web.
16. 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.
17. The CRM system should provide extensive analytics and reporting capability on important KPIs concerning all types of users.
18. The solution should support call routing functionalities.
19. Real-time decision support (analytics) to understand customer intentions and customize services and interactions accordingly.
20. The CRM system shall be integrated with the SL-UDI Information System through suitable APIs. Except KMS and DMS.
21. 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.

5.1.3.3 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. The key features of the application are provided below:

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

5.1.3.4 Identity and Access Management

The function of the Identity and Access management would be to provide single sign on capability

for applications including COTS, Infrastructure 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 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. Administrators can be allowed access on the basis of multi-factor authentication devices.

The proposed features 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.

5.1.4 Support Application

The important support application components are:

(i) SL-UDI Citizen Portal

(ii) SL-UDI Mobile Application

(iii) TSP and UA Software, maximum of three samples

(iv) Fraud Management System

(v) Knowledge Management System

(vi) Learning Management System

The MSI will be required to gather detailed features, functionalities and requirements during the requirement gathering stage. However, the MSI's scope of work related to SL-UDI Citizen Portal, SL-UDI Mobile application and TSP and UA software is given below:

5.1.4.1 SL-UDI Citizen Portal

A citizen portal shall be implemented as part of SL-UDI Information System. The SL-UDI Citizen 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, management of SL-UDI life cycle, etc. The contact center will be able to use applications such as CRM.

MSI shall be responsible for the following:

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

(ii) Development of the SL-UDI Citizen 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 and train the GoSL 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) The MSI is expected to position appropriate qualified and trained manpower to manage the portals.

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

5.1.4.2 SL-UDI 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.

MSI should conduct detail requirement gathering to design and develop the mobile application, 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 platforms such as Android and iOS.

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

(xi) Should provide Role Based Access control.

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

(xiii) The application should be compatible with future OS updates during the contract period time.

5.1.4.3 TSP and UA Applications

(i) A federated model of identity ecosystem will be built with two tiers. In the first tier, the Trusted Service Providers (TSP) will be able to access the SL-UDI solution. In the second tier, the User Agencies (UA) will send the identification service requests to SL-UDI solution through TSP.

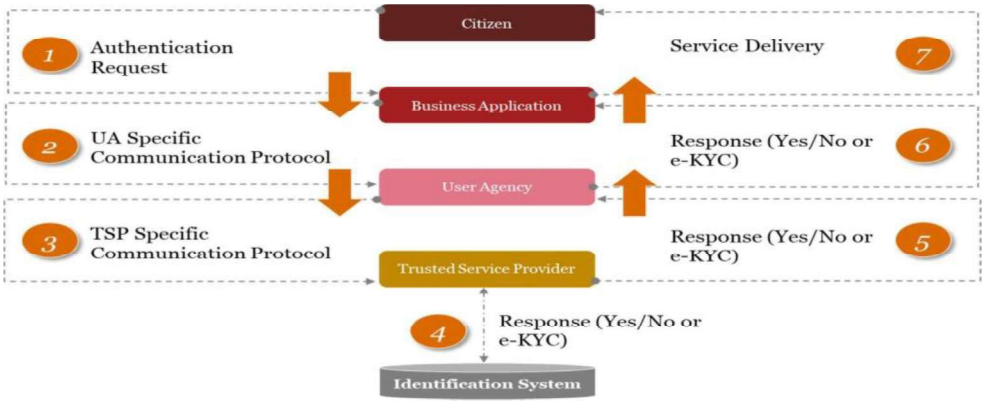

Figure 2: TSP and UA Applications

(ii) For TSP, there will be a software application which will process the request received from UA and send it to SL-UDI Information System and will also process the response received from SL-UDI Information System and send it to UA. As part of handling requests, the TSP application will log requests, validate request, append wrapper information in request and sign request, and forward the request to SL-UDI Information System. As part of handling response, the TSP application will log response, validate response, and forward the response to concerned UA.

(iii) For UA, there will be a software application which will process the request received from user applications and send it to TSP and will also process the response received from TSP and send it to the concerned user application.

5.1.4.4 Knowledge Management System

The KMS delivery scope should include among others the following.

(i) MSI shall be responsible for designing, developing / deploying COTS and maintaining the Knowledge Management System.

(ii) The Knowledge Management System would be integrated with the SL-UDI portal and Document Management System.

(iii) The Knowledge Management System must be designed in a flexible manner so that additional categorization fields can be added in future, as and when required. Also, the system should be able to handle knowledge of any form, including different subjects, structures, and media.

(iv) All capabilities should be available on a web application accessible on mobile smartphones as well as desktops/laptops.

(v) The Knowledge Management System should capture meta data when adding a document such as keywords, date, title, description, target audience, date of issue, date of expiry etc.

(vi) MSI shall be responsible for uploading all the training material prepared for trainings in KMS.

(vii) MSI shall be required to prepare a comprehensive frequently asked questions (FAQs) and

upload them on the KMS.

5.1.4.5 Service Billing System

The Service Billing System (SBS) is designed to allow various stakeholders and citizens 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 designing, developing and maintaining the SBS. The MSI can choose to utilize 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, Citizen 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.

5.1.4.6 Single Sign On (SSO) Module

The GoSL wishes to utilize the unique identity allocated to citizens to be used for the purpose of SSO within the SL-UDI modules as well as in the private and public sector services. For this purpose, the MSI needs to develop, operate, maintain, and support the SSO modules which works on open authentication protocol (AUTH 2.0). The SSO module should provide multi- factor authentication.

The MSI will be required to prepare the developer content, API specifications, FAQs, etc. and publish them on SL-UDI's developer portal upon approval from GoSL. For the period of the contract, MSI will also be expected to extend technical support to government departments who want to integrate with this module. The scope will not include performing software development/customization in the software of such government departments.

5.1.5 Biometric Solution Implementation

The BSP shall supply, customize, and implement the biometric solution in accordance with the approved requirement specifications, design specifications, and according to the project plan and carry out the unit testing of the software in accordance with the approved test plans. The overall solution should be implemented in the data centers mentioned in **Annexure 12:Project Sites and Sites**. The illustrative deliverables for this activity are mentioned below:

(i) Customization of biometric solution including ABIS, Biometric Middleware, Manual Adjudication, SDK, etc.

(ii) Delivery of software along with operational / technical manuals, library files, setup programs etc.

(iii) Unit and Integration testing of the software along with test summary report and bug report

(iv) Necessary modifications to meet the requirements and bug closure report.

(v) BSP shall supply perpetual server licenses and desktop licenses for multi-modal SDK. The SDK licensing should be:

a) Unrestricted, unlimited right to uses, but not machine specific licenses and the right to deploy the solution anytime anywhere.

b) Enrolment SDK licenses must not use hardware license key or keyed to ID (such as CPU, serial number, Ethernet ID)

c) Usable enrolment kits required to perform specified enrolment over the contract period.

d) Authentication servers are required to support peak authentication requests at the specified response time level.

e) Adjudication stations are required to support False Positive Identification Rate (FPIR) for the enrolment rate mentioned above.

f) System monitoring and analysis servers for ABIS configuration to support specified gallery size over the contract period.

g) Matching accuracy rates must meet the Fales Match Rate (FMR) and False nonmatch rate (FNMR) rates required for authentication on operational data.

5.1.5.1 Setup of Biometric Solution

Once MSI has commissioned the infrastructure, it will be responsible for installation and configuration of necessary software to operate the biometric solution. In addition to the biometric solution, the necessary software which have to be provided by the MSI, are operating system, systems software (e.g., virtualization), database, application server software, etc. The MSI should tune parameters for optimal performance of the OS and should configure to harden the OS for prevention against malicious and unwarranted attacks.

On its infrastructure, the MSI should install all necessary software and biometric solution supplied by BSP. In addition to installing and tuning its own software, the BSP will also be responsible for installation and configuration of other software (Anti-virus, enterprise management system, etc.) provided by the MSI. The overall responsibility shall lie with the MSI.

In addition to installing and tuning its own software, the BSP will also be support for installation and configuration of other software being provided by the MSI. The indicative list of such software includes:

a) Enterprise Management System (EMS) Agent

b) Security Information and Event Management (SIEM) Agent

c) Anti-Virus

d) Data Lead Prevention (DLP)

e) Database Activity Monitoring, on database servers

The BSP is required to setup the biometric solution to meet requirements of two phases as given below.

5.1.5.2 Rollout of Biometric Solution

(i) The Biometric solution shall be required to meet the requirement of enrolment of residents. The biometric solution shall at minimum provide:

a. Integration of ABIS component with SL-UDI Application at Server Side

b. Integration of Multimodal SDK with Enrolment Software application. The Multimodal SDK (client-side component) shall be used for biometric capture aspects such as quality, etc.

c. Configuration of business rules and application-level policies related to de-duplication and verification in consultation with GoSL.

d. Perform de-duplication checks (1: N) for enrolment for a gallery size provided in the RFP.

e. Integration of Multimodal SDK libraries with application modules related to authentication. The Multimodal SDK (server-side component) shall be used for biometric authentication (1:1)

(ii) The BSP shall roll out the solution after testing. The BSP shall be responsible for application availability while in production and shall deploy the solution at both Primary and Disaster Recovery sites and adhere to BCP plan.

(iii) With a view on accuracy, throughput, and optimal resource utilization, the BSP shall undertake continuous performance monitoring and improvement.

(iv) Configuration of ABIS solution's own internal persistence/database component with adequate back-up and recovery in compliance with BCP plan and data backup and recovery strategy

(v) Integration of ABIS component with SL-UDI application at server side

(vi) Assist MSI to undertake integration of multimodal SDK with enrolment software, authentication solution, adjudication, and monitoring module.

(vii) Provide training to MSI to undertaken integration of the ABIS and Multimodal SDK with SL-UDI application.

(viii) Submit documentation of key configuration settings, business rules and policies adopted along with key design and solution features along with user manuals to GoSL for their review and acceptance.

(ix) Configure the solution to comply with the SL-UDI policies and other business rules and application-level policies as stated and finalized by GoSL.

5.1.5.3 Integration Service

MSI, themselves or with their BSP, shall be jointly responsible to integrate its solution with that of remaining SL-UDI solution. The major points of integration are as follows:

- Biometric SDK Integration with enrolment software (MSI to integrate, BSP to support)
- Biometric SDK integration with IDMS (MSI to integrate, BSP to support)
- Biometric SDK integration with Authentication Solution (MSI to integrate, BSP to support)
- Integration of the manual adjudication with IDMS (BSP to integrate, MSI to support)
- Integration of ABIS and biometric middleware with IDMS (BSP to integrate, MSI to support)
- The integration of biometric solution with other components of SL-UDI solution as required (BSP and MSI to integrate together)

MOSIP is working on micro-services architecture where integration with components is performed using RESTful APIs. For integration of IDMS with Biometric Middleware, ABIS and Manual Adjudication, MOSIP will provide request and response API specifications. The BSP will have to utilize the given specifications and integrate with IDMS. The MSI will extend necessary support to the BSP in this regard. (**Annexure 11: Overview of Technology**)

5.1.6 Solution Testing

The unit testing will be carried out by the MSI/BSP as part of biometric solution customization activity. In the current stage, the MSI/BSP shall carry out the integration planning and testing, system test, performance testing and security testing.

S. No.	Testing	Description
1.	**Integration Test Planning & Testing (Off Site)**	For integration and its testing, MSI shall identify the critical modules, their priorities, and interfaces. The MSI will be responsible for overall integration and comprehensive testing of all interfaces at server side as well as client-side applications. The scope of integration test will include testing of the integration of the proposed solution components (Server Side ABIS, Server-Side Adjudication, Server-Side SDK and Client Slide SDK) with respective APIs provided by SL-UDI. The actual integration shall be done as per integration plan. The integration will be followed by the integration testing in which log all defects will be maintained and BSP shall ensure these defects are rectified and re-tested. For conducting the integration test, MSI shall develop suitable test cases and include these in integration test plan and submit the same for review to GoSL. The MSI shall maintain the integration test plan along with test results and defect statistics and provide the same to GoSL, if desired so.
2.	**System Test Planning & Testing (Off Site)**	On successful completion of the Integration testing, MSI shall carry out the actual system testing as per the system test plan. The inputs for this phase consist of the software requirement specification document (SRS) and the initial system test plans whereas the outputs consist of system test plan and test results. For system plan and its testing, MSI shall identify the features which will be tested and other features which will not be tested. MSI shall plan out a series of different tests, each test having a different purpose, to verify that all system elements have been properly integrated, and that the system performs all its functions and satisfies all its non-functional requirements. MSI shall ensure that system testing is carried out by an independent team other than the development team. MSI shall setup a separate test environment with test database to carry out system testing. MSI shall maintain the system test plan and test results with defect statistics and provide the same to GoSL on request.

S. No.	Testing	Description
3.	**Security Testing (including Penetration and Vulnerability testing)**	The solution should demonstrate compliance with security requirements as mentioned in the contract including but not limited to security controls in the application, infrastructure and network layers deployed by the MSI. The solution shall have to pass vulnerability and penetration testing for rollout of each phase. The solution should pass web application security testing for the portal and security configuration review of the baseline infrastructure. The MSI should carry out security and vulnerability testing on the developed biometric solution in the exact same environment/architecture as the one set up for production. The security test reports, and test cases should be shared with GoSL. The GoSL may also involve third party auditors to perform the audit/review/monitoring of the security testing carried out by the MSI. During the O&M phase, vulnerability assessment and penetration testing will need to be conducted on a quarterly basis.
4.	**User Acceptance Testing**	The objective of this testing is to determine whether the solution meets the GoSL's requirements. It is mandatory for MSI to incorporate / consider test cases as part of UAT test cases for those customized and/or extensions and/or configured functionalities identified from traceability matrix. The MSI would make the necessary changes to the solution to ensure that it successfully passes through UAT. Test Plans for UAT would be prepared by the MSI with the approval of the GoSL. The MSI will plan all aspects of UAT (including the preparation of test data and test environment) and obtain required assistance to ensure its success. The test cases prepared by MSI shall be approved and used by GoSL for the purpose of testing. GoSL will nominate representatives from different user groups based on inputs from the MSI and would facilitate UAT. The primary responsibility for acceptance testing lies with the user group and GoSL shall coordinate with MSI to ensure necessary support is available to the user group. The user group shall document the test cases / scenarios to ensure that the defined acceptance criteria are validated during the testing. The MSI shall provide support to document the test results along with defects statistics. MSI shall ensure that defects found are corrected and retested by the end user group. The testing shall be done in iterations till the specified requirements are met. At the decision of GoSL, the result of testing may be audited by a third party. On successful completion of User Testing, MSI shall obtain a formal sign- off from GoSL for the solution UAT.

S. No.	Testing	Description
		The MSI shall be required to demonstrate all the features / functionalities as mentioned in the UAT Test Case Scenarios. The prerequisite for carrying out UAT activity shall be: • Submission of a detailed test plan by MSI and approval of this plan by GoSL • All documentation related to solution and relevant acceptance test documents should be completed & submitted before the final acceptance test to GoSL. **Note:** The UAT needs to incorporate and simulate the security arrangements that has been proposed to ensure that no unauthorized access is given. The illustrative deliverables for this activity are mentioned below. • User Acceptance Test Plan • Testing Reports • Necessary modification in software for passing the UAT This testing will be carried out on datasets of 50,000 anonymized Biometric data of citizen or Biometric dummy data. The responsibility of supplying the biometric data or creating dummy data shall lie with GoSL. The MSI shall develop the test plan, test cases, and test data for the purpose of the acceptance testing. The confidential details that may affect the sanctity of this testing will not be disclosed prior to the conduct of testing. The MSI will be responsible to prepare test suite (scripts), creation of test environment, integration of test suite with SDK/ABIS, logging mechanisms for passive tests, etc. This test will be conducted in two parts i.e. (i) one-time testing with only ABIS and (ii) end-to-end testing with middleware, ABIS and other components. The details of this testing will be shared with the GoSL at the start of this phase of testing. For the purpose of this test, GoSL shall form the Acceptance Test Governing Committee as well as the Test Teams (Test Data Team, Test Suit Team and Test Team). The GoSL may decide to co-opt the members from MSI for any of the team(s). The indicative responsibilities of each team are as follows: • *Test Suite Team:* to understand the requirements and create, integrate, and do functionality tests of a test suite that will drive the testing. • *Test Data Team:* For data preparation and should be independent of the BSP. • *Test Team* to physically carry out the testing and create logs of the probes and the results for analysis.

S. No.	Testing	Description
		The MSI will have to clear all the test cases for both ABIS and SDK to be considered as successful in the UAT. If the solution fails in any of the test cases in either of the modules (ABIS or SDK), the corresponding module will have to be subjected to a re-test. All retests will contain new test data that was not used in the previous tests. In this event, the solution will have to undergo a complete test of the failed module, and not the particular test cases that it failed. A complete retest of the module is recommended to ensure that the modification of the module to rectify the observed problem has not impacted any of the other functionalities.
5.	**Biometric Quality improvement testing**	Biometric solution (ABIS/ Biometric SDK) should be optimized to cater to the requirement identified. Further finetuning of the biometric solutions should be done to improve accuracy, efficiency and effectiveness. This should be carried out after defined number of records are available and consultation with GoSL as agreed timeframe based on the implementation plan.

Table 7: Solution Testing

5.1.7 Integration of MOSIP Applications with SL-UDI Information System

5.1.7.1 Overview

The MSI should use the MOSIP application and integrate the same with the support applications. The major components that would need to be integrated by the MSI are listed below:

(i) MOSIP Application

a. FTP and Pre-SEDA Queues

b. Pre-Enrolment Application

c. Enrolment Software

d. Identity Management System

e. PIN Generator

f. Authentication

g. Partner and Device management

(ii) ABIS, Manual Adjudication, and Biometric SDK

(iii) Support Applications

a. BI & Analytics

b. Customer Relationship Management (CRM)

c. Document Management System (DMS)

d. Knowledge Management System (KMS)

e. SL-UDI Portals and Mobile Applications

f. Identity & Access Management

(iv) Security solutions

(v) Other components of the solution as necessary.

5.1.7.2 Integration Details

The SL-UDI Information System has various components which require integration with one another to provide the desired functionalities. The major integration points between different components among others are mentioned below:

(i) Integration of Pre-SEDA

a. Deployment of PRE-SEDA components such as FTP Server, Pre-SEDA Managed Queues.

b. Integration of Pre-SEDA components with enrolment client using FTP approach.

c. Integration of Pre-SEDA managed Queue with IDMS.

d. Deployment of Integration of Pre-SEDA managed queue with FTP server using a Scheduler approach.

(ii) Integration of IDMS with other components

MOSIP would consist of an API based software product. It would have multiple modules/components. Following would be the deployment scope for MOSIP

a. Deployment of Identification Database Management System (IDMS), SEDA components ~~on~~ in Development, Test, Production, and any other environments.

b. Deployment of IDMS application components on the Application Server Grid such as validation, Demo Deduplication component, Biometric Deduplication Component, PIN generator component, etc. as per requirements and support of MOSIP support.

c. Setup and configuration of databases in IDMS as per the guidelines given by MOSIP.

d. Integration of IDMS SEDA with pre-SEDA Queue using API approach.

e. Integration of IDMS SEDA with ABIS using API approach. APIs would be made available by BSP for integration. These APIs would need to be invoked by the IDMS SEDA workflow and would need to be customized by the MSI for integration purposes.

f. Integration of IDMS system with Partner and Device Management System for purpose of validation of Enrolment Officers (EO), CSC, etc.

(iii) Integration of ABIS

a. Deployment of biometric solution consisting of ABIS, Manual Adjudication Component, Biometric Middleware.

b. Integration of IDMS with Manual Adjudication Module of ABIS.

c. Integration of IDMS with ABIS.

d. Integration of IDMS with Biometric Middleware.

e. Integration of SDK with Enrolment Software.

f. Integration of SDK with Authentication Solution.

g. Integration of SDK with IDMS.

h. Customize the IDMS to invoke the relevant APIs to submit Biometric Deduplication Requests and receive the results.

i. ABIS would need to be integrated with IDMS APIs to retrieve archived packets for manual adjudication, etc. This integration with Manual Adjudication Module would need to be done by the BSP with help of MSI.

(iv) Integration of Authentication Solution with other components

a. Deployment of SDKs on the SDK Authentication Server

b. Integration with Biometric SDK Server, HSM, PIN Master

c. Integration of the extraction Message Queue with IDMS as per requirements and specifications of MOSIP.

d. Setup /Configuration of Citizen data store & Integration of workflow with Citizen Data Store.

e. Setup and Integration of Data Cache with Citizen Data Store and Partner Portal Application.

f. Deployment and Integration of Authentication and KYC workflows.

g. Deployment and integration of proxy services from multiple providers such as OTP Server, Authentication Server, SDK Server, HSM, Citizen Data Store, KYC Server, SMS Server, Fraud Server, BI Server.

h. Deployment of APIs on API Gateway and integration with OTP server, Middleware and SMS gateway.

i. SMS gateway

(v) Integration of MOSIP Pre-enrolment Application with other components

a. Integration of MOSIP Pre-Enrolment Application with Enrolment Software using API approach.

b. Integration of Pre-Enrolment Application

c. Integration of Pre-Enrolment Application with API Gateway.

d. Integration of Citizen Portal

(vi) Integration of Support Applications

a. Integration of Partner and Device Management System with SL-UDI Web Portal, SL- UDI Mobile Application and IDAM.

b. Integration of CRM system with SL-UDI Web Portal, SL-UDI Mobile Application and IDAM.

c. Integration of KMS with SL-UDI Web Portal, SL-UDI Mobile Application and IDAM.

d. Integration of BI With SL-UDI Web Portal, SL-UDI Mobile Application and IDAM.

(vii) Existing GoSL Applications such as:

a. ICAO Photo Capturing – Photo Storing Server

b. Card personalization System (track master)

5.2 Hosting Infrastructure

5.2.1 Data Center Site Set-up

5.2.1.1 Data Center Strategy of Project

GoSL has decided to utilize a two-way setup containing DC and DR sites. The DC and DR sites will be in 1:1 configuration i.e., exact replica of each other. For the entire duration, a mechanism for storage and safe keeping of backup tapes, a remote site will be utilized.

GoSL shall utilize its data center for hosting IT Infrastructure in Primary Data Center and Disaster Recovery. The Primary Data Center and Disaster Recovery sites will be in two separate data centers. MSI shall undertake assessment of the data centers, prepare a site plan and rack plan.

The MSI would use connectivity (provided by GoSL) for data replication between the two sites, if required. The MSI shall undertake a capacity assessment and inform GoSL to undertake capacity augmentation to meet the required requirement and performance levels mentioned in the RFP.

5.2.1.2 Site Set-up

GoSL shall provide the physical space for hosting IT Infrastructure in Data Center and Disaster Recovery Center. Upon availability of space for each of the Data Center sites, the MSI shall set-up the site for hosting of SL-UDI Information System. The MSI, in consultation with GoSL for setting up of site, shall:

(i) Undertake a site survey to highlight the positioning of racks, power and backup systems and chart the appropriate and necessary changes, if any.

(ii) Prepare a site survey report capturing desired changes and submit it as a part of the bid.

(iii) Prepare a detailed plan for site set-up and submit with the bid document. MSI should obtain a sign-off from the GoSL before site setup.

(iv) Prepare a rack plan positioning infrastructure set up within the racks.

(v) The proposed solution should be optimized for power, rack space while ensuring high availability and no single point of failure.

(vi) MSI needs to consider the requirement for rack space and power for the suggested infrastructure as part of the proposal.

(vii) MSI will need to consider the required air flow, power outlets placement etc. to align with the facilities of Data Center as per the requirements of the infrastructure.

(viii) Assist in execution of the plan and commissioning the IT infrastructure.

(ix) MSI should work with the network provider to test the network links. The testing should include bandwidth, latency and other parameters decided in discussion with GoSL.

(x) MSI should verify and assess for all the facilities in the Tier III data center approved by GoSL, including but not limited to the following:

Type	Items
Data Center Facilities	• Main Power • Redundant Power (DG, UPS, etc.) • Cooling • Physical Security • Fire Detection and Suppression
Connectivity	• Internet Connectivity • Replication of Primary Site to Disaster Recovery Site • Other forms of connectivity listed in Section 5.2.6
Services	• SMS Gateway • Email Gateway

Table 8: Data Center

5.2.2 Hosting Environments

The MSI will be required to arrange the below mentioned environments, all environments should be fully functional covering end to end requirement to facilitate digital ID lifecycle:

Environment	Description
Development	The necessary development environment for solution should be created by MSI at offsite location.
Quality Assurance	The necessary testing & quality assurance environment for solution should be created in Primary Site as well as Disaster Recovery Site
Staging	Staging environment should be created in Primary Site as well as Disaster Recovery Site, and this staging environment should have downscaled sizing but should be identically configured as per the production environment.
Production	Production environment should be created in Primary Site as well as Disaster Recovery Site

Table 9: Hosting Environment

5.2.2.1 Hosting Infrastructure Requirements

Functional Requirements

1. The infrastructure should be capable of supporting disaster recovery and high availability across both the Primary Data Center and Disaster Recovery sites.
2. The proposed solution shall support distributed processing and load balancing.
3. Ability to provide integrated management for all the components proposed as part of the solution, including but not limited to:
   a. Database
   b. Application Server

c. Integration Server

d. Web Servers

e. User Identity Management

4. The solution should have tools to assist in the administration of:

   a. Configuration management

   b. Performance tuning

   c. System diagnostics

   d. Capacity planning

5. The solution should have the ability to support handling of errors as follows:

   a. Error logging

   b. Ability to redo/rollback a transaction after recovery from software/hardware failure to ensure data integrity.

6. The solution should include unique lifecycle management services that automate day to day operations, from bring up to configuration, resources provisioning and patching/upgrades and simplifies day-to-day management and operations. It should also provide capability for authorised users to start/stop/suspend virtual machines, take snapshot, delete machine, request additional resources and connecting to console through the self-service portal.

7. Solution must provide auto scale so that in case of increase in utilization additional VMs should automatically be created with all networks, security and load balancing assigned. All integration shall be performed to achieve automation.

8. Solution should provide proactive monitoring and management of complete virtualized infrastructure with prebuilt and configurable operations dashboards to provide real-time insight into infrastructure behavior, upcoming problems, and opportunities for efficiency improvements. Solution should monitor utilization of running VMs and should reclaim resources from idle VMs and allocate to other VMs in automated fashion.

9. The solution should be provided with container networking & security for developing microservice based applications and rolling them to the production environment. It should be capable to provide visibility across the container environment as well.

10. The solution 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.

11. Solution shall provide requirement performance to host applications and maintaining optimum hardware, software defined solutions in sustainable and scalable manner.

12. 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.

5.2.3 Installation, Configuration and Testing

As part of the overall lifecycle, the entire infrastructure has to be designed as per the deployment

architecture. This will be supplied and installed at the data center level, commissioned by MSI as per the specifications mentioned (**Refer Annexure 3: Minimum Technical Specification**) for each type of server, storage, network components etc. Acceptance of these equipment should be done as per the acceptance criteria and aspects like mapping of servers with the right set of applications, mapping the LUNs of storage for right level of database servers, setting up firewall equipment with appropriate ports for creation of zones, multiple storage tiers, etc.

High Level Activities are as follows: -

1. As part of service design phase rack space, number of blades and rack servers, network layout, HA, clustering activities will be completed. The design of servers will be done based on the final sizing requirements arrived at, considering the redundancy and high availability requirements. This would include necessary provisions like redundant ports availability, HBA cards, and redundant high-performance disks for operating system and application, etc.
2. The plan and design documents (HLD & LLD) thus developed shall be submitted to SL-UDI for approval and acceptance shall be obtained prior to commencement of any installation. All installations need to be carried out in accordance with the plans and layouts designs as approved by SL-UDI.
3. After completion of design, server build, OS configuration, OS hardening activities will be performed. Supply of servers need to be done keeping in mind the go-live of the entire system, since procurement and installation of the activities will also take time. Power and peripheral devices to be plugged in properly and AC power should be supplied to server through power PDUs. OS hardening should be done during the installation of servers to improve security.
    a) Testing of the servers with respect to the installed images of OS and application should be done, to avoid any mismatch in the configurations and also to avoid any errors during the development, testing or production phase of applications.
    b) Deployment of the servers for the production environment should be done, only after thorough checking of the configurations with respect to each server.
    c) Maintenance of the servers to be done, with appropriate physical cleaning, and all cables appropriately stacked and numbered, interconnecting through access switches and storage components.
4. As part of service design phase rack space, number of switches, HA requirements, failovers planning will be completed. The design of the network will be done based on the final bandwidth requirements arrived at, taking into account the redundancy/failover and high availability requirements. This would include necessary provisions like redundant network appliance availability, port, path, and performance. Network to be segregated into multiple physical, logical zones for security and isolation.
5. Post completion of design, router/switch configuration, routing/switching for failover will be performed. Space for network appliances will be identified in respective racks such as for server access switch, space will be identified in respective server racks. Power and peripheral devices to be plugged in properly and AC power should be supplied to server through power PDUs. Post completion of the build, the network environment will be tested for high-availability, smooth failover, etc. The network configuration will be tested for uniformity and any possible human error, loops etc. The network should also be tested for performance such as packet drops, latency, etc. All network devices should be configured properly for monitoring and management via Network

Management tool.

6. As per the project requirement, Data Center (DC/DR) network shall be divided into multiple zones, with each zone completely isolated from another zone via intrusion prevention devices and next gen firewalls. This is to enable enhanced security and isolation of each subsystem.
7. As part of the service design phase, the server consolidation ratio, VM placement, licensing requirements, storage virtualization, and network virtualization requirements will be reviewed. As part of this phase, the technical architecture, system architecture, security architecture, and virtualization architecture will be designed and agreed with stakeholders.
8. Post completion of design, hosts will have hypervisor configured, VM created, vCPU, vRAM, virtual storage, mount point assigned and registered.
9. Installation and configuration of the software procured as per this RFP or those required to ensure seamless operations of the IT Infrastructure including, but not limited to, Operating System (OS), System software, security suites etc. on the servers will be responsibility of the MSI. The MSI shall also tune parameters for optimal performance of the OS. It may also be kept in mind that MSI is expected to engage OEMs for providing on-site and off-site services in respect of the critical components. The MSI shall undertake necessary changes to harden the OS to prevent malicious and unwarranted attacks.

5.2.4 Design and Commission

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

5.2.5 Server Services

As part of server services rollout, below are the list of activities, but not limited to, which will be carried out as part of DC build work stream.

(i) **Design:** As part of service design phase rack space, number of blades and rack servers, network layout, HA, clustering activities will be completed. The design of servers will be done based on the final sizing requirements arrived, taking into account the redundancy and high availability requirements. This would include necessary provisions like redundant ports availability, card level redundancy, redundant HBA cards, redundant network cards and redundant high performance hard disks for operating system and application, etc.

(ii) **Build and Test:** After completion of design, server build, OS configuration, mount point allocation, OS hardening activities will be performed. Supply of servers need to be done keeping in mind the go-live of the entire system, since procurement and installation of the activities will also take time. Depending upon the type of server (rack/blade), the server should be mounted in the racks as per the installation activities with some spaces between racks to reduce noise level. Power and peripheral devices to be plugged in properly and AC power should be supplied to server through power PDUs. OS hardening should be done during the installation of servers to improve security.

a. Testing of the servers with respect to the installed images of the OS and application should be done, to avoid any mismatch in the configurations and also to avoid any errors during the

development, testing or production phase of applications.

b. Deployment of the servers for the production environment should be done, only after thorough checking of the configurations with respect to each server.

c. Maintenance of the servers to be done, with appropriate physical cleaning, and all cables appropriately stacked and numbered, interconnecting through access switches and storage components.

5.2.6 Network Services

As part of network services rollout, below are the list of activities which will be carried out as part of DC build work stream.

(i) **Design:** As part of service design phase rack space, number of switches, network cables, network layout, HA requirements, failovers planning will be completed. Design of network will be done based on the final bandwidth requirements arrived, taking into account the redundancy/failover and high availability requirements, and enrolment center to DC/DR connectivity and DC/DR replication links. This would include necessary provisions like redundant network appliance availability, port, path, and performance.

(ii) **Build and Test:** Post completion of design, network deployment/build, router/switch configuration, routing/switching for failover will be performed. Space for network appliances will be identified in respective racks such as for server access switch, space will be identified in respective server racks. Power and peripheral devices to be plugged in properly and AC power should be supplied to server through power PDUs. Post completion of the build, the network environment will be tested for high-availability, smooth failover, etc. The network configuration will be tested for uniformity and any possible human error, loops etc. The network should also be tested for performance such as packet drops, latency, etc. All network devices should be configured properly for monitoring and management via NLS tool.

This section describes the network requirements for the SL-UDI solution. The requirements of connectivity, WAN, DC-DR, internet are described in the section. The SL-UDI network proposes 3 different types of networks i.e., WAN, Data Center to Data Center (P2P links) Network, Internet Network.

The network connectivity encompasses the following:

#	Link	Type	Remarks
Partner Network			
1.	User Agency (UA) Connectivity	Not Applicable	MSI will be required to provide guidance documentation for connectivity between UA and its TSP.
2.	Trusted Service Providers (TSP)	P2P	TSPs' which may come on board in the future, the TSPs' will bring their own secured network from their point of aggregation to SL-UDI DC. The MSI will support to the network service provider of these TSP(s). MSI will be required to provide guidance documentation for connectivity between TSP and SL-UDI DC sites.

#	Link	Type	Remarks
SL-UDI Wide Area Network			
3.	Data Center - Interconnecti on Network	P2P	GoSL will provide secure and reliable connectivity.
4.	Data Centers (DC & DR) – NOC	MPLS/SD WAN	GoSL will provide secure and reliable connectivity.
5.	Data Centers (DC & DR) – SOC	MPLS/SD WAN	GoSL will provide secure and reliable connectivity.
6.	Data Centers (DC & DR) – Contact Centre	GoSL IPVPN	GoSL will provide secure and reliable connectivity.
7.	Data Centers (DC & DR) – Technical Helpdesk	MPLS/SD WAN	GoSL will provide secure and reliable connectivity.
8.	Data Centers (DC & DR) – Hosting Infrastructure	GoSL IPVPN	GoSL will provide secure and reliable connectivity, MSI shall work collaboratively with GoSL their network service provider
9.	Data Centers (DC & DR) – Head Office	GoSL IPVPN	GoSL will provide secure and reliable connectivity, MSI shall work collaboratively with GoSL their network service provider
10.	Connectivity at field offices (fixed registration centers)	GoSL IPVPN	GoSL has its own IP/VPN with Sri Lanka Telecom secure network to connect their fixed registration centers. GoSL will provide secure connectivity (including registration center end-point devices) from this network to the SL-UDI DC and DR. The MSI will accommodate and provide necessary support to the network service provider of the GoSL. The MSI should provide necessary network provisioning to terminate the connection.
Internet Connectivity			
11.	Internet for mobile registration centers	Internet	Provision for Internet Dongles will be made by GoSL
12.	***Note : All Network Links and Services contracted through Telecom services provider by GoSL must include DDoS Services/Solutions of required capacity.***		

Table 10: Network Connectivity

Standards and Guiding Principles for Connectivity

- Use Open Standards like TCP/IP (V4/V6) for Network / Transport Layer
- All data in transit and at rest to be encrypted.
- All external network connectivity should be via multiple ISPs.
- All Network links should be highly available – with redundant paths.
- All Network devices should be highly available with no single point of failure and should support redundant network interfaces.
- External Network Links to be provisioned from two different ISPs with different networks. paths
- All ingress traffic to be routed via Firewalls, NIPS, Deep packet inspection devices.
- All incoming packets to be subjected to AV Checks
- Network MUST be designed to handle Microservices, Virtualization, Software Defined Storage requirements.
- Network to be segregated into multiple Physical, Logical Zones for security & isolation.
- Access Control at every layer, MAC / Network / Transport / Application
- All network devices, links, ports should be monitored and managed via the management tools as defined in the EMS section.
- Separate network for data and management

5.2.7 IT Infrastructure Requirements

1. Considering the criticality of IT infrastructure and system software, GoSL expects the MSI to position the best of breed solution that is designed for high availability and enterprise class deployment.
2. MSI should offer latest and proven technologies that are available for items, including but not limited to, Processor model with highest possible clock speed, I/O, Memory and Cache, storage capacity, FC (Fiber Channel) interface and bandwidth, Security products, etc.
3. MSI should provide certified hardware/devices to propose technology stack.
4. MSI should ensure the hosting infrastructure placed at the DC and DR should be prominent products and are also available in the Sri Lankan market (However, this may exclude the systems infrastructure associated with the ABIS solution). This is to ensure efficient continuous upgrades and support & maintenance of the SL-UDI systems infrastructure at DC /DR even after the MSI contract ends.
5. The MSI is expected to work in close coordination with entities involved in SL-UDI project to ensure the success of the project. The MSI is also expected to manage relationships with OEM.
6. The MSI should ensure that none of the components/sub-components are declared end of sale or end of support by the respective OEM's.
    a. The MSI should not propose any component or sub-component which is likely to be declared end of sale **within 36 months** of award of contract. If the OEM declares any of the components or sub-components as **end of sale** for the said period, the MSI should replace proposed

components/sub-components with an equivalent or better alternate that is acceptable to the GoSL at no additional cost and without causing any performance degradation and project delays.

b. The MSI should not propose any component or sub-component which is likely to be declared end of support within the minimum 5-years from the date of signing of contract with GoSL. If the OEM declares any of the components or sub- components as **end of support** for the said period, the MSI should replace proposed components/sub-components with an equivalent or better alternate that is acceptable to the GoSL at no additional cost and without causing any performance degradation and project delays.

7. The MSI shall choose appropriate rack optimized equipment with suitable form factors for optimizing space in Data Centers. The MSI should ensure that the equipment can be mounted into the industry standard racks.

5.2.8 Storage Services

As part of storage services rollout, below are the list of activities which will be carried out as part of DC build work stream.

(i) **Design:** As part of service design phase rack space, number of disks, storage engine configuration, storage area network layout, RAID configuration, storage monitoring metrics will be configured. Design of storage component will be done based on the final sizing requirements arrived and the IOPs requirement. Based on the same, a multi-controller storage solution should be taken with a mix of different types of disks. Buffer at storage disks also need to be taken for global hot spares within the storage solution, providing redundancy and high availability at disk levels.

(ii) **Build and Test:** Post completion of design, RAID configuration, replication configuration, mount point allocation, port zoning activities will be performed. Post completion of mount point configuration for non-production environment server team will be asked to perform installation and carry out test activities. Post conformation from server team setup will be provided to middleware and performance test team to validate configuration and sizing. Supply of storage equipment is to be aligned with the procurement of servers so that appropriate card installation and interconnecting switches are deployed appropriately. Installation of the storage components start with identification of the right set of servers, applications, and data sets. The next key step as part of installation activity of storage is to configure each disk array with appropriate RAID levels. The SAN topology should be defined with respect to each zone viz. test, development, testing, production etc. Interconnection should be done through a pair of switches to ensure high performance and redundancies across the architecture. SAN management software should be used for the entire setup and configuration with servers. This will also help in testing the storage devices through checking appropriate mapping of servers.

5.2.9 Backup and Replication Services

The MSI will be responsible to provide backup and replication services at infrastructure level. The MSI will define the types of backups required and policies for back/replication frequency, in consultation with all the concerned stakeholders and GoSL. The MSI will be also responsible for application-level backup, ensuring the accuracy, completeness, and usefulness of the backup on a continuous basis.

As part of backup and replication services rollout below are the list of activities which will be carried out as part of DC build work stream.

(i) **Design:** As part of service design phase, backup service and replication service policies will be

reviewed, arrive at number of tapes, which will required for performing backup as per SL-UDI team policy. In addition, backup automation and DR automation requirements will be reviewed, and integration points will be identified. Normally backup can be classified into agented or agentless. Depending upon the data type, the same should be configured. Detailed backup policy to be provided during the requirements analysis phase.

(ii) **Build and Test:** Post completion of design backup and replication servers will be configured. Backup and replication services will be configured to pass alerts to monitoring tools. Post configuration of backup and replication server backup and replication success ratio, backup and replication failures backed up and replicated data amount, data encryption success will be monitored.

5.2.10 Virtual Environment Services

As part of virtual environment services rollout below are the list of activities which will be carried out as part of DC build work stream.

(i) **Design:** As part of the service design phase, the server consolidation ratio, VM placement, licensing requirements, storage virtualization, and network virtualization requirements will be reviewed. As part of this phase, the technical architecture, system architecture and virtualization architecture will be designed and agreed with stakeholders.

(ii) **Build and Test:** Post completion of design physical, hosts will have hypervisor configured, VM created, vCPU, vRAM, virtual storage, mount point assigned and registered with virtualization management server. Post configuration of virtual services, VM will be provided to middleware and testing team to complete testing and provide configuration on completion of environment.

Some of the key minimum functionalities to be considered in a proposed virtualization solution are as follows:

1. Virtualization solution should include bare metal hypervisor with functionality of high availability, zero downtime & zero data-loss, live migration, network QOS, dynamic resource scheduling, hot add (CPU, Memory, Storage & Network)
2. Virtualization solution should provide secure boot or equivalent for protection for both the hypervisor and guest operating system and it should have inbuilt distributed switch to centralize network provisioning, administration and monitoring using data center-wide network aggregation.
3. Virtualization solutions should provide monitoring and management of virtualized infrastructure with configurable, customizable operations dashboards to provide real- time insight into infrastructure behavior, and for capacity analytics. It should also provide infrastructure and operations analytics to eliminate time-consuming problem resolution processes through automated root cause analysis.
4. Virtualization solution should offer virtualized workload at the VNIC level to be protected with a stateful firewall engine based on constructs such as Mac, IP ports, objects and tags, active directory groups, security groups etc. and the security policies must follow the VM in the event of migration within the data center.
5. Virtualization solution must provide the NAT function for multitenant deployment, distributed in-kernel routing with support of routing protocols like OSPF and BGP, SSL VPN capabilities in the virtual environment, and it should protect east-west traffic by leveraging VM — based attributes like VM names, Security tags, OS type, logical switches etc.

5.2.11 Container & OS Environment Services

MSI is responsible for procuring & providing end to end support for the container platform. The MSI is also responsible for procuring the secure application & container monitoring solution. MSI also has responsibility for bringing and managing supporting OS, applications software, Web Security Testing tools, performance testing tools.

SL-UDI applications core module and other components shall be deployed in container formats across all environments. Container runtime shall not be limited to microservice based core application and other components such as API etc. shall also be deployed in containers to maximize the benefits. Management of container instances shall be done using enterprise level container orchestrations solutions.

MSI to ensure proposed container platform shall support a secure, enterprise-grade orchestration that provides policy-based control and automation for applications. Container platform should have following capabilities inbuilt into the system:

1. The platform shall have capability to run both stateful and stateless applications.
2. The container platform shall support deployment and orchestration of multiple containers formats (for e.g., docker etc.) for preventing any technology lock in.
3. The platform shall have inbuilt management and monitoring capabilities.
4. The platform shall have automated application build capability – from source code to a runnable container image.
5. The platform shall have/support integration with CI/CD tools. Integrated CI/CD tools have to be part of the solution.
6. The platform shall provide auto scaling capability for automatically running appropriate number of container instances as per load requirements.
7. The platform shall provide container instance auto healing capability.
8. The platform shall provide application/container version management, auto build of new application container instance in test environment basis on application code new version commit. Roll back to the earlier version.
9. The platform shall provide deployment strategies support such as for ensuring no/minimum downtime for application updates/upgrades.
10. The platform shall provide centralized logging capability (including applications logs from container instances) for audit, logs analysis & ease of management purpose.
11. The platform shall provide integrated container native persistent storage capabilities.
12. Generic/Shared Components as per the Solution Architecture Blueprint can be non – microservice/container based.

5.3 Field Infrastructure

5.3.1 Biometric Registration Kit – (As per the BOQ)

A registration kit at the enrolment desk shall comprise of the following components, not limited:

#	KIT Item	Provider
1.	Laptops	MSI
2.	Dual Display Monitor	MSI
3.	Printer cum Scanner	MSI
4.	Power Extension	GoSL
5.	Background Screen	MSI
6.	Web Camera	MSI
7.	USB Hub	MSI
8.	Enrolment – Fingerprint Scanner (4-4-2)	MSI
9.	Enrolment – Iris Scanner (Dual)	MSI
10.	Signature Pad	MSI
11.	Container to Transport	MSI

Table 11: Biometric Registration Kit

Note: In the enrolment kit, the enrolment software is installed which is integrated with Biometric-SDK

It is required to facilitate Mobile Kits with including the KIT items.

#	MOBILE KIT Item
1.	Laptop
2.	Document Scanner
3.	Printer
4.	Enrolment – Fingerprint Scanner (4-4-2)
5.	Enrolment – Iris Scanner (Dual)
6.	Web Camera
7.	UPS / Battery Backup
8.	USB Hub
9.	Flash Drive
10.	Background Screen
11.	Container

Table 12: Mobile Kits

Authentication Devices

Authentication Devices should be from 3 different OEMs.and should be supplied in the ratio given below :

Type	Qty. (MSI)	OEM-1	OEM-2	OEM-3
Fingerprint Authentication Device	Please refer to			

Type	Qty. (MSI)	OEM-1	OEM-2	OEM-3
Iris Authentication Device	BOQ [Section 7]	60%	30%	10%
Face Authentication Device				

Table 13: Volume of Authentication Biometric Capturing Devices

Note:

1. The devices from OEM-3 (10% quantity) should be a contactless device for iris registration device.

5.3.2 Supply, Installation and Commissioning of Enrolment Kits

(i) To enroll the individuals under the SL-UDI program, facilities for enrolments shall have to be created. The GoSL envisages reusing existing enrolment centers as well as setting up new enrolment centers across the country that would be equipped with enrolment kits for biometric enrolment. At present, it is estimated that fixed and mobile enrolment center will get established.

(ii) The MSI shall be responsible for supply, installation, testing and commissioning of these enrolment kits. The MSI shall be responsible for coordination with supplier of biometric kits and provider(s) of network connectivity for providing assistance for successful supply, integration, installation, and commissioning of enrolment kits.

(iii) It is expected that the enrolment software developed by the MOSIP shall be compatible/interoperable with biometric capture devices (fingerprint, iris, and photograph) of at least three leading and reputed OEMs. In order to ensure this, MSI is expected to provide each type of biometric capture devices (fingerprint, iris, and photograph) from three different OEMs.

(iv) In addition to the given quantity (specified in the Schedule of Requirements, Volume 2), additional biometric devices may be procured through the BSP at the rates specified in the contract signed between GoSL and MSI. In such a case, the scope of work for these additional biometric devices will be same as those for the original biometric devices.

(v) The responsibility of the BSP is to supply brand new, unused, defect free, and standard products without any damage. If, during the maintenance period, any biometric device has any failure on three occasions, it shall be replaced by equivalent new biometric device by the MSI at no cost to the GoSL.

5.3.2.1 Pre-Supply Activities

A summary of pre-supply activities is provided in the table given below:

Quality of Goods and Services	The equipment/product must conform to the specifications given and of desired quality. The MSI shall guarantee that the item/s delivered to the project sites/sites is/are brand new. Consistency in delivery shall be maintained for the entire lot of products ordered. For each product, all the required quantity of product/s in schedule of requirement shall be of the same brand and model number and the MSI/OEM shall not substitute any internal components or subsystems of the product by similar items of different OEMs. All the equipment shall be supplied with the relevant interface cables and necessary standard accessories. Also, all the equipment shall be provided with global standard, 3-pin power square plugs (230V supply voltage and 50 Hz, as required).
Custom Clearance	The MSI is completely responsible for clearing the imported goods through customs in an efficient manner free of any additional cost.

Table 14: pre-supply activities

5.3.2.2 Delivery

The MSI will be responsible to supply the enrolment kits at the project sites/sites (or any other location prescribed by GoSL) where the basic checks and testing have to be performed. A list of the locations of enrolment centers where such registration kits would be deployed has been given in **Annexure 12: Project sites and Sites.**

5.3.2.3 Testing and Certification

The MSI is required to perform various types of testing for the biometric devices which includes (quality report to be submitted), Installation & Integration Test, and User Acceptance Tests. The MSI is required to obtain prior approval of GoSL. The MSI is also required to submit the test reports and obtain approval of GoSL.

The biometric capture devices will be subject to an additional set of tests and certification requirements. As these devices will handle the biometrics of citizens, they should be compliant with functional requirements, technical specification, and security requirements. This will ensure we are working with devices compliant with requirements & specifications, operating as per open standards/protocols, have positioned in place security controls for biometric capture devices, etc.

On the immediate basis, the requirements for the biometric capture devices to be supplied under this program are as follows:

- MSI (and biometric device OEMs) are mandated to use legally procured digital certificates (a certifying authority in the country) for establishing legal bindings on transactions.
- MSI (and biometric device OEMs) must be contractually obliged to upgrade the SBI (Secure Biometric Interface) if there is a need, in a time MOSIP Advanced Compliance Program bound fashion. MSI will demonstrate the first level validation of the devices using MOSIP interface test kits.

5.3.2.4 Installation and Commissioning

To enroll the citizens under SL-UDI program, facilities for registration shall have to be created. The GoSL envisages utilizing existing and setting new enrolment centers across the country that would be equipped with Biometric Registration Kits for biometric registration of citizens.

The MSI shall be responsible for supply and operationalization of the overall registration kit with pre-installed Enrolment Software to the specified enrolment kit. The MSI is expected to test, install, commission, and ensure the functioning of Enrolment Kits in accordance with the plan approved by the GoSL.

For successful deployment of registration kits, the MSI shall:

- Prepare an installation, commissioning, and testing plan of the Enrolment Kits at enrolment centers and obtain approval from the GoSL.
- Demonstrate successful operation of enrolment kits (integrated with biometric devices and all components) to GoSL prior to supply of registration kits to enrolment centers.
- Successful functioning of fingerprint capture devices, digital camera and iris capture devices being procured from various OEMs should also be demonstrated.
- Port the Enrolment Software on the Enrolment Kits prior to supply of Enrolment Kits to the

enrolment centers.

- Follow the distribution plan approved by GoSL for supply, installation, and commissioning of registration kits. Safely transport kits at each enrolment center in accordance with the distribution plan. Monitoring of safe transportation of enrolment kits at enrolment centers in accordance with the distribution plan.
- MSI should also check the network connectivity at each enrolment centers and provide feedback to GoSL and suggestions to make improvements where necessary at enrolment centers.
- MSI is expected to commission and test the functioning of Enrolment Kits in accordance with the plan approved by the GoSL. The testing should also include integration testing for upload of the Enrolment packet from the Enrolment Kits to the Primary Data Center and Disaster Site. Also, sample enrolments should be carried out for a successful demonstration of commissioning of the Enrolment Kits.
- Post completion of the installation, commissioning, testing of registration kits and prior to commencement of registration a commissioning report must be prepared by the MSI (with support from BSP) and approved by GoSL. The format of this report must be prepared in consultation with GoSL.
- Note that the enrolment kit, registration kit terminology used above refers to both fixed enrolment kits used at enrolment centers/citizen service centers as well as the mobile enrolment kit.

5.3.3 Service Centers and Spares

In order to ensure uninterrupted enrolment services, the MSI for enrolment kits would be responsible. The MSI will be responsible for monitoring of the spares and maintenance activity of the enrolment kits and report deviations to the expected performance levels to GoSL.

5.3.3.1 Service Center

MSI should either utilize its existing service center or open a service center OR partner with existing service centers for repair and maintenance of biometric devices. The location of service center should be decided in consultation with GoSL, preferably in Colombo.

5.3.3.2 Protection against risk of obsolescence

MSI/OEM will make the spare parts for the systems available for a minimum period of three years from the time of Go-Live/Commencement of live operations.

If there is a model change is required due to market unavailability during the delivery of devices, MSI is expected to provide a device with an equal or higher technical spec having obtained the approval from GoSL.

5.3.3.3 Spares and Resolution of Issues

In order to ensure uninterrupted registration services, the MSI would maintain the inventory of spares and upon receiving a complaint of a damaged enrolment kit, the MSI should adhere to the given guidelines as per the **Annexure 9: Service-Levels (Section: Service Levels for Biometric Registration Kits).**

5.3.3.4 Software Updates

The MSI is required to provide software updates (including firmware, MOSIP SBI, etc.) of the biometric devices within specified timeline of the release of such update from the OEM and obtain prior approval of the GoSL. The below mentioned timelines are in reference to the date of release of such update from the

OEM:

- Regular Software Update – Three months
- Critical Security Update/Patch – As per the agreed schedule but no later than 15 days

5.4 Enrolment Centers

GoSL is setting up a wide network of registration centers across the country. The citizens can do their biometric registration (and updates) in these registration centers. These centers will be located in identified premises and will have the government staff to undertake the registrations under the SL-UDI program. The civil and electrical setup in these centers will be managed by the GoSL. In addition, the seating arrangements for citizens as well as government staff (including furniture) will also be made by the GoSL. GoSL needs to facilitate requirements from the MSI for monitoring.

The MSI needs to do the following:

- **Network Connectivity**: Monitor and support the network connectivity from enrolment center to DC/DR (refer Section 5.2.6)
- **Enrolment Kits:** Supply, Install, Test, Commissioning and Maintain the registration kits (Section 5.3)

Note: *Registration kits also include mobile enrolment kits*

5.5 Identity Cards

The GoSL will issue a polycarbonate card to the citizens registered under the SL-UDI program. The GoSL will do the procurement of such cards and card management system at their end and its own cost. The GoSL has the necessary software, hardware and manpower for card personalization, quality assurance, dispatch, and activation of cards. (**Refer Annexure 13: Card Printing and Personalization Solution**)

The GoSL will be responsible to provide the necessary card management solution and card personalization solution which will be capable of performing the below mentioned activities:

- **Inventory management**: Maintain an inventory of cards in their various stages i.e., blank, under personalization, rejected post personalization during QA, destroyed after rejection, lost cards (in internal processes), etc.
- **Personalization Workflow Management**: During the personalization the card passes through multiple stages. The software needs to track the status of the card from receipt of request for personalization onwards till activation. In case of lost card or expiry of validity, the cards' status needs to be updated accordingly.

5.6 Training and Capacity Building

During implementation and operation of SL-UDI Information System, MSI shall be required to train key resources to ensure successful implementation and operations of SL-UDI Information System in consultation with GoSL. The following shall be the responsibilities of the MSI for training:

5.6.1 Training Needs Assessment

MSI in consultation with the GoSL shall identify the training required to be imparted to GoSL team/different stakeholders for successful implementation and operations of SL-UDI Project. Both technical and support function training shall be identified by the MSI and approved by the GoSL. Manpower to be trained shall be identified by the GoSL in consultation with the MSI. Th training shall

be imparted on the Training of trainers (TOT) model where GoSL shall identify the master trainers to be trained by MSI. The master trainers in turn shall train the rest of the stakeholders. Maximum MSI shall train not more than 100 Master trainers. (**Annexure 14: Indicative List of Trainings**)

5.6.2 Preparation of Training Plan

(i) Post identification of the training needs, MSI shall prepare a training plan that highlights training type, target trainees, date of training, venue for training, trainer details, agenda of training etc.

(ii) Obtain approval on the training plan and schedule from GoSL

(iii) Prepare and finalize the training content to be delivered during the training session in consultation with GoSL. Obtain sign-off on the training content from GoSL.

(iv) Prepare training manuals in Tamil, Sinhalese, and English to be distributed to trainees during the training. Obtain sign-off on the training manual from GoSL. The actual bifurcation of the manuals to be printed in Tamil, Sinhalese, and English shall be obtained from the GoSL. The approved training manuals will be uploaded on the KMS portal by MSI.

(v) Prepare online tutorials, videos, presentations to be which shall be uploaded on the KMS portal. Obtain sign-off on the online tutorials, videos, presentations from the GoSL. Upload the content on KMS post approval.

5.6.3 Impart Trainings (Refer Annexure-14-List of Indicative Trainings)

(i) MSI shall be responsible for imparting the identified training in accordance with the training plan. MSI shall also be responsible for preparation of training material and training aids (document, audio, or video) that are required for successful completion of the training. During the training, MSI needs to provide copies of the relevant training material.

(ii) MSI has to ensure that the personnel deployed for training are properly qualified and understand the area of their training in depth.

(iii) The facilities for training like training classroom, projector, screen etc., would be provided by the GoSL.

5.6.4 Ensure Training Effectiveness

(i) MSI has to ensure that the training sessions held are effective and that the attendees will be able to carry on with their work efficiently. For this purpose, it is necessary that the effectiveness of training sessions is measured. The MSI will prepare a feedback form that will capture necessary parameters on measuring effectiveness of the training sessions. This form will be discussed and finalized with GoSL.

(ii) MSI is expected to design the test methodology in consultation with GoSL. MSI shall also devise a test for trainees, the test questionnaires must be approved by GoSL. GoSL shall also supervise all training provided by MSI and the Master Trainers at the regional level.

(iii) After each training session, feedback will be sought from each of the attendees on either printed feedback forms or through a link available on the web portal. The feedback received would be reported to GoSL for each training session.

(iv) For each training session, the MSI will categorize the feedback on a scale of 1 to 10, where 10 will denote excellent and 1 will denote unsatisfactory.

(v) The training session would be considered effective only after the cumulative score of the feedback [sum of all feedback divided by number of attendees] is more than 7. In case the

cumulative score of the feedback is less than 7, the MSI shall undertake re-training at no additional cost.

(vi) Prior to commencement of the enrolment, all Registration Officers who pass the test must be allocated certifications as well as a biometric based credential by the MSI.

5.7 Performance Testing, Security Compliance & Audit, Acceptance and Go-Live

Prior to Go-Live of the SL-UDI Information System, MSI shall be responsible for supporting the GoSL in User Acceptance testing, undertaking performance testing & security compliance/audit, and commissioning the SL-UDI Information System.

5.7.1 Performance Testing

(i) The Performance testing is intended to evaluate the ability of the solution implemented by MSI who scale to the intended usage. It is envisaged to cover the entire SL- UDI Information System, including its applications/software, other component solutions of SL-UDI Data Store, and all related interfaces. The Performance testing does not intend to simulate all the aspects of SL-UDI Information System however all design parameters of components and related interfaces shall be considered.

(ii) The following section outlines the guidelines to identify Performance testing values applicable for the tests.

a. The Performance testing should cover the entire Foundational ID platform and evaluate its ability to scale to support the expected usage levels.

b. The MSI will be responsible for creating the relevant Performance testing test cases to cover the scope identified. The MSI shall also provide the relevant scripts, tools, etc. necessary to conduct and complete the exercise successfully. All test cases should be discussed and approved by the GoSL.

c. The MSI shall assist the GoSL teams to performance test the DR setup.

d. The MSI should demonstrate at least one successful (live) run. Once the exercise is complete, the results of the exercise must be reported to the GoSL for approval.

e. GoSL may appoint a 3rd party agency to review and approve the benchmarking results on behalf of GoSL.

(iii) Performance testing shall be in accordance with the production deployment and solution deployed in accordance with the solution proposed by MSI.

(iv) MSI shall be responsible for undertaking the performance testing of the SL-UDI Solution. The MSI shall:

i. Prepare Performance test cases and obtain sign-off on the test cases from the GoSL.

ii. Supply, build, commission, configure, tune, and execute the benchmarks of the Disaster Recovery Set-up

iii. Provide the tools (load generator), scripts etc. for Performance testing. GoSL should not require licenses for such tools.

iv. Create test data (duplicate / dummy data)

v. Demonstrate at least one successful (live) run.

vi. Fingerprint (1 or multiple), Iris (both), Face or any combination thereof will be used for Performance testing.

vii. The report will be measured on average as well as 90 percentile bases.

viii. Undertake Performance testing of the SL-UDI Information System as per the parameter shown in the table below:

Test Scenario	Test Description	Gallery Size	Enrolment Rate	Test Duration	Number of BSPs
Enroll_0 to 4 Mn	Basic Performance Test with proposed sizing and associated IT Hardware	0	8000/Hr.	24 Hours	1
Enroll_4 to 8 Mn	Scalability with proposed sizing and associated IT Hardware	4 Mn	8000/Hr.	24 Hours	1

Table 15: Performance of the SL-UDI Information System

Where:

Enrolment Rate – Successful capture and encryption of demographic and biometric details of citizen at the rate of 25 minutes per enrolment per kit (1650 kits => 3960 per hour)

Test Duration – Duration in which 1: N deduplication of each enrolment packet should get completed in 24 hours' time cycle.

Test Scenario	Test Description	Gallery Size	Authentication Request Rate	Test Duration	Number of Concurrent Users
Auth_1	Basic Performance Test with proposed sizing and associated IT Hardware	4 Mn	0.45 Mn/Hr.	8 Hours	800
Auth_2	Advanced Performance Test with proposed sizing and associated IT Hardware	8 Mn	0.36 Mn/Hr.	8 Hours	800

Table 16: Performance of the SL-UDI Information System

Where: **Request Rate –** 70% of 1.75 million transactions spread over a 12–hour normal day period.

Authentication Request Rate (Basic Performance) – 0.1 million Authentication Requests are expected per hour with a response service time of 0.5 to 1 second with 800 concurrent users during basic performance test at system level.

Authentication Request Rate (Advanced Performance) – 0.1 million Authentication Requests are expected per hour with a response service time of 0.5 second with 800 concurrent users during advanced performance test.

Test Duration – Duration in which 1:1 matching authentication completes as per expected SLA of 0.5 to 1 second at the system level.

Test Scenario	Test Description	Gallery Size	No. of Users	Test Duration	Concurrent
Core MOSIP Application + Legacy Application	Basic Performance Test with proposed sizing and associated IT Hardware	2 Mn	1000 per 8 hrs.	24 Hours	2000
Deployed SL-UDI Solution	Scalability with proposed sizing and associated IT Hardware	10 Mn	4000 per 8 hrs.	24 Hours	8000

Table 17: Performance of the SL-UDI Information System

Basic Test – OTP based; Advanced Test – e-KYC including biometric authentication.

i. Report the performance testing output in the format specified by GoSL or its appointed agency. Key guidelines for reporting performance testing output are as follows:

(a). Reports for resource usage should have graphs with a sampling interval of 3 minutes for all resources (all servers, routers, switches, disk arrays, firewalls etc.)

(b). Response Time Reports should include minimum, maximum, average and 90 percentile response times. Response Time should be shown as a function of time for the duration of the test.

(c). ~~The test should measure the cumulative power consumed (KWh) for all the equipment's used for the performance testing with drill down of consumption by each equipment).~~

(d). The test results should also include the iterative configuration changes/tuning required to achieve the performance testing results.

(e). The list of equipment used for the test shall be the same as proposed by the MSI, if however, there is a shortfall in the quantity of the equipment proposed, the MSI shall provide the required quantity of equipment/licenses as the case may- be to achieve the performance testing results and SLA.

ii. GoSL shall witness the performance testing or appoint an agency to verify and validate the benchmarking environment and certify the results of the benchmarking. Performance test report provided by the MSI shall be verified and certified by the GoSL.

iii. In the event the solution and the corresponding Bill of Materials proposed by the MSI fails to meet the benchmarking performance criteria, MSI shall enhance/augment and supply additional components (including server, storage, networking equipment, etc.) without any additional cost to the GoSL such that the benchmark performance is delivered by the solution proposed.

iv. The MSI is expected to define parameters to measure performance of SL-UDI Information System in consultation with the GoSL.

5.7.2 Acceptance

Completion of activity of 5.7.1 (mentioned above) of the SL-UDI Information System, the GoSL shall undertake a user acceptance of the entire system. Acceptance for the SL-UDI Information System can be divided into the following phases:

5.7.2.1 Pre-Acceptance phase

I. ***Creation of Acceptance Plan***

(i) The MSI shall first identify areas of acceptance of the SL-UDI Information System. The MSI shall then prepare a draft acceptance plan comprising of acceptance methodology for identified areas, test schedule, timeline of acceptance testing activities and deliverable due dates. The test schedule prepared should identify major test areas, test execution, and test reporting activities. As a part of acceptance plan, MSI will also identify roles and responsibilities of the individuals to carry out the acceptance.

(ii) The MSI shall be responsible for creating the acceptance plan consisting of the following:

a. The required key area covered by the acceptance plan (b). Acceptance methodology for the identified areas

b. Test plan including schedule, timeline, duration, test activities and due deliverable dates.

c. Detailed acceptance tests

d. Format for acceptance reports.

e. Highlight any major test areas and reporting activities (g). Key individuals and responsibilities

(iii) The acceptance plan should be in alignment with the overall project plan. It will enable MSI and GoSL to plan the overall project timelines and resource requirements for acceptance phase.

(iv) The Acceptance of the solution shall be provided by the GoSL only after the following conditions have been met successfully to the satisfaction of GoSL.

a. Successful go-live of the solution to Primary site and to Disaster Recovery site to the extent necessary for meeting the desired objectives.

b. Successful operation for 30 working days after complete rollout of the system meeting the defined Services Levels.

c. Completion of all the documentation required as part of this RFP and as desired by GoSL to their satisfaction.

d. Installation and Configuration of all the components of the solutions including hardware, software, storage, accessories to the satisfaction of GoSL at both the sites and successful testing of all components.

e. The MSI should demonstrate the performance of the application in "live" condition at Disaster Recovery Site to the satisfaction of within a timeframe of three months from the date of successful go-live from the Primary site.

II. ***Assistance in formulating detailed acceptance criteria***

MSI shall prepare draft acceptance criteria for each of the above-mentioned areas of acceptance. Acceptance criteria prepared should be in accordance with the system specifications and functional specifications of the products/service.

III. ***Preparation of detailed Pre-Acceptance and Acceptance checklists***

(i) MSI shall prepare a detailed checklist of the activities and pre-requisites that are required to be completed before and during the phase of acceptance by GoSL. This shall include, but are not limited to:

a. Required approvals.

b. Availability of testing tools, monitoring tool and test management tools

c. Preparation of acceptance test scenarios, test cases and test data

d. Setup of hardware and software etc.

(ii) The test cases and scenarios developed should be well documented in the format approved by the GoSL.

IV. ***Preparation of required environment and facilities***

(i) ***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.***

(ii) The MSI should prepare draft versions of the acceptance criteria in alignment with the functional, system and non-functional specifications of the Foundational ID platform. The Acceptance Criteria should cover all of the above-mentioned Foundational ID platform areas.

(iii) The following is the indicative acceptance criteria for some of the deliverables and work products.

a. Acceptance criteria for Biometric Solutions

- Successful testing/re-testing of all the application test cases.
- Adherence to the acceptance test cases developed for each requirement of solution component.
- Review and acceptance of all the application deliverables including documentation.
- Successful adherence to service levels on SLA testing/measurement undertaken.
- Successful execution of the application related training to all identified users
- Successful go-live and closure of all incidents of the solution

b. Acceptance criteria for Documented Work Products/Deliverables

- Finalization of expected contents of work product with GoSL prior to submission of draft document
- Submission of draft document for GoSL review after sufficient internal review by the MSI
- Closure of review comments from GoSL within the timelines stated.
- Acceptance of revised draft(s) by GoSL based on adequacy and quality of the final submission.

5.7.2.2 Acceptance Phase

V. ***Execution of Tests***

(i) MSI shall assist the GoSL's acceptance test team in executing the defined test cases and scenarios. In the event of unexpected test results / bugs, MSI shall log tickets according to the severity of the issue.

(ii) GoSL may take assistance from an Agency for support in activities related to acceptance of SL-UDI Information System. The MSI must provide all necessary support to the agency for undertaking the acceptance including sharing of system specifications, functional specifications,

acceptance plan, and test cases.

(iii) The MSI will be required to log necessary tickets with appropriate severity ratings for issues/bugs identified during the testing.

VI. ***Resolution of issues identified during the acceptance testing***

(i) All issues and defects identified by GoSL's acceptance test team will be recorded in a defined template. For each incident, the MSI's defect tracking system should document each issue/defect identified, how it occurred, when it occurred, the tester who discovered it, what system baseline was being used, and a preliminary assessment of the severity.

(ii) The MSI should track and report on open defects until they are closed.

(iii) The MSI shall undertake following activities for root cause analysis and take preventive measures:

a. For every defect reported, the MSI team shall carry out root cause analysis (RCA) and document the same.

b. At agreed upon intervals, the GoSL's acceptance team and MSI's team should meet to review the identified defects and decide upon their prioritization and disposition.

c. MSI shall undertake remedial actions for resolution of the defect.

d. MSI shall work out preventive measures so that the incident does not occur in the future.

(iv) A sample template for reporting the defects shall be prepared by MSI.

(v) Upon resolution of defects and internal testing, for a maximum of three iterations, the MSI shall be responsible for retesting the issues at no additional cost. The MSI shall support the GoSL's acceptance test team in re-executing the acceptance test procedures and retest each corrected defect. GoSL's acceptance test team can also undertake additional testing if required. If the incident does not re-occur the GoSL's acceptance test team shall recommend closure of the defect. In case incident continues to occur, the GoSL's acceptance test team shall inform the MSI, and the defect shall remain open.

(vi) The MSI shall commission the entire system in the GoSL Primary Data Center and Disaster Recovery Site. After successful commission of the application, the GoSL shall undertake a user acceptance of the entire system.

5.7.2.3 Post Acceptance Phase

VII. ***Acceptance Documentation and Signoff***

1. The MSI shall assist GoSL's acceptance test team in creating the reports for acceptance testing. The reports shall summarize the test activities and identify outstanding deficiencies and issues.

2. The Acceptance Test Final Report shall be the detailed record of the acceptance test activities. It shall record which tests were performed, the pass/fail status of each test, and the discrepancies or issues found.

3. MSI shall be responsible for the following deliverables at the end of acceptance testing:

a. Acceptance Test Plan

b. Acceptance Test Schedule

c. Acceptance Test Environment Inventory

d. Acceptance Test Summary Report

e. Acceptance Test Final Report

4. Post completion of required documentation and due diligence, MSI shall obtain signoff from the GoSL's acceptance test team. This will constitute Go-Live.

5.8 Information Security and Business Continuity

5.8.1 Information Security

The GoSL is preparing the following, but not limited to:

(i) Information Security Policy & Plan

(ii) Access Control Policy and Procedure

(iii) Business Continuity Management Plan

(iv) Incident Management Policy and Procedure

(v) Information Backup Management Policy and Procedure

(vi) Information Security Policy for Technical Users

(vii) Vulnerability Management Policy and Procedure

(viii) And other policies and guidelines

These reports shall be shared with the MSI for study under a Non-Disclosure Agreement. The MSI is required to study these documents and consider the recommendation of these documents while implementing the solution, disaster recovery and business continuity policy and the risk management plan. The security solution of SL-UDI Information System should comply with the international security standard ISO 27001.

MSI shall adopt and follow the switch over strategy (SOS) for enrolment, authentication, CRM etc. in consultation with the GoSL.

MSI needs to utilize one of the existing Certification Service Provider (CSP) under the National Certification Authority (NCA) for Digital Signatures in Sri Lanka (Maximum 5000 Digital Signatures). The design should be done in such a manner that the SL-UDI operations should be able to switch to another CA within a reasonable time with minimal effort without losing any data, in case required.

Alternatively, MSI can bring in own digital signature issuance infrastructure as a part of the solution.

Note: The MSI should ensure that all the components can be accessible only within Sri Lanka and not accessible outside.

5.8.1.1 Processes and Procedures

Some of the indicative and non-exhaustive security processes and procedures that shall be developed, documented, implemented, and maintained by MSI are listed and described below:

(i) **Process for security of SL-UDI data repository:** MSI shall develop processes to secure the data repository, which contains information that SL-UDI intends to store and retain. This data store consists of various records such as demographic data, biometric data, enrolment records, authentication records, ecosystem information etc. Since this repository contains information that is of paramount importance to identify a citizen and establish trail of events specific to a record,

it needs to be protected at every stage of its lifecycle.

(ii) **Key management process:** MSI shall develop processes for securing cryptographic keys in SL-UDI ecosystem. Key management is crucial to the success of identity and authentication services for all stakeholders other than citizens. It helps establish an identity, confidentiality/availability, integrity and ensures in non-repudiation of system users. HSM shall be used for effective key management and HSM management process shall be developed.

(iii) **Logging and auditing process:** Logs provide useful information to support troubleshooting, forensics, audits, trend analysis, internal investigations, incident response, and optimizing system and network performance. It is essential that SL-UDI collects, periodically reviews, and securely archives the security log data, including encryption logs (i.e., logs from HSM and other cryptographic processes, where applicable), for a defined period of time. MSI shall develop logging and auditing processes ensuring security and retention of security logs.

(iv) **Process for use of portable media:** MSI shall develop and implement processes for use of portable media in SL-UDI premises such as USB drives, CDs, magnetic tapes, mobile devices, etc.

(v) **IT asset certification process:** MSI shall review, enhance, and implement necessary security guidelines and measures before introduction or deployment of an IT asset in SL- UDI environment. MSI shall also evaluate and minimize impact to other existing processes, applications, devices, etc. affected by introduction of the new asset.

(vi) **Risk assessment and treatment process:** MSI shall develop and implement processes for identification, estimation, assessment, and treatment of security risks in SL-UDI's applications, systems, office, and DC/DR locations, etc. basis SL-UDI's risk management framework.

5.8.1.2 Minimum Baseline Security Standards (or referred to as Hardening standards)

(i) MSI shall be responsible for development, documentation, implementation, and maintenance of minimum baseline security standards for all procured SL-UDI IT infrastructure, such as virtualization and software defined data centers, OS, network devices, security devices, application platforms, databases, etc.

(ii) MSI shall develop, implement, and maintain version-wise hardening standards for all IT infrastructure while referencing CIS benchmarking or MSI specifications for hardening. The cyber Security Policy applicable to Public Authorities (as per The Government of Sri Lanka cabinet decision- August 2022) will be notified to the successful bidders, along with other policies. All minimum baseline security standards shall be prepared in consultation with GoSL.

5.8.1.3 Security Components for Implementation

1. An indicative list of the security components and tools considered for security solution is given below. The MSI shall be responsible for procurement, deployment as well as daily operations of all security tools and technologies in SL-UDI environment.
    a. Next Gen Firewall (Internal and External)
    b. Web Application Firewall
    ~~c.~~ HIPS/NIPS
    d. SSL VPN Solution
    e. HSM

f. Anti-DDoS - DDoS As A Service to be provided by GoSL . MSI to monitor the same

g. DLP Solution.

h. Web Gateway.

i. 2-Factor Authentication.

j. SIEM.

k. PIM and PAM.

l. Database Activity Monitoring.

m. Code Review Tool

n. Network Vulnerability Scanner.

o. Anti-APT.

p. Patch Management Solution.

q. Antivirus

r. IDAM

s. Network Detection and Response

t. Endpoint Detection And Response

u. Application Vulnerability Scanner

For reference, the requirement of solutions on endpoints as well as servers is provided in the table given below, in addition, the MSI is expected to do its own analysis, design and estimation for the requirement quantity of these solutions.

#	Security Solution	Coverage	
		Endpoint (Desktops, Laptops etc.)	**Servers**
1.	NextGen Firewall (Internal and External)	Not Applicable	Firewall is an appliance that will be placed in DC and DR
2.	Web Application Firewall (WAF)	Not Applicable	WAF is an appliance that will be placed in the DC and DR to provide protection to web applications hosted behind the WAF
3.	Host Intrusion Prevention System (HIPS)	All 4000+ endpoints (Including endpoints to be used in enrolment centers)	All Servers in Data Center and DR across all environments (Prod/Staging/QA etc.)
4.	Endpoint Detection and Response (EDR)	All 4000+ endpoints (Including endpoints to be used in enrolment centers)	Server hosting the centralized EDR console (In DC and DR)

#	Security Solution	Coverage	
		Endpoint (Desktops, Laptops etc.)	**Servers**
5.	Data Loss Prevention (DLP)	Endpoint DLP – All 4000+ endpoints (Including endpoints to be used in enrolment centers)	Network DLP – All Servers/Network gateways in Data Center and DR across all environments (Prod/Staging/QA etc.)
6.	Web Gateway	Not Applicable	Deployed on the network at the gateways which provide access to the internet
7.	2-Factor Authentication (2FA)	2FA sizing is generally done per user/account	Server hosting the 2FA tool (DC + DR)
8.	Code Review Tool	Not Applicable	Server hosting the code review tool
9.	Patch Management Tool	Agents to be installed on all endpoints for installing patch	Server hosting the centralized Patch Management console + Agents are installed on all servers integrated with patch management tool
10.	Network Vulnerability Scanner	Not Applicable	Server hosting the network vulnerability scanner tool
11.	Hardware Security Module (HSM)	Not Applicable	HSM is an appliance that will be placed in DC and DR
12.	Security Information and Event Monitoring (SIEM)	Not Applicable	Server hosting the SIEM tool (DC + DR) + Agents are installed on all servers/databases/app servers etc. to integrate with SIEM
13.	Privileged Access Management (PAM) / Privileged Identity Management (PIM):	PIM/PAM sizing is generally done per user/account	Server hosting the PIM/PAM tool (DC + DR)
14.	Access Control System and Directory Services	All 4000+ endpoints (Including endpoints to be used in enrolment centers)	All Servers in Data Center and DR across all environments (Prod/Staging/QA etc.) + Standalone server hosting the tool
15.	Database Activity Monitoring (DAM)	Not Applicable	DAM agent to be installed on all Database servers in Data

#	Security Solution	Coverage	
		Endpoint (Desktops, Laptops etc.)	**Servers**
			Center and DR across all environments (Prod/Staging/QA etc.) + Standalone server hosting the tool
16.	Anti-Advanced Persistent Threats (Anti- APT)	APT should cover all endpoints, to monitor endpoint behavior, traffic etc.	Anti-APT is an appliance that will be placed in DC and DR
17.	Anti-DDoS	Not Applicable	Anti-DDoS services will be provided by GoSL Teleocm Service Provider
18.	Identity and Access Management	Not Applicable	Server hosting IDAM suite
19.	Network Detection and Response	Not Applicable	Server hosting NDR/NDR server console

Table 18: Requirement of Solutions on Endpoints as well as Servers

5.8.1.4 Security Requirements – Software Security Requirements

The requirements for software security are as listed below:

1. Ensure security of enrolment, authentication software and other software brought by the Software service provider.
2. Configure and implement the software securely as per SL-UDI risk assessment in this document and policies specifically ensuring encryption of sensitive data, secure communication, strong passwords, secure storage of application passwords, integration with HSM for usage of encryption keys, enable security logging in the software, integrate with security solutions of SL-UDI, other security configurations communication from time to time.
3. Enable security logging and support integration with security solutions. Logs shall be time stamped and shall include details like events and the activities performed, date and time stamps, terminal identity or location, user IDs, records of successful and rejected system access attempts, records of successful and rejected data and other resource access attempts, etc.
4. Ensure access control configuration to support SL-UDI access control policies.
5. Apply Security patches as per SL-UDI policy.
6. Ensure compliance to other security policies of SL-UDI.
7. The SL-UDI Platform software shall conform to the level of assurance and shall provide different, multifactor authentication services.
8. Ensure API Security or Microservice in line with SL-UDI. (This should be fully encrypted).
9. Ensure system security when doing the system scalability and increase concurrent user and transaction at a time.

5.8.1.5 Security Requirements – ABIS and Biometric Device Security Requirements

The requirements for ABIS and Biometric Devices security are as listed below:

1. Ensure security of ABIS software and biometric device drivers.
2. Ensure encryption of Biometric databases with at least AES 256-bit for symmetric encryption and RSA 2048 bit for asymmetric encryption or any other tool by BSP for encrypting the data.
3. Ensure Biometric databases do not have the corresponding SL-UDI number or any other individual identification number present in the databases. The biometric databases shall be federated to protect the individual's identity and to ensure security by design.
4. Ensure only certified Biometric devices are deployed for SL-UDI project.
5. Ensure encryption of enrolment packet at biometric device hardware level within the Secure element of the Biometric Hardware.
6. Ensure only registered devices are deployed for the SL-UDI project.
7. Configure and implement the ABIS software and Biometric device driver as per SL- UDI risk assessment in this document and policies specifically ensuring encryption of sensitive data, secure communication, strong passwords, secure storage of application passwords, integration with HSM for usage of encryption keys, enable security logging in the software, integrate with security solutions of SL-UDI, other security configurations communication from time to time.
8. Enable secure logging and support integration with security solutions.
9. Deploy and integrate security solutions with the ABIS solution and biometric devices.
10. Apply security patches as per SL-UDI policy.
11. Backdoors and other vulnerabilities should be checked in a sandbox environment prior to installation.
12. Ensure multimodal biometrics compatibility.
13. Ensure device and security compliance compatibility. (Sri Lankan Laws, Policies, and International Compliance).
14. Ensure that audit logs (ex: User Activities, Exceptions, Information Security Event logs) and relevant logs can be integrated with SL-UDI audit logs management solution.
15. Ensure fast matching in verification, identification, and deduplication modes. E.g., million comparisons per second on **each node** of the system.
16. Support scalable, modular architecture with high availability and fault tolerance.
17. Ensure that customization is possible for specific project needs.
18. Ensure availability of SDK's.

5.8.1.6 Security Requirements – Infrastructure Security Requirements

The requirements for infrastructure security are as listed below:

1. Ensure security of Infrastructure components
2. Maintain a comprehensive asset register for all infrastructure components as per SL-UDI policy.
3. Ensure security configuration of the infrastructure components as per SL-UDI policy.

4. Ensure access control on the infrastructure components as per SL-UDI policy.
5. Enable security logging and support integration with Security solutions.
6. Implement BCP/DR policy as per SL-UDI Guidelines
7. Ensure load balancing capability.
8. Conduct infrastructure system audit.
9. Apply security patches as per SL-UDI policy.
10. Backdoors and other vulnerabilities should be checked in a development environment prior to installation.
11. Configure and implement the ABIS software and Biometric device driver as per SL- UDI specifically ensuring encryption of sensitive data, secure communication, strong passwords, secure storage of application passwords, integration with HSM for usage of encryption keys, enable security logging in the software, integrate with security solutions of SL-UDI, other security configurations communication from time to time.

5.8.1.7 Security Requirements – Security Operations

1. Design security operations model including detailed technical design.
2. Implement SOC infrastructure, security tools and integrate with the SL-UDI network.
3. Deploy Security solutions as per architecture agreed with the SL-UDI team.
4. Ensure installation and integration of all Security solutions on all components.
5. Perform continuous monitoring of the cyber security posture in SL-UDI by analyzing, detecting, preventing, and responding to cyber security threats and incidents.
6. Provide BCP/DR provisions and maintain compliance as per BCP policy.
7. Ensure the SOC Infrastructure meets standard benchmarking requirements like ISO, NIST Cybersecurity framework etc
8. Support SL-UDI during external certification and other security audits – such as ISO 22301, ISO 27001, etc.
9. Integrate Security solutions with other systems components such as Infrastructure, Container Platforms, Virtual Appliances, Software etc.
10. Highlight gaps on a periodic basis to SL-UDI management.
11. Enable security logging and support integration with Security solutions.

5.8.1.8 Security Processes and Procedures

The MSI shall ensure **design yearly update** of security processes and procedures, and document them as part of their scope. Some of the indicative security processes and procedures that shall be updated, documented and maintained by the MSI are listed and described below:

1. **Key management process**: MSI shall develop processes for securing cryptographic keys in SL-UDI ecosystem. Key management is crucial to the success of identity and authentication services for all stakeholders other than residents. It helps establish an identity, confidentiality/ integrity and ensures in non-repudiation of system users. HSM shall be used for effective key management and HSM management process shall be developed.

2. **Logging and auditing process**: Logs provide useful information to support troubleshooting, forensics, audits, trend analysis, internal investigations, incident response, and optimizing system and network performance. It is essential that SL-UDI collects, periodically reviews, and securely archives the security log data for a defined period of time. MSI shall develop logging and auditing processes ensuring security and retention of security logs.
3. **Access management process**: MSI shall develop and implement processes that allow tracking and recording the persons/entities who have any type of access, inclusive of remote access, to or custody of SL-UDI related information.
4. **Asset management process**: MSI shall develop a process and achieve and maintain complete protection of SL-UDI assets by inventorying all assets, assigning ownership to them, and maintaining appropriate security controls of assets. An appropriate asset management tool may be implemented for this process.
5. **2-factor authentication process**: MSI shall develop and implement secure login process and avoid unauthorized access via implementation of combination of password, OTP, Biometrics, etc.
6. **Business Continuity and Disaster Recovery processes**: MSI shall develop and implement processes and response procedures for business continuity and disaster recovery. MSI shall ensure compliance to ISO 22301 standard.
7. **Biometric exception process**: MSI shall develop and implement processes to capture biometric exceptions for residents who are unable to provide fingerprints or any other biometrics, owing to reasons such as injury, deformities, or any other relevant reason.
8. **Enrolment packet quality check process**: MSI shall develop processes and undertake quality checks for enrolment packets which will contain citizen PII such as biometric and demographic information.
9. **Patch management process**: MSI shall implement patch management and develop and implement processes for managing (acquiring, testing, and installing) patches or upgrades for software applications and technologies deployed in SL-UDI.
10. **Secure login process**: MSI shall develop and implement processes for secure login, authentication, and access to SL-UDI systems.
11. **Internal audit process**: MSI shall develop yearly plan for internal security audit and vulnerability assessment. MSI shall identify the systems, applications, and processes, to be covered under vulnerability assessment and penetration testing activities and prepare a plan for the same. Additionally, MSI shall implement corrective and preventive actions for non-compliance observed and plan and implement new information security tools authorized by SL-UDI management.
12. **User Acceptance Testing Process**: MSI shall conduct UAT of all releases of SL-UDI software systems/solutions on behalf of SL-UDI, inclusive of both functional and non- functional test cases. MSI shall provide acceptance testing environment inclusive of all supply, install, integrate, build, and commission activities that may be necessary.

5.8.1.9 Security Controls - Enrolment related Security

VIII. ***The following security controls shall be put in place by MSI with respect to enrolment. MOSIP built in security should be enforced) Security while capturing Biometrics through Enrolment Devices***

1) Every machine shall be uniquely identified via online registration.

2) Enrolment software shall only run-on systems that have been sufficiently hardened as per SL-UDI specifications.
3) All officers shall have SL-UDI number, shall be trained, and certified, and registered with SL-UDI.
4) Every enrolment packet shall be biometrically signed by the officer.
5) Resident data including raw biometrics shall be encrypted at run time.
6) Every enrolment packet shall be encrypted. Encryption shall be done on the biometric capture device at hardware level (AES 256 and PKI 2048 bit).
7) Encrypted biometric packets shall not be stored at any other place other than enrolment packet.
8) Enrolment software shall run an automated purging script to securely delete any enrolment packets older than the policy requirement.
9) Secure channels such as HTTPS shall be used to transmit the enrolment packer to SL-UDI DS.
10) Enrolment packet shall be digitally / biometric signed, and signature shall be validated at server for every transaction.
11) GPS devices shall be installed at the enrolment system and enrolment software shall capture the Geo location and send along with the enrolment packet to ensure that enrolment is not done outside the country.
12) Enrolment station (laptop, Desktop) shall protect with endpoint extended detection and protection solution.

IX. ***Security while transferring enrolment packets from Enrolment Devices***

1) Every enrolment data packet shall "always" be stored in PKI encrypted, tamper proof files or database.
2) Enrolment data shall "never" be decrypted in transit until it is reached SL-UDI.
3) The 2048-bit PKI encryption ensures that it is not possible to decrypt and extract any information even if enrolment packets are available to anyone in transit.
4) The enrolment software having feature for secure upload of encrypted enrolment packets to SL-UDI shall be provisioned.
~~5)~~ All uploads shall happen only through registered upload stations.
6) Malware checks shall be done on the enrolment packets received in SL-UDI DS before processing the packet.

X. ***Security while storing enrolment packets in Identity Repository***

1) Validation of "all" enrolment packets for authenticity of source, authenticity of officers, overall validity of data, any tampering, viruses, etc.
~~2)~~ Additional metadata shall be collected as part of every enrolment packet for performance.
3) Enrolment packets shall be kept in encrypted format within SL-UDI.

5.8.1.10 Security Controls - Authentication related Security

Following security controls shall be put in place by the MSI with respect to authentication:

I. ***Security while capturing Biometrics through Authentication Devices***

1) End to end encryption of identity data shall be enforced.
2) Only certified biometric devices, with liveness detection features, shall be used for authentication.
3) Biometric Devices shall encrypt data at hardware level.
4) The identity data block in the authentication data shall be encrypted at capture (using AES-256 and followed by a 2048-bit public key) at device level.
5) HMAC within the authentication packet shall ensure no tampering is done.
6) Authentication server shall have replay (presentation attack) detection capabilities. Controls shall be deployed so that the authentication packet once sent for authentication cannot be used again for authentication. ISO/IEC has provided a framework, data format, and testing methodology via its standards ISO/IEC 30107-1, ISO/IEC 30107-2, and ISO/IEC 30107-3 respectively to detect such presentation attacks, and the same shall be leveraged by the MSI to thwart presentation attacks.

II. ***Security while transferring Authentication packets from Authentication server to Identity Repository***

1) TSP to Authentication Server connectivity shall be only over a leased/ ~~MPLS~~ P2P network terminating the data centers along with IP filtering.
2) Traffic from the various TSP's shall hit the DMZ of SL-UDI only after going through security mechanisms such as IDS/IPS and Firewall.
3) HMAC and DSC shall ensure end-to-end data integrity while 2048-bit encryption and SSL shall ensure end-to-end data confidentiality.
4) Authentication packet shall be transmitted only on secure connection such as LAN, HTTPS or MPLS (if public network)
5) Encrypted biometric shall not be stored by the authentication agency post sending the authentication request to SL-UDI data store (DS)
6) Malware checks shall be done on the authentication packets received in SL-UDI DS before processing the packet.
7) Authentication packets that are rejected in the malware scan shall be securely deleted from the authentication server.

III. ***Securing authentication packets in the Authentication Server***

1) All authentication requests (HTTPS protocol only) shall terminate in DMZ and only connect via a private secure network which has IPS/ IDS, Firewalls, and virus scanners.
2) Every authentication request shall be validated for authenticity of source (DSC), access control (License keys), structure (XSD), and integrity of identity data block (HMAC).
3) All biometric/OTP authentication requests shall be notified to citizens/residents.

4) The Authentication database shall be encrypted all the time.

IV. ***Securing and monitoring authentication for all critical systems related to SL-UDI***

1) All authentications shall be channeled via a privileged access manager (PAM), to protect against accidental or deliberate misuse of privileged access by streamlining the authorization and monitoring of privileged users.

2) The solutions shall be designed and implemented according to the requirements of SL UDI.

5.8.1.11 Security Controls - Security of SL-UDI data centers, and data stores

Following controls shall be put in place w.r.t security of SL-UDI data centers, data stores and administrative offices.

Risk	Controls
Cyberattack from Internet	a. NG-Firewalls to allow specific traffic. b. NG-WAF for monitoring layer 7 (application level) attacks c. NG-IPS to monitor anomalies. d. NG-SIEM to monitor real time attacks. e. Vulnerability assessment and application testing tools f. Anti-DDoS solution to prevent DDoS attacks. Anti-DDoS services will be provided by GoSL Teleocm Service Provider as a part of GoSL Responsibility. g. HSM for secure storage of keys h. NG-SOC solution to monitor and prevent attacks.
Cyberattacks from Authentication partner network	a. Firewalls to allow specific traffic. b. IPS to monitor anomalies. c. SIEM to monitor real time attacks. d. Vulnerability assessment and application testing tools e. Anti-DDoS solution to prevent DDoS. Anti-DDoS services will be provided by GoSL Telecom Service Provider as a part of GoSL Responsibility. f. HSM for secure storage of keys g. NG-SOC solution to monitor and prevent attacks. h. Encryption of all data at storage and transmission to minimize the impact of cyber attack
Biometric data leakage from internal staff And Demographic data leakage from internal staff	a. DLP solution to prevent any data leakage. b. HSM for secure storage of keys c. PIM to control access to servers at OS level. d. DAM to monitor access to databases.

Risk	Controls
	e. SIEM to log internal activities and monitor real time violation of policies. f. Encryption of data in storage and transmission to minimize the impact.
Biometric data integrity within SL-UDI DS, and Demographic data integrity within SL-UDI DS	a. PIM to control access to servers at OS level. b. DAM to monitor access to databases. c. Encrypted raw packet is stored as it is and can be used to recreate the data.

Table 19: Security of SL-UDI data centers, data stores and administrative offices

5.8.2 Business Continuity and Disaster Recovery

The SL-UDI project is of immense importance to the Government of Sri Lanka, as it will be a biometrically de-duplicated repository containing information of the citizens. In this regard, it becomes important that the MSI plan to not only take maximum security measures but also plans to create a resilient environment/system which can be recovered in case of a disaster.

The strategy for the Data Center to be utilized for this project is given in Section 5.2. As per the Business Continuity Plan of SL-UDI, the following are key points:

(i) Primary Site and Disaster Recovery site shall have 1:1 capacity.

(ii) MSI shall endeavor zero data loss while switching from Primary Site to Disaster Recovery site by maintaining a very high level of RTO and RPO.

(iii) The switching from Primary Site to Disaster Recovery site (and vice-versa) should happen as per the Business Continuity Plan (BCP)

(iv) GoSL will be responsible to transport the tapes to the far site (including retrieval) and its safe and secure storage. Employer will provide the location with a (if deemed as appropriate biometric lock enabled) fireproof cabinet, etc.

MSI shall be responsible for performing operations as per the BCP plan and shall ensure recovery/backup as per the BCP policy. The MSI will also be responsible for resuming (including rolling back to Primary Site) the biometric solution and associated data. Thus, MSI will be responsible for managing the RTO and RPO. The MSI shall also be responsible for coordinating with the BSP and OEM(s).

The MSI is required to conduct the following as part of the Business Continuity and Disaster Recovery planning, however not limited to.

1. Develop BCP/DR plan.
2. Identify and review risks and gaps created by disruptive events that may impact the Foundational ID platform.
3. Execute the processes and procedures as per BCP/DR plan and conduct periodic (preferably, on an annual basis) BCP/DR drills (refer SLA). The MSI should coordinate with GoSL and other associated partners to ensure successful completion of the BCP/DR activities.
4. Create the functional Business Continuity working plans for GoSL's approval.

5. Plan, implement, execute, and maintain a disaster preparedness strategy which enables identification of BCP deficiencies and also verifies the disaster recovery procedures documented for the SL-UDI Solution.
6. Work with the SL-UDI management in defining the BCP organization structure and identifying roles and members. It is possible that the members may change over time. In such a case, each new member must get orientation training and complete education upon induction before being declared as ready to serve.
7. Develop a crisis communication plan to address external and internal communication before, during and after a disaster, to be executed by the management team.

BCP or DRM is defined as the way of recovering from a disturbance to, or a destructive incident in regular business operations impacting the services.

The main features of the BCP/DR policy to be considered in designing solution are as follows:

(i) DR solution with a comprehensive IT infrastructure offering core services such as virtual environment, container environment, computing, network and connectivity, and other supporting services.

(ii) Replication built-in feature, virtualization manager replication, storage replications, third- party tools etc. will be defined for each service and application during the design phase.

(iii) The Primary and Secondary sites will be configured in an Active-Active (for citizen web portal and Authentication application etc.) and Active-Passive mode (for other applications).

(iv) Both RPO and RTO will be as per Annexure 16 RACI Matrix. MSI shall confirm the RTO and RPO of their solution in the technical response to the RFP.

(v) Replication between the Primary site and the Secondary site will be enabled and configured.

(vi) Virtual servers for DR will be built on top of virtualization manager hypervisor offering an industry-leading virtualized platform and best-of-breed technologies to maximize the reliability and availability of your applications.

(vii) MSI will monitor and manage DR components 24x7.

A detailed disaster recovery plan is required to be formulated for SL-UDI to ensure that the processes and policies for handling the disaster situation and recovery models to be followed to ensure business continuity to be addressed.

MSI shall design, document, implement, and maintain all processes under BC/ DR such as tape recovery, data backup, HSM backup, data replication, remote working, infrastructure recovery, data and technology recovery, people recovery, emergency response procedures etc. for SL- UDI Programme, as well as country wide rollout basis the following details:

(i) Primary Data Center for continuous operations.

(ii) Disaster Recovery site (Secondary Site), for failover of operations.

(iii) Network connectivity required for replication will be provided by GoSL

The illustrative deliverables for this activity are mentioned below.

(i) Devise a Replication-and-Restore policy.

(ii) Update the Business Continuity Plan (BCP) Plan

(iii) Regular Drill Exercises at pre-decided frequencies (tentatively annually) and improvement in BCP

(iv) Bring up/roll back the solution in case of any systems failure in line with the approved BCP.

5.8.2.1 Process/component wise Recovery Strategy

An indicative list of recovery strategies, processes and components is given below. The MSI is expected to validate the list and add/modify/delete and finalize the recovery strategy in consultation with GoSL.

#	Process/ Component	Recovery Strategy
1.	Enrolment	• Active – Passive (DC – DR), or offline tape backup
2.	Authentication	• Active – Active (DC – DR),or offline tape backup
3.	Critical portals	• Active – Active (DC – DR), or offline tape backup
4.	Other portals	• Active – Passive -(DC – DR), or offline tape backup if any data other than logs
5.	CRM	• Active – Passive (DC – DR), or offline tape backup
6.	SOC	• Active – Passive (DC – DR), or offline tape backup
7.	Admin offices	• Active – Passive (DC – DR),or offline tape backup

Table 20: Indicative List of Recovery Strategy of Processes

5.8.2.2 Data Backup

The MSI is required to finalize the data back-up strategy in consultation with the GoSL's archival policy. From time-to-time should restore and ensure that the backups are restored properly. An indicative strategy for Data backup is given below.

(i) **Data Backup Strategy**: Grandfather-Father-Son (GFS): Key Aspects of GFS Strategy, to be implemented by the SL-UDI Master System integrator:

a. On the last day of every month, a full backup shall be performed and labelled "grandfather". The tape shall be stored permanently offsite.

b. On the last day of every week, a full backup shall be taken called the "father" and stored offsite.

c. Daily incremental backup shall be done called the "son". Son tapes can be stored onsite or offsite depending on the volume of data changes. Onsite tapes shall be kept in fireproof cabinet.

d. Tapes shall be **moved by GoSL** to offsite location on Daily basis at a geographically separate location with appropriate physical security controls.

e. For a 7-day working week, there are 6 son tapes, 3 father tapes, and a new grandfather tape every month.

f. Tapes shall be encrypted with symmetric key algorithm with highest key strength (such as AES GCM 256).

	Mon	Tue	Wed	Thurs	Fri	Sat	Sun

Week1	Son 1a	Son 1b	Son 1c	Son 1d	Son 1e	Son 1d	Father 1
Week2	Son 2a	Son 2b	Son 2c	Son 2d	Son 2e	Son 2d	Father 2
Week3	Son 3a	Son 3b	Son 3c	Son 3d	Son 3e	Son 3d	Father 3
Week4	Son 4a	Son 4b	Son 4c	Son 4d	Son 4e	Son 4d	**Grandfather**

	Daily incremental Backup
	Weekly full backup
	Monthly full Backup (Archive)

(ii) Type of data to be backed up shall include among others:

#	Data systems	Type of Data	Frequency	Storage
1.	Data in Databases	Encrypted raw enrolment packets, Encrypted Enrolment Databases, Authentication Databases, Authentication logs databases, POI POA documents databases, ABIS galleries, Encryption Keys databases (if any)	Daily, Weekly, and Monthly	Offsite location (other than DC, and DR) in fireproof safe
2.	Applications	Application databases, Application logs, Application configurations, Application software version repository, Demographic data	Daily, Weekly, and Monthly	Offsite location (other than DC, and DR) in fireproof safe
3.	Configurations	Latest Server configuration images, network configurations, Virtualization configuration, container configurations, COTS configuration, Security Configuration	Daily, Weekly, and Monthly	Offsite location (other than DC, and DR) in fireproof safe
4.	Documentation	Policy, process documents, Standard Operating procedures, any other important documents	Quarterly or when document is updated	Offsite location (other than DC, and DR) in fireproof safe
5.	Keys (HSM) – Encryption, Signing, etc.	HSM encryption keys	Every time a new key pair generated	HSM backup docks in biometric lockers

5.8.2.3 HSM Recovery

MSI shall ensure HSM encryption keys (signing, encryption keys and master keys) are replicated to the High Availability HSM cluster and backed up every time a new key pair is generated, and the keys are stored securely in HSM.

HSM recovery is critically important, to safeguard important cryptographic objects against unforeseen

damage or data loss. No device can offer total assurance against equipment failure, physical damage, or human error. Therefore, a comprehensive strategy for making regular backups is essential. MSI shall perform the following operations, depending on implementation.

(i) Develop and document a backup and recovery plan

(ii) To ensure that backups are always available, build redundancy into backup procedures

(iii) In the event of a catastrophe, such as a flood or fire, it might lose both your working HSMs and locally stored backup HSMs. To fully protect against such events, always store a copy of your backups at a remote location.

(iv) Execute recovery plan at least semi-annually (every six months) to ensure that fully recover key material. This involves retrieving stored Backup HSMs and restoring their contents to a test partition, to ensure that the data is intact, and that recovery plan works as documented.

#	Data	Frequency	Media	Storage
1.	Encryption Keys	Every time a new key pair is generated	HSM Backup Docks	Offsite location (other than DC and DR) in fireproof safe
2.	Master Key			Offsite location (other than DC and DR) in biometric enabled locker with dual access control

Table 21: HSM Recovery

Note: *(1) The MSI to provide separate HSMs for the production environment and other non-production environments (DC and DR), (2) The MSI should provide the production HSMs in a high availability manner, meeting specifications, performance requirements.*

5.8.2.4 VPN Access

(i) MSI shall enable remote working of Data Center staff via VPN in case the sites are physically inaccessible.

(ii) VPN facility to be kept enabled for key staff.

(iii) Key staff to run the operations from locations designated by GoSL, if data center site is physically inaccessible.

(iv) Minimal staff may be present in the Data Centers as far as feasible for on ground support.

(v) This facility could be used when movement of staff is restricted due to natural disasters such as floods, strikes, or pandemic.

5.8.2.5 Disaster Recovery Strategy and Procedures

(i) MSI shall enable recovery strategies in case of any natural or man-made disasters, including but not limited to the following:

#	Issue	Recovery Strategy
1.	One Data Center facility is down	• Alternate Data Center with 100% capacity capability • Active-Active or Active-Passive based on criticality of operations and feasibility

#	Issue	Recovery Strategy
2.	Any system component is down	• Redundancy at component level in DC • Redundancy for critical components in DR • Failover to DR in case DC is completely down or vice versa
3.	Data unavailable	• Real time replication of all critical data in DR site and vice versa • Worst case scenario if data is lost from both data centers (DC and DR), recovery shall be done from tapes stored in a third offsite location
4.	Any telecommunication link is down	• Dual path telecom connectivity • Dual Service providers • Different Telecom service providers for DC and DR • Failover to DR in case DC is completely down or vice versa
5.	People unavailable	• Critical Operations run in automated mode and will continue to run unless technical support is required • VPN facility shall be provided for key staff to enable work from home.

Table 22: Disaster Recovery Strategy and Procedures

(ii) Step by Step Recovery procedures shall be established by system integrator for various scenarios. Some of the outcomes following a disaster for which:

a. Natural Disaster resulting in physical damage to DC (DC unavailable).

b. Man Made Disaster resulting in physical damage to DC (DC unavailable).

c. Disasters affecting the movement of personnel (Staff unable to travel to DC).

d. Power unavailability.

e. Particular technology components go down resulting in unavailability of a particular process.

f. Cyber-attacks including ransomware, DDOS etc. resulting in unavailability of services.

g. Recovery from Tapes.

5.8.2.6 Retention

(i) The retention period for backup shall be in conformance with the legal and regulatory requirement of data retention like as defined in the law of the land or other applicable law/act

(ii) The retention period for backup of other data which is not defined in law of the land shall be decided by the Business Owner / Department heads and shall be reviewed by the MSI Security Head

(iii) **Daily Backup:** Core data shall be backed up on a daily basis and shall be maintained for two

weeks along with version history on unique media. No tape shall be overwritten for two weeks, including daily incremental.

(iv) **Weekly Full Backup:** Weekly backups shall include operating system data, B/R software data, content data, configuration files, registry files and application software data. Weekly data should not be overwritten for at least three months. This set of data should be considered for duplicates.

(v) **Monthly Full Backup:** Similar to the weekly full backup, the monthly activity shall include all data content and files and not be overwritten for at least 1 year. This data shall be duplicated as needed.

(vi) **Annual Full Backup:** In this case, all data and files are vaulted off-site immediately. This data must be duplicated as needed.

5.8.3 Deliverables for Information Security and Business Continuity

The overall List of deliverables for information security and business continuity are as follow.

#	Deliverable	Description	Periodicity
1.	SL-UDI SLA methodology creation	Prepare SLA measurement methodology documents for all service level agreements included in this RFP. The methodology shall include methods to measure the SLAs, tabulate, in a template, all possible measurable parameters as defined in the SLAs and provide examples using mock data for SLA calculations.	One Time (Before Go-live)
2.	SL-UDI Security and Privacy Policy review and update	Review / Augment the information security policy and privacy policy that will provide the baseline controls to be implemented across SL-UDI ecosystem. MSI is also expected to review/update (or create) security and privacy policies for ecosystem partners of SL-UDI.	**First time**: Within 3 months of Go-live. Review on an annual basis subsequently
3.	Designing of Security and Privacy Procedures	MSI shall ensure the end- to-end design/update, documentation, implementation, maintenance, and yearly update of security processes and procedures as part of their scope, compliant to the information security policy prepared by the SL-UDI, the international security standard ISO 27001, and relevant laws of land within Sri Lanka. Indicative list of processes is as follows – 1) Personnel security process 2) Physical and environmental security process 3) Process for security of SL-UDI data repository 4) Process for securing network components	**First time:** Within 3 months of Go-live. Review on an annual basis subsequently

#	Deliverable	Description	Periodicity
		5) Process for ensuring device level encryption 6) Key management process 7) Logging and auditing process 8) Processes to manage security solutions and devices 9) Access management process 10) Asset management process 11) 2-factor authentication process 12) Business Continuity and Disaster Recovery processes 13) Biometric exception process 14) Enrolment packet quality check process 15) Process for blacklisting of enrolment officers 16) Process for use of portable media 17) Process for de- duplication checks 18) Process for distribution of enrolment software 19) Patch management process 20) Secure login process 21) New installations and maintenance process 22) Change management process 23) Security incident management process 24) Secure SDLC process 25) System hardening process 26) Biometric device certification process 27) IT asset certification process: 28) Application certification/ onboarding process 29) Internal audit process ad) Application security testing process 30) User Acceptance Testing Process 31) Vulnerability assessment and penetration testing process 32) Risk assessment and treatment process	

#	Deliverable	Description	Periodicity
		33) Security aspects in API specifications 34) Security Exception Process 35) Third Party Management Process 36) Training and Awareness process 37) Data Backup and Restoration Process 38) Secure Configuration Management 39) Privacy Policy related procedures such Data Retention, Data Archival, Notice and Consent, Data Governance etc.	
4.	Minimum Baseline Security Standards (or referred as Hardening standards)	MSI shall develop, implement, and maintain version-wise hardening standards for all IT infrastructure (OS, DBs, Servers, Security solutions implemented such as Firewall, WAF, Network Devices such as Routers, Switches, Storage devices etc.) while referencing CIS benchmarking or vendor specifications for hardening. All minimum baseline security standards shall be prepared in consultation with GoSL.	**First time:** Within 3 months of Go-live. Review on an annual basis subsequently
5.	Asset management review	MSI shall design the process and implement the same to do review of asset management to validate the implementation of necessary security guidelines and measures before introduction or deployment of an asset in SL-UDI environment and make enhancements to the existing process. MSI shall also evaluate and minimize impact to other existing processes, applications, devices, etc. affected by introduction of the new asset.	**First time:** Within 3 months of Go-live. Review on a half-yearly basis subsequently
6.	Backup review	**1) Backup Processes** MSI shall review the process of backup and recovery that is being followed in SL-UDI to identify process gaps and provide recommendations as per industry best practices and shall also review the process of handling the backup tapes and backup servers. **2) Backup Drills** As part of review, MSI shall conduct periodic backup drills to check the state of backup and provide assurance of data recovery. Drill shall be conducted for all components of SL-UDI	**First time:** Within 3 months of Go-live. Review on a half-yearly basis subsequently

#	Deliverable	Description	Periodicity
		infrastructure including but not limited to databases, applications, application and device configurations, etc.	
7.	Incident management review	MSI should analyze and report the incidents logged by the SOC and conduct analysis to try to identify any patterns or trends. The scope of the exercise shall include but not limited to average time to fix an incident, percentage of incidents resolved, quality of tickets, quality of root causes documented, incidents due to SLA Violations, Source of incident detection, Incident fix type (permanent fix, workaround), Number or percentage of incidents converted into problems, Open incidents by – partner ecosystem, process, and technology, time it is open, expected time to closure, business impact, and criticality among others.	During operations and maintenance phase on a quarterly basis
8.	BCP-DR	**a) BCP/DR strategy and plan** MSI shall assess compliance to BCP/DR policies and adherence to BCP procedures. **b) BCP/DR testing** MSI shall study the BCP/DR test plan and ensure the various tests and drills are conducted as per the defined procedures.MSI shall conduct end to end BCP/DR testing and perform a number of activities including but not limited to scope document review, conduct pretest and post-test calls with various owners, review the DR drill conducted and ensure its effectiveness.	**First time:** Within 3 months of Go-live. Review on a half-yearly basis subsequently
9.	Internal security audit	MSI is required to perform the detailed internal audit covering end-to-end activities of SL-UDI ecosystem. MSI shall develop yearly plans for internal security audit and vulnerability assessment. MSI shall identify the systems, applications, and processes, to be covered under internal audit activities and prepare a plan for the same. Additionally, MSI shall implement corrective and preventive actions for non-compliance observed and plan and implement new information security tools authorized by SL- UDI management. The audit will be carried out only after the audit plan	**First time:** Within 6 months of Go-live. Review on a half-yearly basis subsequently

#	Deliverable	Description	Periodicity
		will be approved by SL-UDI. Internal audit scope shall include security policy, procedures, ISO 27001 standard and regulatory compliance requirements as well.	
10.	Risk assessment methodology design/review	Risk Assessment Methodology Design and update a document to define how the risk assessment would be conducted for the SL-UDI ecosystem and the subsequent steps for the same. Risk assessment methodology shall identify the steps that must be taken to effectively manage risk: identify, analyze, plan, track, control, and communicate Risk methodology. MSI shall refer to international standards such as ISO 31000, 27005 for risk assessment processes.	**First time:** Within 3 months of Go-live. Review on annual basis subsequently
11.	Risk assessment and treatment plan	Risk assessment and treatment plan of all SL-UDI processes - MSI shall assess risk within the SL-UDI ecosystem. The results should guide and determine the appropriate management action and priorities for managing information security and privacy risks and for implementing controls selected to protect against these risks. MSI shall also develop and drive risk treatment plans that will mitigate risks within the ecosystem. For those risks where the risk treatment decision (in consultation with SL-UDI) is to apply appropriate controls, these controls should be selected and implemented by MSI to meet the requirements identified by risk assessment. a) Risk Assessment - Risk Assessment shall involve identification of information security risks that may have an adverse impact on the SL-UDI business processes and analysis of these risks to determine the likelihood of occurrence and its consequences on SL-UDI's operations. It will involve identification, assessment and management. b) Risk Treatment- Provide a comprehensive set of recommendations/ steps to mitigate the risks to ensure the risks in the SL-UDI ecosystem are reduced by doing continuous follow with the relevant business owner/process owners	**First time:** Within 6 months of Go-live. Assessment on annual basis subsequently

#	Deliverable	Description	Periodicity
12.	Risk register	**Risk Register** The assessment should be reported and identified risks should be stored in a "risk register" which is a central repository for maintaining all known risks in the SL-UDI ecosystem	**First time:** Within 6 months of Go-live. Assessment on annual basis subsequently
13.	Data Leakage Prevention (DLP) and End Point Detection Response (EDR) review	MSI shall review the implementation of DLP and EDR solution including but not limited to integration process followed to integrate more than 4000+ servers and endpoints and monitor all the integrated devices. MSI shall also review the process to investigate the alerts generated by DLP and EDR solution and process to respond to the incidents detected.	During operations and maintenance phase on a quarterly basis
14.	Vulnerability assessment and penetration testing before go-live	Vulnerability assessment of applications, servers, network, security devices etc. before go-live - Vulnerability assessment of all IT assets should be carried out before go-live. MSI shall discover the live hosts, take IP range from GoSL every quarter and take information from asset management database to identify the scan range. MSI shall also provide vulnerability closure for the vulnerabilities as per the Vulnerability Management process before Go-Live of any component.	Before Go-live of applications, servers, network, security devices etc.
15.	Design of fraud management process	MSI shall review and monitor the Fraud Risk Management (FRM) process to identify and address the Risk within the processes of SL-UDI and its ecosystem partners. MSI is required to create, update and finalize a Fraud Risk Management process in- consultation with SL-UDI. MSI shall ensure that an adequate fraud risk management program is in place, including a written policy (or policies) to convey the expectations of the board of directors and senior management regarding managing fraud risk.	One Time (Before Go-live)
16.	Review and enhancement of existing	Indicate list of activities include - a) Fraud risk exposure should be assessed periodically by MSI to identify potential	During operations and maintenance

#	Deliverable	Description	Periodicity
	fraud rules	schemes and events that needs to be mitigate. MSI shall take steps to mitigate the same. b) MSI shall review and validate the effectiveness of prevention techniques to avoid potential key fraud risk events and ways to mitigate possible impacts. c) MSI shall review and validate the effectiveness of Detection techniques to uncover fraud events when preventive measures fail, or unmitigated risks are realized. d) MSI shall review the investigation and corrective action methods used for addressing potential fraud in an appropriate and timely manner e) MSI shall recommend based on leading practices in fraud management. f) Identify frauds in Enrolment and authentication and revise fraud rules accordingly	phase on a quarterly basis

Table 23: Deliverables for Information Security and Business Continuity

5.8.4 Support (Contact Center and Helpdesk)

5.8.4.1 Contact Center Setup and Administration

(i) The SL-UDI Information System will require a Contact Center which will be facilitated by GoSL. The Contact Center shall act as a citizen and partner touchpoint and provide resolution of queries of residents and Ecosystem Partners regarding SL-UDI services, Enrolment services, Authentication services, Trusted Service Providers (TSP) and User Agency (UA) related queries, etc.

(ii) GoSL will provide a toll-free number for the Contact Center and will bear the operational cost of this number.

(iii) GoSL shall provide physical space for the contact center along with necessary Electrical (Power Supply, Wiring, Power Sockets, Lights, etc.) and Physical Infrastructure (Tables, Chairs, etc.).

(iv) MSI will be required to provide necessary IT (Hardware, Software, Network) and Non- IT Infrastructure (Communication Equipment such as EPBX, IVR, Dialer, Telephones, Headsets, etc.).

(v) MSI will be responsible for supplying and implementing Customer Relationship Management (CRM) software to support Contact Center Agents / GoSL Officials at the Contact Center.

(vi) GoSL will also be required to maintain the infrastructure provided at the Contact Center for a period of entire contract.

(vii) The GoSL will provide necessary manpower i.e., supervisors and contact center agents to run the Contact Center. The MSI will be responsible to train the aforementioned manpower for the resolution of citizen and partner queries.

(viii) GoSL shall be responsible for ensuring that the infrastructure provided by it is operational from 8 AM – 6 PM for Monday to Saturday excluding government holidays.

(ix) The contact center will provide support in Sinhalese, Tamil, and English languages.

5.8.4.2 Deployment of CRM Solution for Contact Center Operations

Scope of work for deployment of CRM solution has been given in Section 5.1.3.2

5.8.4.3 Deployment of Infrastructure for Contact Center Operations

(i) GoSL will provide PRI lines and a toll-free number for the Contact Center and will bear the operational costs of these items.

(ii) GoSL shall provide physical space for the Contact Center along with necessary IT, Electrical and Physical Infrastructure as follows:

a. Premises & Furniture

b. Required floor space

c. Lighting

d. Basic amenities e.g., water facilities

e. Power connection

f. Standard fire-fighting systems

g. Cubicles, chairs, cabinets, etc. constructed / provided to suit a typical Contact Center

h. Network Connectivity between Contact Center and DC, and Contact Center and DR

(iii) MSI should provide recommendations for GoSL to establish the Contact Center with requisite IT and other Infrastructure to support the project requirements.

(iv) MSI should integrate CRM, Contact Center Software, Ticketing System, Helpdesk and other integrations with DC/DR.

5.8.4.4 Other responsibilities of MSI for Contact Center Operations

(i) MSI should assist GoSL in preparing a detailed plan for setting up of Contact Center Operations with timelines and activities.

(ii) Training is an important aspect of the Contact Center agents. The MSI should impart proper training in soft skills like call handling, exposure to related applications etc. so as to prepare the customer service executives to attend to incoming calls effectively. MSI shall also prepare the required training material.

(iii) MSI shall prepare standard operating procedures of contact center including call handling processes, quality assurance and escalation management.

(iv) MSI will extend all the required support to GoSL during their Random or Regular audits of the contact center operations and contact center facilities.

(v) Disaster Recovery and Business Continuity: The MSI shall ensure proper procedures are established for Contact Center systems in the event of a disaster to protect and ensure

continuation of Contact Center services.

5.8.4.5 Reporting

(i) MSI shall support MSP to generate standard reports to measure/verify various KPIs, to monitor the performance of agents, etc.

(ii) MSI shall support MSP to prepare and submit reports to GoSL as per the mutually agreed reporting structure. These reports shall include but not limited to the following:

a. Incident, devices, and system logs/ security logs (category, severity, and status of call etc.)

b. Incidents escalated

c. SLA compliance/non-compliance report

d. Problem Management

e. Key learning from similar previous experience

f. Escalation procedure for handling significant issues

g. Contact Center staffing

(iii) MSI, MSP and GoSL will mutually agree on the format of the reports. At minimum the following reports may be necessary:

a. Reports based on time period

b. Type of grievances/queries/demand/analysis

c. Repeat request or complaints analysis.

d. Call waiting time.

e. Lost calls

f. Call time (Average Talk Time/Hold Time/Handle Time)

g. Hourly call details

h. Complaints pending for more than the defined time period.

i. Calls Handled

j. Abandoned Call Rate

k. Delay Before Abandon (Average/Longest)

l. Staffing related Report

m. Other monthly MIS, SLA reports, number of agents logged in.

5.8.4.6 Monitoring

(i) MSI shall train MSP to extend all the required support to SL-UDI team for monitoring and accessing all subsystems and records pertaining to contact center operations for GoSL.

(ii) MSI shall be responsible for assisting the SL-UDI officials in monitoring the contact center agents and operations.

5.8.4.7 Key features of the proposed Contact Center

The key features of the proposed Contact Center are enlisted in the table below:

No. of Seats	12 seats (Year-1 and Year-2) 10 seats (Year-3)
Languages supported	Sinhalese, Tamil, and English
Operations	• 6 days a week (Monday – Saturday) • 8:00 AM to 6:00 PM
Accessibility	Accessible through a Toll-Free Number, IVR Solution
Quarterly Review	Half-Yearly review of call volumes and number of seats required to provide services
Offsite/Onsite	Onsite at premises provided by GoSL
Features	The Contact Center should include mechanism of calls, email, chat, chatbot, voice over IP (VoIP) and website support. Note: Chatbot should be trained to answer questions and should learn based on the responses provided and other knowledge bases.

Table 24: key features of the proposed Contact Center

An illustrative list of queries and grievances that may be posted with the SL-UDI Contact Center is given in Section 5.8.5.8 to assist the MSI in understanding the nature of support to be provided using the CRM solution.

5.8.4.8 Sample Queries at the Contact Center

An illustrative list of queries and grievances that may be posted with the SL-UDI Contact Center is given below to assist the MSI in understanding the nature of support to be provided using the CRM solution.

Queries (Sample)	Queries (Sample)
General – Queries/Grievances of Citizen for Enrolment • Where can I register • How to book an appointment • Can I reschedule the appointment? • What documents are required for enrolment/update • Is there any fee for enrolment / update? • What is the status of my enrolment? • My enrolment has been rejected, what should I do • How to update my demographic details	General – Queries/Grievances of Ecosystem Partner • I want to register myself as TSP/UA • What is the application procedure, timelines and documents required? • Whom do I contact for registration? • Authentications are not working • E-KYC is not working • OTP is not being received • Which authentication devices should

Queries (Sample)	Queries (Sample)
• How to update my biometric details • At what age, can my child register • I do not have NIC, what should I do • Do I need to take pre-enrolment slip for enrolment? • I have lost my pre-enrolment slip, what can I do	I use? • What is the procedure for registration of authentication devices? • What is the virtual identity, can I use it
General – Queries/Grievances of Enrolment Officers • I am unable to login • I am unable to download pre-enrolment information • My enrolment software is not working • My enrolment kit is not working • I cannot upload the enrolment packet • My enrolment software is not allowing me to enroll more residents • I am unable to capture biometrics • What to do when citizen has problem with quality of biometrics or missing fingers	General – Queries/Grievances of Residents for Authentication • How can I generate my virtual ID? • How can I lock/unlock my biometric? • Can I change my PIN? • I have lost my PIN, and I cannot authenticate • I cannot authenticate despite repeated attempts • I have received an alert of authentication/ e-KYC

Table 25: Sample Queries at the Contact Center

5.8.5 IT Helpdesk

A key requirement is the setting up of and operating a National Integrated Service Desk (UDI-SD) for SL-UDI. The envisaged IT Helpdesk shall operate a 24x7 center to handle end user (can be internal users of SL-UDI or other users involved in SL-UDI Field Operations) queries and service requests, which may be in the form of an omnichannel interface (call, email, online ticket, paper, etc.).

The MSI will operate a 7x24 hour IT Help Desk for management of data center and IT infrastructure, functionality, and performance issues. The MSI shall not allow any service request to go unresolved due to lack of ownership or lack of coordination with other support teams. The MSI shall:

(i) Staff the service desk with technically qualified system admin, application, IT infra and Biometric specialists in two shifts 24*7.

(ii) Respond and resolve all incidents and issues reported to the IT Help desk and,

(iii) Support requests to troubleshoot application, security, connectivity, and performance issues which may be related to the infrastructure.

The objective of IT helpdesk is to provide issue log and issue resolution pertaining to SL-UDI Software System, Field Hardware and SL-UDI DS, Security Operations, Network Operations, BSP team etc.

MSI shall be accountable and responsible for all the proposed components and shall adhere to the Service

Level Agreement provided as part of the RFP.

The helpdesk manpower will leverage the Incident Management module of EMS (supplied by MSI as part of this engagement) to achieve the intended objective. The helpdesk should be integrated with CRM.

5.8.5.1 Helpdesk Setup and Operations

(i) MSI shall be responsible for setting up an IT helpdesk operation to support IT issue resolution.

(ii) MSI shall operate and maintain the IT Helpdesk according to ITIL standards.

(iii) MSI shall deploy CRM software / Incident Management module of EMS for the helpdesk which shall be accessible to limited users (maximum 10) of the SL-UDI application for logging issues.

5.8.5.2 Deployment of Infrastructure for IT helpdesk

(i) GoSL will provide physical space for the IT helpdesk along with necessary IT, Electrical and Physical Infrastructure as follows:

a. Premises & Furniture

b. Required floor space

c. Lighting

d. Basic amenities e.g., water facilities

e. Power connection

f. Standard fire-fighting systems

g. Cubicles, chairs, cabinets, etc. constructed / provided to suit a typical IT helpdesk

h. LAN connectivity

(ii) MSI should ensure that the IT helpdesk has the requisite IT and other Infrastructure to support the project requirements. MSI shall be required to provide and maintain all IT required for successful operations of the IT helpdesk including, but not limited to, the following:

a. Hardware such as Desktop/Laptop, Monitor, etc.

b. Software such as helpdesk software, computer telephony interface connector to integrate helpdesk.

c. Network Connectivity between IT helpdesk and DC, and IT helpdesk and DR

d. Automatic Call Distributor (ACD) for distribution of incoming calls to IT helpdesk staff as they are received. MSI shall be responsible for installation of the ACD. ACD should have at least the following features:

- System should be able to intelligently route the callers to IT helpdesk staff based on their specialization and availability

e. Integrate Ticketing System, Helpdesk, Contact Center, other integrations with DC/DR.

(iii) MSI will be responsible for integrating the infrastructure provided by GoSL with infrastructure provided by MSI to make the IT helpdesk operational

(iv) The MSI is expected to provide infrastructure for IT helpdesk. In case the GoSL requires infrastructure related to additional seats, the GoSL may place separate order for relevant infrastructure for additional seats with MSI on the rates provided in the commercial bid.

5.8.5.3 Training to Helpdesk Manpower

(i) For details about L1, L2 and L3, please refer to Section Support Mechanism– 5.11.2

(ii) MSI should make arrangements for imparting proper training in soft skills, call handling, exposure to related application, required technical skills to the current IT Help desk of GoSL at the time of actual transfer to MSP. In case GoSL wants to associate its IT Help Desk persons, the MSI will facilitate after assessment and will deploy them in IT Help desk in consultation with GoSL.

5.8.5.4 Set up IT Infrastructure for Helpdesk Operations

MSI shall arrange for the associated hardware, software, and network components for operationalizing the IT Help Desk.

(i) Help Desk application (CRM or Incident Management Module of EMS solution):

a) MSI would provide and implement a comprehensive IT Helpdesk application using the CRM or Incident Management module of the EMS solution. The license of the Helpdesk application shall be in the name of the GoSL.

b) The application shall support IVR, Teplephone Email, letter and Web based complaint lodging, resolution, and response features using channels such as Telephone , SMS, Email, and Web.

c) IT Helpdesk application shall record all incidents as service requests.

d) The IT Helpdesk application would maintain a complete incident history of all incidents recoded at the IT Helpdesk.

e) IT Helpdesk application should provide workflow and hierarchy through which each incident should move based on Incident severity, classification, and owner.

f) IT Helpdesk application should log the calls

g) IT Helpdesk application shall capture all the relevant information of incident logger, incident under consideration etc.

h) IT Helpdesk application should be integrated with the CRM solution and EMS solution as the case may be.

5.8.5.5 IT Helpdesk operations

IT Helpdesk would have following major activities and tasks:

(i) Log incidents/issues as service requests and provide a unique service request number. Acknowledgement should be sent to user along with service ticket number through an email immediately on issue logging. All issues logged should be assigned a severity level (L1/L2 or L3). Indicative severity level definitions are given below:

Severity	Definition

L1	L1 problems could have any of the following characteristics: • No impact on processing of normal business activities. • A low impact on the efficiency of users • Has a simple workaround • Enhancement requests
L2	L2 level problems are the ones which have a significant business impact. These problems could have any of the following characteristics: • The efficiency of users is being impacted • Has a viable workaround • Severely degraded performance (slow service)
L3	L3 problems could have any of the following characteristics: • Entire or part of any service unavailable (including APIs) • Incorrect behavior of the system (wrong calculations, etc.) • Security Incidents • Data Theft/loss/corruption • Severe impact on customer satisfaction • No work-around to mitigate the disruption in service • Repeat calls (same problem that has occurred earlier reported more than 2 times)

Table 26: Level Definition

(ii) The Helpdesk staff shall have provisions through the application for coordinating with concerned MSI in case issues are pertaining to any external entity product/support like:

a. Respective OEM team

b. DC/DR Support Team

c. Network Provider

d. End User Devices support provider

(iii) MSI shall analyze L3 level incidents and provide a root cause analysis report on a periodic basis for all the recurring incidents. MSI shall ensure that resolution is provided for these problems by respective technical teams to prevent further issues due to the same cause. The report for the same should be submitted to GoSL.

(iv) Escalate the issues/complaints, if necessary, as per the escalation matrix of MSI.

(v) Notifying users, the problem status and resolution through the tickets over email or SMS or both.

(vi) Each service request would have a unique service request number.

(vii) It is the responsibility of MSI to ensure the quality of the IT Helpdesk.

(viii) All incidents should be recorded. These records shall be retained on hard disk for 30 days for

easy retrieval.

(ix) Incidents which are not meeting SLAs, and which are exceptional in nature (highly critical, wider spread etc.) shall be escalated as per defined escalation matrix.

(x) IT Helpdesk should comply with SLAs applicable to them as mentioned in this RFP. Non-adherence to SLAs shall result in imposition of penalty (liquidated damages).

(xi) MSI shall prepare and submit reports to MSP/GoSL as per the mutually agreed reporting structure.

From the biometric solution perspective (except biometric capture devices), for L1 support the BSP should either choose to utilize its administrator for this function or propose a separate manpower, and the L2 and L3 support is expected to be provided offsite. In case of L3 ticket, the following process will be adopted:

a. BSP will classify the issue as Critical or Non-Critical

b. BSP will undertake troubleshooting and communicate the estimated resolution time to the MSI

c. BSP shall inform the estimated resolution time to GoSL.

d. For critical issues, the BSP will provide a work around solution as soon as possible in agreed timeline

e. For all issues, the MSI will provide a resolution solution in timeline as per SLA.

5.8.5.6 Reporting

(i) MSI should generate standard reports to measure/verify various service level(s), to monitor the performance of agents, etc.

(ii) MSI shall prepare and submit reports to GoSL as per the mutually agreed reporting structure. These reports shall include but not limited to the following:

a. Incident, devices, and system logs/ security logs (category, severity, and status of call etc.)

b. SLA compliance/non-compliance report

c. Helpdesk staffing

(iii) MSI and GoSL will mutually agree on the format of the reports to be submitted to GoSL.

(iv) MSI should extend all the required support to SL-UDI team for monitoring and accessing all subsystems and records pertaining to helpdesk operations for GoSL.

(v) MSI shall be responsible to assist the SL-UDI officials in briefing of the helpdesk agents and operations.

5.9 Security and Network Operations

5.9.1 Security Operations (Complying with SOC-2 standards)

5.9.1.1 SOC Setup

Note: GoSL will provide the location, utilities, LAN network, furniture, and desks

MSI may refer to Section 5.8.1.3 which provides a list of security components required for implementing security solutions and security operations centers. The MSI is required to setup the SOC for which physical space will be provided by GoSL. The MSI will be responsible to integrate all required components with the SOC to ensure security operations work in the desired manner. The

responsibility of the MSI include the following:

(i) Define objectives, key activities, technical and physical controls of SOC

(ii) Design security operations model including detailed technical design

(iii) Undertake integration of tools and infrastructure architecture and prepare a process for reporting requirement

(iv) Provide, Implement and Integrate the SOC IT Infrastructure.

(v) Manage events log, events, incidents and operations of SOC

(vi) Deploy adequate manpower to provide 24x7 SOC services

MSI shall develop and implement formal security event reporting and escalation processes, distinct roles and responsibilities for management of security events, and a continual improvement process. MSI shall ensure management of security incidents, inclusive of incident classification, and incident closure. MSI shall establish a security exception management process. MSI shall identify and report information security exceptions against security policies and processes.

An indicative manpower for SOC is provided below, the MSI should do its own analysis, design and estimation of arrive at the number of manpower required:

(i) Analysts – 2

(ii) Technical Manager – 1

(iii) Supervisor - 1

(iv) Total - 4

An indicative bill of material for SOC related items is provided below, the MSI should do its own analysis, design and estimation of arrive at the number of components required:

#	Component
1.	Desktops / Monitors including Keyboard & Mouse

Table 27: Indicative Bill of Material for SOC

5.9.1.2 SOC Services

SOC administration services will provide L1, L2 and L3 support services for security monitoring of the infrastructure. L1 services will comprise of monitoring, L2 services will comprise of validation of incidents and SIEM management and L3 activities will cover supervision of the SOC team.

As part of security operations below are the indicative set of activities that will be performed as part of SOC operations are provided in table given below:

Level	Services
Level 1 support services will comprise of monitoring and incident identification	• Detect Incidents by monitoring the SIEM console, Rules, Reports and Dashboards. • Monitor the SIEM console resources to identify any anomalies. • Report the incident to the concerned team along with the SOC. • Escalate the incident whenever the SLAs are not met.

Level	Services
	• Monitor the health of the SIEM tool. • Communicate with external teams in proper incident resolution
L2 support activities will comprise of incident validation and SIEM management	• Validate the Incidents reported by L1. • Escalate timely when the SLA for alerting is not met. • Identify the incidents if there are any missed by L1 • Interact with external parties to resolve the queries relating to the raised incidents. • Manage the SIEM, incidents knowledge base. • Generate the daily reports, weekly reports, and monthly reports on time. • Maintain the timely delivery of reports. • Maintain the updated and latest log baselines
L3 support activities will comprise of SOC supervision and management	• Manage the security response processes and procedures • Conduct advance analysis of security incident and prepares the remediation advisory after performing impact analysis, attack projection and reclassification of security incident • Recommend use case improvements • Identify relevant threat feeds to enhance threat detection and response • Design and coordinate responses to security events • Perform security testing and build security utilities and tools • Derive functional requirements • Manage SOC system architecture and realize SOC infrastructure • Coordinate major incidents at SOC infrastructure level (application and use case related) and invoke application recovery plan or reactive disaster recovery plan for SOC infrastructure • Accept and prioritize problem • Plan, accept and verify change implementation • Operate and monitor infrastructure services, manage event, capacity, and availability issues

Table 28: part of SOC operations

Note: MSI shall provide access to logs to GoSL

5.9.2 Network Operations

5.9.2.1 NOC Setup

Note: GoSL **will provide the location, utilities, LAN network, furniture, and desks**

The MSI is required to setup the NOC for which physical space will be provided by GoSL. The responsibility of the MSI include the following:

(i) Define objectives, key activities, technical and physical controls of NOC

(ii) Design network operations model including detailed technical design

(iii) Undertake integration of tools and infrastructure architecture and prepare a process for reporting requirement

(iv) Provide, Implement and Integrate the NOC IT Infrastructure.

(v) Manage events log, events, incidents and operations of NOC

(vi) Deploy adequate manpower to provide 24x7 NOC services

MSI shall develop and implement formal network event reporting and escalation processes, distinct roles and responsibilities for management of network events, and a continual improvement process. MSI shall ensure management of network incidents, inclusive of incident classification, ~~BIA~~, and incident closure. MSI shall establish a network exception management process. MSI shall identify and report information network exceptions against policies and processes.

5.9.2.2 NOC Services

NOC administration services will provide L1, L2 and L3 support services for network monitoring of the infrastructure. L1 services will comprise of monitoring, L2 services will comprise of validation of incidents and network monitoring tools management and L3 activities will cover supervision of the NOC team.

As part of network operations below are the indicative set of activities that will be performed as part of NOC operations are provided in table given below:

Level	Services (Indicative)
Level 1 support services will comprise of monitoring and incident identification	• Detect Incidents by monitoring the network monitoring tool console, Rules, Reports and Dashboards. • Monitor the console resources to identify any anomalies. • Report the incident to the concerned team along with the NOC. • Escalate the incident whenever the SLAs are not met. • Monitor the health of the NMS tool. • Communicate with external teams in proper incident resolution.
L2 support activities will comprise of incident validation and NMS management	• Validate the Incidents reported by L1. • Escalate timely when the SLA for alerting is not met. • Identify the incidents if there are any missed by L1 • Interact with external parties to resolve the queries relating to the raised incidents. • Manage the NMS, incidents knowledge base. • Generate the daily reports, weekly reports, and monthly reports on time.

	• Maintain the timely delivery of reports. • Maintain the updated and latest log baselines
Level 3 support activities will comprise of NOC supervision and management	• Manage the network incident response processes and procedures • Conduct advance analysis of network incident and prepares the remediation advisory after performing impact analysis, attack projection and reclassification of network incident • Recommend use case improvements • Identify relevant threat feeds to enhance threat detection and response • Design and coordinate responses to network events • Perform network testing and build utilities and tools • Derive functional requirements • Manage NOC system architecture and realize NOC infrastructure • Coordinate major incidents at NOC infrastructure level (application and use case related) and invoke application recovery plan or reactive disaster recovery plan for NOC infrastructure • Accept and prioritize problem • Plan, accept and verify change implementation • Operate and monitor infrastructure services, manage event, capacity, and availability issues

Table 29: NOC operations

5.10 Business and Technical services

5.10.1 Business Services

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

5.10.1.1 Impact Assessment for initial rollout

MSI is expected to undertake an impact assessment exercise to identify process, technology, and operation issues of SL-UDI System. MSI shall closely monitor the initial roll-out in order to find any improvement areas in the SL- UDI Information System, process of enrolment and operations of enrolments and delivery of service.

*V. **Methodology of Impact Assessment***

MSI may follow the following to undertake impact assessment:

(i) **Discussion with Key Stakeholders:** MSI may undertake interviews, focused group discussions with key stakeholders such as enrolment operators, users etc. to identify areas of improvement in the SL-UDI Information System and its operations

(ii) **Discussion with the System Users:** MSI shall undertake a discussion of GoSL staff who are working on the SL-UDI Information System to identify software bugs, enhancements,

potential improvement areas etc. MSI shall consolidate the survey result and categorize the inputs into current software issues, must have improvement areas and potential improvement areas.

(iii) **Assessment of Reports:** MSI shall generate and analyze the reports on enrolment, authentication and e-KYC to identify the transaction volumes, time for each transaction etc.

MSI shall be responsible for impact assessment including, but not limited to, the following activities:

(i) Identify and record all system issues.

(ii) MSI is expected to monitor and measure the end-to-end time taken from enrolment stage till the generation of SL-UDI Number. In other words, this process should identify the time taken for processing one enrolment packet.

(iii) During impact assessment, the MSI is expected to monitor the enrolment and authentication activities. MSI is expected to:

a. Present a report on the quantity of daily enrolments. The report should include the number of enrolments requested, number of requests processed, number of requests which failed, along with the reason for failure, time taken to process such requests.

b. Present a report on quantum of authentications. The report should include the number of authentications requested, number of requests processed, number of requests which failed, along with the reason for failure, time taken to process such request.

c. Present a report on quantum of e-KYC requests. The report should include the number of e-KYC requested, number of requests processed, number of requests which failed, along with the reason for failure, time taken to process such request.

(iv) Provide fortnightly report on the number of enrolments, authentications etc.

VI. ***Outcome of Impact Assessment***

(i) Create a final impact assessment report to record all issues, resolutions, learnings, improvement areas etc. gathered during the impact assessment exercise.

(ii) Enhanced SL-UDI Software System

(iii) Identification of process and operations issues and improvement areas

5.10.1.2 Enrolment Services

Enrolment is one of the key services under the SL-UDI program. In this service, the citizens are enrolled in the SL-UDI program using the enrolment kit at the enrolment center and using mobile enrolment kits. The support in enrolment covers the following aspects:

I. Field services related to enrolment

a) Monitoring of maintenance of Enrolment Kit: The solution utilized for the purpose of enrolment may need to be maintained to ensure it is fit for performing enrolment. The services may include hardware maintenance/replacement, software upgrades, patches, etc. The MSI will be responsible to monitor the maintenance performed by the MSI for enrolment kits

II. Enrolment Processing

b) Quality Assurance: The services of assuring quality of enrolments including sampling. The

GoSL will provide its manpower and MSI will be required to train this manpower.

c) **Manual Adjudication:** The enrolments flagged during the biometric deduplication may undergo a manual process of adjudication where authorized officers may re-verify the results of automated matching. The GoSL will provide its manpower and MSI will be required to train this manpower.

d) **Biometric exception process:** MSI shall assist GoSL to develop and implement processes to capture biometric exceptions for residents who are unable to provide fingerprints or any other biometrics, owing to reasons such as injury, deformities, or any other relevant reason. The GoSL will provide its manpower and MSI will be required to train this manpower.

e) **Enrolment packet quality check process:** MSI shall assist GoSL to develop processes and undertake quality check for enrolment packets which will contain citizen Personal Identifiable Information (PII) such as biometric and demographic information. The GoSL will provide its manpower and MSI will be required to train this manpower.

III. Other enrolment related services

a) **Maintenance of Enrolment Software:** The software utilized for the purpose of enrolment may need to be revised to accommodate changes and improvements. The improvements may be related to location dictionary, name dictionary, performance upgrade, etc. The changes or maintenance may be related to bug fixes, renewal of encryption certificate, new OS support, new device support, etc.

b) **Training of Enrolment Manpower:** The training of enrolment officers and support staff is an important part of the enrolment operations to ensure good quality of enrolment.

5.10.1.3 Service Delivery

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

(i) **On-boarding of Trusted Service Provider**: The service of on-boarding the TSP involves administrative procedure, technical integration support, compliance audit, maintenance of secure keys for data exchange, etc.

(ii) **On-boarding of User Agencies**: The service of on-boarding the UAs involves administrative procedure, technical integration support, compliance audit, maintenance of secure keys for data exchange, etc.

(iii) **Registration of Devices**: The service of maintaining and updating the list of registered devices for all the UAs.

5.10.1.4 Ecosystem Partner Management

VII. ***Enablement of Partners for Enrolment***

The management of ecosystem will be driven by the Enrolment Partner Management Module of the Web Portal (Partner Management). The major activities of the MSI in enablement of partners for enrolment would be as follows:

(i) Creation of users for SL-UDI officials.

(ii) Conduct training for users of SL-UDI officials on the Enrolment Partner Management Module.

(iii) Definition of a proper working protocol with the partners including definition of roles and responsibilities between the SL-UDI and the ecosystem partners to ensure proper understanding of operations.

*VIII. **Enablement of Partners for Authentication Services***

The key activities of MSI with respect to the authentication services partner on-boarding would involve the following:

(iv) Provide handholding and guidance to the ecosystem partners in order to enable them to setup adequate facilities and IT infrastructure for leveraging authentication services.

(v) Drafting of sample Memorandum of Understanding (MoUs) for the authentication service partner i.e., TSP and UA. The MoUs should set out the expectations and intentions of both the parties for collaboration and for facilitation of subsequent agreements and documents for working with SL-UDI

(vi) Create manual related to standards, processes, and procedures to help SL-UDI officials and Partners for the on-boarding.

(vii) Providing relevant data capture Application Programming Interfaces (APIs) and technical support.

(viii) Addressing and resolving any queries and concerns pertaining to on-boarding by the ecosystem partner.

(ix) Facilitating the registration and specifications of authentication devices on make, model and specifications and making the details available on the relevant portal for the partners.

(x) Providing relevant reports to SL-UDI officials through SL-UDI Information System to ensure a consolidated, single-view, integrated reporting of performance of the authentication service partners.

*IX. **Process for Enrolment Services Management***

This section details the process and services to be provided by the MSI. MSI's scope of services shall cover the following stages of On-boarding:

- Step 1: Setup and preparation
- Step 2: Enrolment Software support
- Step 3: Preparation of manual, trainings, processes, etc.
- Step 4: De-duplication and SL-UDI number generation

The key activities of MSI in each of these steps are outlined below.

(i) *Step 1 – Enrolment center setup and preparation*

a. Provide "Train the Trainer" training for Enrolment officers and administrators.

b. Integrate the Public Key of the GoSL in Enrolment Software.

c. Assist in enrolment and PIN generation of the administrative users of GoSL.

d. Create the administrative users of the GoSL.

e. Contact Center and Technical Support – Provide technical support to the Enrolment Administrator and associated Enrolment Officer.

(ii) ***Step 2 – Enrolment Software Support***

a. Monitor first-time client software installation at enrolment center and provide issue resolution, where necessary. This will also include installation, testing, and integration.

b. Perform setup of Enrolment Administrators (ETA) and send confirmation back to enrolment center on completion of setup through the Admin Portal.

c. Provide patches/updates to Enrolment software.

d. Provide technical support to GoSL to enable them to establish connectivity with the SL-UDI technology solution.

(iii) ***Step–3 - Data Receipt and Pre-ABIS Quality Checks***

a. MSI will provide access to the MOSIP compatible enrolment packet upload mechanism (e.g. SFTP) to the enrolment center.

b. MSI shall be responsible for analysis of data quality and identifying frequently occurring issues. MSI shall communicate these specific issues of enrolment data quality to GoSL and provide recommendations where possible on solutions for mitigating the data quality issues. Where necessary, MSI shall report any unnatural or fraudulent activities on the Enrolment Software and suggest remedial measures to the SL-UDI.

c. MSI shall deliver data quality reports to GoSL.

(iv) ***Step–4 - De-duplication and unique identity generation***

a. MSI shall assist the SL-UDI officials in manual adjudication.

(v) ***Management of Master Data and Profiles of GoSL, Operators and Enrolment Officers:***

a. MSI shall create a master database with detailed profiles and contact information of enrolment centers, and Enrolment Administrators & Officers.

b. MSI's scope will include addition, modification and deletion of profiles including associated status changes of each profile.

(vi) ***MSI shall also assist in creating MIS reports and dashboards for monitoring enrolment activities.***

(vii) MSI shall develop and maintain the Technical Manual to assist in on boarding of enrolment centers.

5.10.1.5 Authentication Services Management

(i) MSI is expected to design the authentication solution for the purpose of implementation of SL UDI System.

(ii) Unique identity-based authentication services would be one of the main services of SL-UDI

System. It is expected that GoSL would appoint TSP and User Agencies (UA) in Sri Lanka for unique identity-based authentication services. It is expected that the GoSL and its nominated agency would be one of the first TSP and UA for using authentication services. This section outlines key responsibilities of the MSI for authentication services management and providing support to UA.

(iii) MSI Shall be responsible for developing the Unique Identity - Authentication Services Implementation Framework which will be a document comprising set of standards, processes, protocols and specification of authentication devices. The various entities involved in authentication are:

(i) **Citizens and Residents of Sri Lanka** - Beneficiaries who have been issued a unique identity and need to authenticate in order to avail a service.

(ii) **Terminals –** Terminal devices are devices employed by the TSP and UA in both the government and the private domains. These devices would have to be registered by the MSI

(iii) **User Agencies (UA) –** An organization or entity representation TSP for using unique identity-based authentication. These may be Government Departments, Social Sector Agencies, etc.

(iv) **Trusted Service provider (TSP) –** Entities proposed to be engaged that shall provide authentication services to various UAs.

The MSI shall be responsible for the following:

(i) Manage the authentication activation request from respective TSPs and UAs: MSI shall be responsible for performing all necessary coordination with the respective UA to ensure that the authentication activation request is completed in a timely fashion.

(ii) In case GoSL decides to make authentication services a paid service, the revenue generated from such services shall be electronically collected through a payment gateway.

(iii) Collection, billing, and accounting of authentication fees shall be undertaken by the GoSL as per the rules of Government of Sri Lanka. The process, role, and responsibility of MSI in this regard will be finalized in consultation with GoSL and the scope and terms & conditions including finance shall be decided mutually.

(iv) The authentication services shall be provided from the authentication solution outside the ABIS system. MSI shall be responsible for maintaining the authentication solution as per the service levels defined in this RFP.

(v) GoSL may appoint more than one service provider called as “Trusted Service Provider” (TSP) for the purposes of authentication services in different geographical areas.

(vi) MSI shall be responsible for management of IDs of TSPs and UAs, registration of authentication devices and accessing SL-UDI Data Store including managing addresses, email ID, telephone numbers and other contact information of TSPs and UAs.

(vii) MSI shall prepare detailed security architecture for the authentication services and implement the same.

5.10.1.6 Manual Adjudication

(i) On all the enrolments a manual adjudication[3] process shall be performed as a check on the data

submitted and eliminate errors after the duplication process. It is also useful in cases where the biometric solution is not able to make a clear "duplicate/no duplicate" decision, after the de-duplication.

(ii) Manual adjudication process is undertaken both after the demographic and after biometric deduplication

(iii) Pre-demographic de-duplication is used to eliminate errors such as incorrect photograph, incorrect gender etc.

(iv) Post biometric de-duplication is used for scrutinizing cases which are suspect match with existing records.

(v) For demographic manual adjudication, MSI shall be responsible for:

a. Establish the process for Manual Adjudication

b. Training of GoSL's manpower to undertake manual adjudication

c. Define a mechanism to correct the data

(vi) For biometric manual adjudication, MSI shall be responsible for:

a. Support BSP MSI to define a process for biometric manual adjudication

b. Support BSP MSI in training on biometric manual adjudication process

(vii) MSI shall be responsible for deploying the manual adjudication module of BSP adjudication as part of SL-UDI Software System.

(viii) MSI shall be responsible for provision of required IT Hardware for manual adjudication including desktops.

5.10.2 Technical Services

5.10.2.1 Asset Management

X. ***Inventory Management***

(i) MSI will be required to maintain and manage the inventory of all assets (hardware, software, application, and network) being procured, supplied, and commissioned as part of this engagement.

(ii) MSI will be required to identify a single point of contact, responsible for stock and inventory management. Stock management should involve the inflow and outflow of all assets from GoSL/SL-UDI premises.

(iii) As part of the inventory management services, MSI will be required to forecast the demand of required asset and the same should be reported to GoSL with schedule for informed decision making.

(iv) MSI will be required to assess the inventory and identify gaps in procurement or supply of assets and share a report on a monthly basis or as the case may be for effective management of inventory.

(v) MSI will maintain the inventory of spares for all the assets to meet the immediate requirements of the project.

XI. ***ICT Infrastructure***

(i) MSI will be responsible to manage the assets procured, supplied, and commissioned as part of this engagement. The assets will cover all ICT components supplied in Primary Data Center and Disaster Recovery and at the Citizen Services Centers for Enrolment and Authentication.

(ii) MSI will take necessary approvals from the GoSL regarding any transfer, addition and change of assets. This includes but not limiting to, approval on the schedule, specifications of assets in case of any addition and change in asset, location, etc.

(iii) MSI will be responsible for all the logistics and associated arrangements for transfer, addition and change in the assets as part of the ATS or AMC services. GoSL will not make any payments to MSI specifically for asset management activities.

(iv) MSI should ensure that transfer, addition and change of assets to or from the location of its commissioning should not disrupt the operations of SL-UDI. MSI should prepare a schedule for such activity for the approval of GoSL.

(v) MSI will be responsible for reinstating the operations including the date and application after any transfer, addition and change of assets including coordination with any third party.

(vi) In case change of assets results in disposal of assets, MSI will be responsible to dispose the assets as per rules and regulations of Sri Lanka in consultation with GoSL.

(vii) MSI will be responsible for testing the newly added or changed assets in the SL-UDI Information System, for seamless integration and smooth operations.

(viii) MSI will be responsible for forecasting the requirement of any asset transfer, movement and change and also reporting after the activity successfully gets completed.

(ix) MSI will be responsible to link the assets with their ATS and/or Annual Maintenance services by recording details of incidents and problems observed and rectified vis-à-vis each asset.

5.10.2.2 Software Asset Management

(i) MSI will be required to manage the software licenses including the utilization of licenses, license validity, renewal process and date, etc.

(ii) MSI will be required to coordinate with third party software suppliers and OEMs for effective management of software and licenses.

(iii) MSI will be required to use software license management tools to manage the software assets.

(iv) MSI will be responsible to link the software assets with their annual technical support and maintenance services by recording activities of updates, upgrades, patches, bug fixes, major functional changes, etc. for each software asset.

(v) The license of the proposed/ deployed solution should be an enterprise level on perpetual basis in name of GoSL.

5.10.2.3 Field Network Management

(i) MSI will be required to provide management services for the upkeep and maintenance of the network. The MSI shall undertake the tasks to manage all network related operations at Primary Data Center, Disaster Recovery Site, Network Operations Center, and GoSL will be responsible for Enrolment Centers. MSI will be responsible for maintaining the desired Service Levels of network uptime and resolving issues pertaining to the network as given in **Annexure**

9: Service-Levels.

(ii) Monitoring of network will be the responsibility of MSI team. Stakeholders will log incident calls through the Contact Center to report the network related problems. MSI will undertake troubleshooting of issues and incidents logged by stakeholders.

(iii) MSI will establish a mechanism to receive information pertaining to incident and problem logged at the Contact Center for necessary action required.

(iv) MSI shall be responsible for management of network assets as defined in the Asset Management related scope of work.

(v) MSI shall interface with local Telecom companies and other services providers to maintain the network services and uptime for service delivery.

(vi) MSI will be responsible to assess the incidents and reported problems related to the network. MSI shall be responsible for resolution of these problems and improve the performance and optimize the utilization of network.

(vii) MSI will be responsible to ensure to support the SL-UDI team in managing the performance of the network.

(viii) MSI will be required to establish procedures, rules, and manuals for troubleshooting network problems and also for effective monitoring of network using EMS.

(ix) MSI will set-up NOC for management of network operators.

5.10.2.4 IP Address Management

The MSI Shall be responsible for IP Address Management for the SL-UDI Information System including, but not limited to, the following activities:

(i) Planning for IP Address Management

(ii) Automated IP address tracking

(iii) Integrated DHCP, DNS, and IP address management

(iv) IP alerting, troubleshooting, and reporting

5.10.2.5 Software Management

SL-UDI Software System maintenance and management support includes troubleshooting and addressing functionality/availability and performance issues and also implementing change requests, license management, updated and upgrades, etc.

5.10.2.6 SMS Services

(i) SL-UDI Information System should be enabled to send and receive SMS based notifications primarily for sending alerts to users (officials, beneficiaries) and receiving SMS requests from citizens to get service request update information.

(ii) Outbound SMS shall be automated based on an event or time during the service life cycle. For example, upon successful generation of a PIN number, enrolled beneficiary shall receive an SMS notification providing the PIN number.

(iii) MSI must integrate with an SMS Gateway to enable inbound and outbound SMS services. Cost of SMS Gateway, Identification and SMS charges shall be borne by the GoSL.

(iv) The SMS application will expose API to initiate the SMS broadcasting or alert notification.

(v) The SMS service should support USSD codes and should follow the ANRT norms.

(vi) Support automated alerts that allows to set up triggers that will automatically send out reminders.

(vii) Provide provision for International SMS.

(viii) Include provision to resend the SMS in case of failure of the message.

(ix) Must have common features like non-acceptance of landline numbers, unacceptable mobile numbers etc.

(x) Should automatically create a log of SMS sent.

(xi) The message shall be sent through command line interface/API, Web Interface.

(xii) The MSI shall maintain Do Not Disturb (DND) controls.

(xiii) Should provide standard reports like success/failure report on current as well as historical/cumulative basis.

(xiv) MSI should prepare a draft SMS content and obtain a sign-off from the GoSL on the SMS content before rolling out the SMS services.

5.10.2.7 Payment Gateway

The MSI will be responsible for integration of the SL-UDI software system with multiple payment gateways. The GoSL will take responsibility of engaging these payment gateways (incl. security deposit), recurring charges, usage charges, PCI-DSS compliance etc.

5.10.2.8 Biometric Solution Management

The Biometric Service Provider (BSP) will supply, install, commission, operate and maintain the ABIS solution, Biometric SDK, Manual Adjudication, etc. in the Data Center managed by the MSI. The responsibility of the MSI in setup and management of the biometric solution is as follows:

(i) The MSI shall provide adequate data center space for hosting the racks of the BSP.

(ii) The MSI shall provide physical separation of the BSP racks shall be considered as part of the Primary Site and Disaster Recovery Site design by the MSI in consultation with BSP and GoSL.

(iii) The MSI shall design the DC LAN, Security Architecture and Network Architecture in a manner to integrate the ABIS solution of the biometric solution provider. The MSI needs to create a detailed architecture considering the biometric solution as a part of SL-UDI Information System.

(iv) The security components and network components provided by MSI would be shared common resources. Thus, MSI needs to provision for suitable number of licenses, ports, etc. to meet this requirement. The MSI will assist BSP in installation and update (patch, upgrade, etc.) of security related endpoints on the servers of BSP.

(v) After the backup, the BSP will hand over the tapes to MSI. GoSL will be responsible to transport the tapes to off site and its safe and secure storage.

(vi) BSP shall be responsible for performing operations as per the BCP plan and shall ensure recovery/backup as per the BCP policy. The BSP will also be responsible for resuming

(including rolling back to Primary Site) the biometric solution and associated data. Thus, BSP will be responsible for managing the RTO and RPO as per the BCP.

(vii) BSP shall be responsible for coordinating with OEM(s) of infrastructure provided by it.

(viii) MSI will provide the helpdesk services to the BSP. BSP will position a dedicated resource in the helpdesk to attend to the queries and incidents related to biometric solution.

(ix) As part of the project, the BSP shall impart training to staff of GoSL and MSI, on the solution related to configuration, usage, API, performance tuning and measurement and technical reports.

(x) The BSP shall supply client-side and server-side SDKs. SDKs will be used in the enrolment software, manual adjudication (for duplicates), authentication solution, and analytics module. The MSI will undertake the training from the MOSIP as well as BSP during knowledge transfer and training. In case of SDK updates and upgrades, the MSI would be responsible for integration of newer versions of SDKs with the support of MOSIP.

(xi) The BSP shall supply ABIS for biometric deduplication and verification during the enrolment process. The workflow and integration of ABIS shall be the responsibility of BSP with support from MSI.

(xii) The Manual Adjudication application of BSP shall be used for manual adjudication post deduplication and for resolution of duplicates. The workflow and integration of manual adjudication shall be the responsibility of BSP with support from MSI.

(xiii) For any integration or coordination with BSP (other than one specified in the RFP), the MSI will have lead responsibility and BSP shall support the MSI in this activity.

5.11 Operations and Maintenance

Support and Maintenance of the SL-UDI will commence with Go-Live.

5.11.1 Support and Maintenance Services

(i) The Support and Maintenance should include OEM warranty for all IT related equipment and software for a period of 12 months from Go-Live of Iteration 1.

(ii) MSI will be required to provide the comprehensive Annual Maintenance Services and Annual Technical Support of IT infrastructure supplied under this engagement for a period of 2 years after the completion of the period stated in point (i) above.

(iii) GoSL may opt to procure Annual Maintenance Services for all the infrastructure supplied under this engagement for further period of 2 year(s) beyond the Support and Maintenance.

(iv) For all components where perpetual licenses are available, the MSI should provide the perpetual licenses. For other components (only subscription-based licenses are available), MSI will be required to supply licenses till the validity of the contract. For all open-source components (including underlying tools and technologies of MOSIP), the MSI is expected to provide enterprise support till the validity of the contract, wherever available.

(v) For enrolment kits, the OEM shall provide support and maintenance for the O & M period (3 years from Go-Live). The support and maintenance shall cover the equipment/products should be repaired and made operational, failing which a replacement should be given till the equipment is repaired.

(vi) MSI will be responsible for coordinating with the OEM for the rectification of any problem covered under the support and maintenance.

(vii) MSI will be responsible for resolution of any problem in IT hardware as per defined service levels.

(viii) MSI will be required to maintain a log of support and maintenance and AMC status of each of the existing assets.

(ix) For assets whose AMC is due for expiry, the intimation to GoSL shall be provided at least 3 months prior to the expiry of the contract and MSI shall take action for renewal/extension of AMC as per agreement with the GoSL.

(x) In case any hard disk drive of any server, SAN, or client machine is replaced during AMC, the unserviceable HDD will be property of GoSL and will not be returned to MSI.

5.11.2 Hosting Infrastructure (SL-UDI-DS and its Operations, Maintenance and Administration Services)

As part of the overall Operations and Maintenance, following are the key activities:

1) During the Operations and Maintenance phase, MSI shall ensure that services of professionally qualified personnel are available for providing comprehensive onsite maintenance of the product or specified hardware/software and its components. Comprehensive maintenance shall include, among other things, day to day maintenance of the product or specified hardware/software a reloading of firmware/software, compliance to security requirements, etc. when required or in the event of system crash/malfunctioning, fine tuning, system monitoring, log maintenance, etc. MSI shall provide services of an expert engineers at DC and Disaster Recovery site, whenever it is essential. In case of failure of product or specified hardware/software, MSI shall ensure that product or specified hardware/software is made operational to the full satisfaction of the GoSL within the given timelines.

2) Any equipment that has had a hardware failure on four or more occasions in a period of less than three months should have a replaceability assessment and agreement with the hardware supplier.

3) In case of any disk failure on any server or SAN/HCI, this shall be replaced during AMC. Due to security reasons, the same will not be returned to MSI.

4) Preventive Maintenance (PM) should be carried out of all hardware and testing for viruses, if any, and proper records should be maintained at both DC and DR site. The preventive maintenance should be carried out at least once every six months.

5) Corrective Maintenance may be carried out for maintenance/troubleshooting of supplied hardware/software and support infrastructure problem including network (active/passive) equipment, security, and rectification of the same. There should be complete documentation of problems, isolation, cause, and rectification procedures for building knowledge base for the known problems in centralized repository.

6) There should be a support and maintenance for all hardware, equipment, accessories, spare parts, software, etc. procured and implemented against any manufacturing defects during the support and maintenance period specified in the tender document.

7) support and maintenance should be monitored to check adherence to preventive and repair maintenance terms and conditions. These warranties should comply with the agreed technical standards, security requirements, operating procedures, and recovery procedures.

8) Adequate stock for spare parts may be maintained as per the SLAs

9) Perform regular hardening, patch management, testing and installation of software updates issued by OEM from time to time after following agreed process

10) MSI shall provide maintenance support for support software's and Operating system over the contract period

11) Ensure overall security and ensure installation and management of every security component at every layer including physical security

12) Design and maintain Policies and Standard Operating Procedures

13) The MSI shall perform periodic audits to measure license compliance against the number of valid End User software licenses consistent with the terms and conditions of license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions.

14) The MSI shall report any exceptions to license terms and conditions at the right time to SL- UDI. However, the responsibility of license compliance solely lies with the MSI which shall be audited/verified by GoSL on regular intervals. For any license related non- compliance during the contract duration, the financial impact (sanctions, penalties, etc.) will be borne by the MSI at its own cost.

15) The MSI shall be responsible for coordination with MSP and agencies to resolve issues and oversee implementation. The MSI is also required to resolve conflict between BSP in case of borderline integration issues

16) Proactive monitoring and Troubleshooting (related to Virtualization, Storage, Network etc.)

17) Perform Incident, Problem and Change Management w.r.t. to all Infrastructure and Security components included as part of the RFP

18) Asset Lifecycle Management and providing integration interface for relevant data to be pushed in asset management solution

19) MSI shall provide operations and management services for compute, storage, and Database

20) MSI shall perform Backup Monitoring, Management, Reporting, including a backup management solution

21) MSI shall provide Data Replication and DR management and shall leverage relevant tools to integrate the replication solution with monitoring solution for seamless DR activity

22) The MSI shall leverage log monitoring solution for Reporting and Access Management

23) The MSI shall optimize capacity by ensuring, unused for defunct VMs to be reclaimed and deleted to release capacity and appropriate distribution of load where necessary

24) Notify, escalate, and communicate to senior management on status of critical service requests, major incidents, and changes as necessary

25) Implementing policies, Access Controls, managing clusters and certificates

26) User access management to infrastructure resources shall be managed by MSI.

27) MSI to ensure that all proposed frameworks, components, platforms, and runtime have 24x7 support including bug fixes, patches, updates, and upgrades from OEM for duration of the

contract.

Note: The operations and maintenance would cover the entire systems and processes i.e., software systems, hardware infrastructure, networks, security systems, field infrastructure, contact center, enrolment centers, NOC, SOC, etc.

As part of the overall Operations and Maintenance, following are the key activities:

1) A comprehensive and onsite manufacturer's support and maintenance should be available in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. for all the components mentioned above. There should be a support and maintenance for all hardware, equipment, accessories, spare parts, software, etc. procured and implemented against any manufacturing defects during the O & M period.
2) Any equipment having a hardware failure on four or more occasions in a period of less than three months should have a replacement ability assessment and agreement with the hardware supplier.
3) In case of any hard disk drive of any server, SAN, or client machine is replaced during AMC, the unserviceable HDD should be maintained by the SL-UDI team.
4) Preventive Maintenance (PM) should be carried out of all hardware and testing for viruses, if any, and proper records should be maintained at both DC and DR site for such PM.
5) Corrective Maintenance may be carried out for maintenance/troubleshooting of supplied hardware/software and support infrastructure problem including network (active/passive) equipment, security, and rectification of the same. There should be complete documentation of problems, isolation, cause, and rectification procedures for building knowledge base for the known problems in centralized repository.
6) Warranties should be monitored to check adherence to preventive and repair maintenance terms and conditions. These warranties should comply with the agreed technical standards, security requirements, operating procedures, and recovery procedures.
7) Adequate stock for spare parts may be maintained as per the SLAs.
8) 24x7 monitoring and management of availability and security of the infrastructure and assets.
9) Perform regular hardening, patch management, testing and installation of software updates issued by OEM from time to time after following agreed process.
10) Ensure overall security - ensure installation and management of every security component at every layer including physical security.
11) Prepare documentation/policies required for certifications included in the scope of work.
12) Preventive maintenance plan for every quarter.
13) Performance tuning of system as required.
14) Design and maintain Policies and Standard Operating Procedures.
15) User access management.

5.11.2.1 Management of Data Center Sites (DC and DR)

MSI shall be responsible for undertaking the following activities for infrastructure maintenance:

(i) Ensure compliance to relevant SLA's

(ii) 24x7 monitoring and management of availability and security of the infrastructure and assets

(iii) Perform regular hardening, patch management, testing and installation of software updates issued by OEMs from time to time

(iv) Ensure overall security by installation and management of every security component at every layer including physical security

(v) Prepare documentation/policies required for certifications included in the scope of work

(vi) Prepare preventive maintenance plan for every quarter

(vii) Undertake performance tuning of system as required

(viii) Design and maintain Policies and Standard Operating Procedures

(ix) User access management

(x) Other activities as defined/to meet the project objectives and SLAs

(xi) Periodic update of all documents.

5.11.2.2 Infrastructure Management

This includes the design of an appropriate system administration policy with precise definition of duties and adequate segregation of responsibilities. Following includes, but not limited to, the various activities to be performed by the MSI for the System Administration of the solution:

(i) Overall management and administration of infrastructure solution including servers, networking & security components, storage, etc.

(ii) Performance tuning of the system may be needed to comply with service level requirements on a continuous basis.

(iii) Monitor and track server performance and take corrective actions to optimize the performance on a daily basis.

(iv) System administration tasks such as creating and managing users etc.

(v) Data storage management activities including backup, restore and archival etc.

(vi) Attend to user request for assistance related to usage and management of the solution

(vii) Replacement of equipment as per service levels

(viii) Other important activities shall include but not limited to:

a. Maintenance of system configuration

b. Implementation of system security features as per the guidelines

c. Tracking the server's performance and take remedial and preventive actions in case of problems

d. Proper upkeep of storage media for taking backups

5.11.2.3 Server and Virtual Services Operations

Server and Virtual services will provide L1, L2 and L3 support services covering server, storage, backup, replication and virtual services. L1 services will comprise of monitoring, L2 services will comprise of triaging, troubleshooting, L3 activities will cover new services rollout and new service configuration. As part of server operations below are the set-off activities which will be performed

are provided in table given below:

Level	Services
Level 1 support services (monitoring and basic operations as per SOP	• Normal Start-up and Shutdown • Apply Naming Convention, Home Directory, Group Creation as per Policy • User access management • Monitor Concurrent Logins /Connections. • Basic server troubleshooting • Monitor Disk space, Processor Utilization, Network Utilization related to server • Backup Operation and Monitoring
Level 2 support activities will comprise of (regular server administration operations as per SOP)	• Server Reinstallation and configuration • Support during Software Installation • Define Account Policy • Password policy management • Define Administrator /Supervisor Password restrictions • Managing Disk space, Processor Utilization, Network Utilization related to server • Problem Management • Backup Configuration • Restoration Drill • Patch Management and Testing • Server Build • Task automation/Scripting • Systems Continuity Management
Level 3 support activities will comprise of trouble shooting and policy level activities	• Security Audit on Server OS. • Performance Tuning • Defining backup Policy • Patch feasibility study • Security Policy definition for Server • Root Cause Analysis • OS hardening

Table 30: Server and Virtual Services Operations Activities

5.11.2.4 System Maintenance and Management

(i) MSI shall be responsible for tasks including, but not limited to, setting up servers, configuring and apportioning storage space, periodic backup of data, execute hardware and software updates when necessary and automate reporting tasks. MSI shall be responsible for undertaking the following activities:

a. MSI shall provision skilled and experienced manpower resources to administer and manage the entire system at Primary Data Center, and Disaster Recovery.

b. MSI shall be responsible for identification, diagnosis and resolution of problem areas pertaining to the IT Infrastructure and maintaining the defined SLA levels.

c. MSI shall implement and maintain standard operating procedures for the maintenance of the IT infrastructure based on the policies formulated in discussion with MSP & GoSL and based on the industry best practices/frameworks. MSI shall also create and maintain adequate documentation/checklists for the same.

d. MSI shall be responsible for managing the usernames, roles, and passwords of all the relevant subsystems, including, but not limited to servers, other devices, etc. However, the access controls for the respective components will be given through MSP. MSI shall be required to set up the directory server. Logs relating to access of system by administrators shall also be kept and shall be made available to GoSL on a need basis.

e. MSI shall implement a password change mechanism in accordance with the security policy formulated.

5.11.2.5 System Administration

MSI's scope of work for System Administration includes the following:

(i) 24*7 monitoring and management of the servers in the Primary Data Center, and Disaster Recovery site.

(ii) MSI shall also ensure proper configuration of server parameters and performance tuning on a regular basis. MSI shall be the single point of accountability for all hardware maintenance and support the IT infrastructure.

(iii) MSI will be responsible for operating system administration, including but not limited to management of users, processes and preventive maintenance. MSI will also be responsible for management of upgrades including updates, upgrades and patches to ensure that the system is properly updated.

(iv) MSI will be responsible for installation and re-installation of the hardware(s) as well as the software(s) in the event of system crash/failures.

(v) MSI will also be responsible for proactive monitoring of the applications hosted

(vi) MSI shall appoint system administrators to regularly monitor and maintain a log of the monitoring of servers to ensure their availability at all times.

(vii) GoSL shall undertake regular analysis of events and logs generated in all the sub systems including but not limited to servers, operating systems etc. The system administrators shall undertake actions in accordance with the results of the log analysis. The system administrators shall also ensure that the logs are backed up and truncated at regular intervals.

(viii) The system administrators shall adopt a defined process for change and configuration management in the areas including, but not limited to, changes in servers, operating system,

applying patches, etc.

(ix) The system administrators shall provide hardening of servers in line with the defined security policies. Validation of hardening configuration will be carried out quarterly and deviations must be tracked through SLA reporting

(x) The system administrators shall provide integration and user support on all supported servers, data storage systems etc.

(xi) The system administrators shall provide directory services such as local LDAP services, DNS services and user support on all supported servers, data storage systems etc.

(xii) The system administrators shall be required to troubleshoot problems with web services, application software, server relationship issues and overall aspects of a server environment like managing and monitoring server configuration, performance and activity of all servers.

(xiii) The system administrators should be responsible for documentation regarding configuration of all servers, IT Infrastructure etc.

(xiv) The system administrators shall be responsible for managing the trouble tickets, diagnosis of the problems, reporting, managing escalation, and ensuring rectification of server problems as prescribed in Service Level Agreement.

(xv) The system administrators should have experience in the latest technologies so as to provision the existing and applicable infrastructure, if required.

5.11.2.6 Storage Administration

MSI's scope of work for Storage Administration includes the following:

(i) MSI shall be responsible for the management of the storage solution including, but not limited to, preparation of storage management policy, configuration and management of disk array, SAN fabric/switches, tape library, object storage, etc.

(ii) MSI shall be responsible for storage management, including but not limited to management of space, SAN/NAS volumes, RAID configuration, LUN, zone, security, business continuity volumes, performance, etc.

(iii) The MSI will be required to identify parameters including, but not limited to, key resources in the storage solution, interconnects between key resources in the storage solution, health of key resources, connectivity and access rights to storage volumes and the zones being enforced in the storage solution.

(iv) MSI shall be responsible to create/delete, enable/disable zones in the storage solution.

(v) MSI shall be responsible to create/delete/modify storage volumes in the storage solution.

(vi) MSI shall be responsible for creating/delete, enable/disable connectivity and access rights to storage volumes in the storage solution.

(vii) MSI shall be responsible to facilitate scalability of solution wherever required.

(viii) The storage administrators positioned by the MSI will also be required to have experience in technologies such as virtualization, object storage, and cloud computing so as to provision the existing and applicable infrastructure, if required.

As part of storage operations below activities will be performed are provided in table given below:

Level	Services
L1 support services (monitoring and basic operations as per SOP)	• FC /director port monitoring • Array event monitoring • Storage array performance monitoring • Disk drives health monitoring • Array disk space capability monitoring /reporting • Event monitoring
L2 support activities will comprise of (regular server administration operations as per SOP)	• LUN/Meta device configuration (creation, deletion, allocation) • Host systems configuration in the array manager (addition, modification) • Array event analysis • Mirror/snapshot configuration • FC/HBA configuration in the host server • Multi-path configuration • Port configuration • Zone configuration • Event analysis
L3 support activities will comprise of (regular server administration operations as per SOP)	• Storage Array performance analysis • Hardware modification (replacement/expansion) • Volume data replication configuration • FC/HBA hardware modification (replacement/expansion) • Device parameter configuration • Fabric firmware upgrade /management • Switch port performance analysis • FC cable connectivity modification (new/changes)

Table 31: Storage Operations Activities

5.11.2.7 Database Administration

MSI's scope of work for Database Administration includes the following:

(i) MSI shall be responsible for monitoring database activity and performance, changing the database logical structure to embody the requirements of new and changed programs.

(ii) MSI shall be responsible to perform physical administrative functions such as reorganizing the database to improve performance.

(iii) MSI shall be responsible for tuning the database, ensuring the integrity of the data and

configuring the data dictionary.

(iv) MSI will follow guidelines issued by GoSL in this regard, including access of database by system administrators and guidelines relating to security of database.

(v) Database administration should follow the principle of segregation of duties to ensure no single DBA can update production tables/data singularly.

(vi) In addition to restrictions on any direct change in data by any administrator, the Databases shall have Auditing features enabled to capture all activities of administrators.

5.11.2.8 Backup/Replication/Restore/Archival

MSI's scope of work for Backup/Restore/Archival includes the following:

(i) MSI shall be responsible for implementation of backup and archival policies as finalized with GoSL. The MSI is responsible for getting acquainted with the storage policies of GoSL before installation and configuration. It should be noted that the activities performed by the MSI may be reviewed by GoSL.

(ii) The data shall be online in DR for a period of 3 years after which it shall be archived permanently. It is expected that the data in the archives remains non-editable by any means

(iii) MSI shall be responsible for monitoring and enhancing the performance of scheduled backups, scheduled regular testing of backups and ensuring adherence to related retention policies.

(iv) MSI shall be responsible for prompt execution of on-demand backups of volumes and files whenever required by GoSL or in case of upgrades and configuration changes to the system.

(v) MSI shall be responsible for real-time monitoring, log maintenance and reporting of backup status on a regular basis. MSI shall appoint administrators to ensure prompt problem resolution in case of failures in the backup processes.

(vi) MSI shall undertake media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fireproof cabinets.

(vii) MSI shall also provide 24 x 7 support for file and volume restoration requests at the Primary Data Center, and Disaster Recovery.

(viii) The MSI shall follow industry best practices for backup, replication, archival and restore.

As part of backup operations below activities will be performed are provided in table given below:

Level	Services
L1 support activities will comprise of	• monitoring and basic operations as per SOP
L2 support activities will comprise of	• regular server administration operations as per SOP
L3 support activities will comprise of	• regular server administration operations as per SOP

Table 32: Backup Operations Activities

MSI shall develop processes to secure devices/ products/ solutions that provide secure storage, processing, and transmission environment in the data network.

5.11.2.9 Networking Monitoring

MSI's scope of work for Network Monitoring includes the following:

(i) MSI shall provide services for management of network environment to maintain performance

at optimum levels on a 24 x 7 basis.

(ii) MSI shall be responsible for monitoring and administering the network within the Primary Data Center, Disaster Recovery site up to the integration points with customer premises equipment (CPE). MSI shall be required to provide network related services for routers, switches, load balancer, NTP services etc.

(iii) MSI shall be responsible for creating and modifying VLAN, assignment of ports to appropriate applications and segmentation of traffic.

(iv) MSI shall also be responsible for break fix maintenance of the LAN cabling within Primary Data Center, and Disaster Recovery, and responsible for break fixing maintenance internet service provider terminating connectivity

(v) MSI shall also provide network related support and will coordinate with connectivity service providers of TSPs who are terminating their network at the Primary Data Center, and Disaster Recovery sites for access of system.

5.11.2.10 Security Management

MSI's scope of work for Security Management includes the following:

1) Regular hardening and patch management of components of the SL-UDI Information System as agreed with GoSL.
2) Performing security services on the components that are part of the GoSL environment as per security policy finalized with GoSL.
3) Manage and monitor safety of information/data (IT Security Administration).
4) Reporting security incidents and resolution of the same.
5) Proactively monitor, manage, maintain, and administer all security devices and update engine, signatures, and patterns as applicable.
6) Managing and monitoring of anti-virus, anti-malware, phishing, and malware for managed resources.
7) Ensuring 100 percent end point detection and response coverage with patterns not old more than period agreed on any given system.
8) Reporting security incidents and co-ordinate resolution.
9) Monitoring centralized pattern distribution (live update) and scanning for deficiencies.
10) Maintaining secure domain policies.
11) Secured IPsec/SSL/TLS based virtual private network (VPN) management.
12) Performing firewall management and review of policies on at least quarterly basis during first year of O&M and then after at least on half-yearly basis.
13) Resolution of calls for security notifications, system alerts, vulnerabilities in hardware/software and alerting GoSL as appropriate.
14) Performing patch management using software distribution tool for all security applications including content management system, antivirus, and VPN.
15) Providing root cause analysis for all defined problems including hacking attempts.

16) Monthly reporting on security breaches and attempts plus the action taken to thwart the same and providing the same to GoSL.
17) Maintaining documentation of security component details including architecture diagram, policies, and configurations.
18) Performing periodic review of security configurations for inconsistencies and redundancies against security policy.
19) Performing periodic review of security policy and suggesting improvements.
20) Reviewing logs daily of significance such as abnormal traffic, unauthorized penetration attempts, any sign of potential vulnerability. Security alerts and responses. Proactive measures in the event a problem is detected.
21) Policy management (firewall users, rules, hosts, access controls, daily adaptations).
22) Modifying security policy, routing table and protocols.
23) Performing zone management (DMZ, MZ).
24) Sensitizing users to security issues through regular updates or alerts/periodic updates/Help. Support GoSL in issuance of mailers in this regard.
25) Performing capacity management of security resources to meet business needs.
26) Rapidly resolving every incident/problem within mutually agreed timelines.
27) Testing and implementation of patches and upgrades.
28) Network/device hardening procedure as per security guidelines.
29) Implementing and maintaining security rules.
30) Performing any other day-to-day administration and support activities.
31) Development of a process for Hardening of all SL-UDI Information Systems such as OS, desktops, servers, network devices, storage devices etc.

In addition, the MSI shall be responsible for implementing measures to ensure the overall security of the solution and confidentiality of the data in compliance with the Information Security Plan and Guidelines. The MSI shall monitor solution for events or activities, which might compromise (fraudulently or accidentally) the confidentiality, integrity, or availability of the Services. Following includes, but not limited to, the various activities to be performed by the MSI for information security of the solution:

i. Compliance to the Information Security Plan and Guidelines
    a. Monitoring the security of the system
    b. As per the incident reports shared by the MSI, GoSL, etc.
    c. Audit review tools
    d. Manual processes
ii. The MSI shall co-operate with the appointed representatives of the GoSL in case of security incidents. The incident response process will seek to limit damage and may include the investigation of the incident and notification of the appropriate authorities. A summary of all security incidents shall be made available to the GoSL on a weekly basis. The significant security incidents will

be reported on an immediate basis.

iii. The MSI shall produce and maintain system audit logs on the system for a period agreed by the MSI and the GoSL, at which point they will be archived and stored off-site or as desired by the GoSL. The MSI will regularly review the audit logs for relevant security exceptions.

5.11.2.11 Event Correlation

The MSI should facilitate correlation of events as part of the different components monitoring and also as part of the security events. This should identify the events raised by the system, which may or may not require human intervention and would result in automatic resolution also.

5.11.2.12 Incident Management

To complement the IT Service Desk support functions, the Incident Management process(es) are defined to monitor progress of open Incidents to resolution [end to end life cycle of incidents]. These ITIL Processes are ISO20000 compliant, and the process flows for the overview of the Service Desk Processes are provided below.

To manage the Incident Management process, SL-UDI will leverage its Enterprise IT Service Management tool to register, categorize and prioritize Incidents and apply a pre-agreed Service Level target to each and every Incident. The primary objective of the Incident Management Process is to restore normal service operation as quickly as possible and minimize the overall adverse impact on business operations. This ensures that the best possible levels of service quality and availability are maintained. ITIL defines normal service operation as that which is stated within the Serviced Level Agreement (SLA).

Some of the key incident management terms applicable for SL-UDI are as below:

(i) **Incident:** Incident is defined as any act

a. Failure of a service

b. Reduction in service performance, against the targets stated in the SLA

c. Known potential failure resulting from Events and monitoring

Incident's scope includes services directly delivered to customers as well as services to support the operational environment. Incidents detected by Operations (either manually or as an end result of the Event Management process) should be reported to the process and registered, handled and solved as if users had reported them.

(ii) **Service Requests:** 'Service Requests' are not part of the scope of this Incident Management Process; they are handled by the Request Fulfilment Process Service Requests include 'Standard Changes' and contact with the Service Desk that refers to any 'how to' questions by a user not able to use the service as part of the normal operation.

(iii) **Events:** 'Events' are also not part of the scope of this Incident Management Process; they are handled by the Event Management process.

(iv) The following are policy statements applicable to the SL-UDI's Incident Management process and govern the activities within the process.

a. Incident Management will be governed by internationally recognized best practice frameworks and tools.

b. For IT Service Management, ITIL v3 is the chosen framework and ISO/IEC20000 is the chosen quality standard.

c. All incidents should be recorded, reported and open to inspection via audit. Incidents not reported via the correct process are outside the scope of this process.

d. All incidents are stored in a common repository and updated throughout their lifecycle.

e. Information on the status and progress of incidents will be available to the client of the affected service.

f. Predetermined restoration targets shall exist for incidents based upon their Service Level Agreements.

g. Incidents will be prioritized and resolved based on the impact and urgency assigned to them.

h. A full escalation management policy will exist to ensure unresolved incidents become resolved.

i. All aspects of major incidents are controlled and coordinated by the Incident Manager.

j. A continual process of process improvement will take place utilizing the 'plan-do-check-act' cycle.

5.11.2.13 Configuration Management (Updates/Upgrades)

The scope of Configuration Management includes identification, recording and reporting of IT components in the production environment for SL-UDI, including their versions control, constituent components and relationships among the components.

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

(i) Account for all IT assets and configurations within the SL-UDI and its services, breaking down the infrastructure into Configuration Items (CI's). This goal supports the activities of 'identification' and 'status accounting'.

(ii) Provide accurate information on configurations to support all the other SL-UDI Service Management processes.

(iii) It ensures that no CI is added, modified, replaced, or removed without appropriate controlling documentation. This supports the activity of 'control'.

(iv) Verify the CMDB database against the infrastructure CI and correct any exceptions. This supports the activity of 'verification'.

MSI shall prepare and submit configuration manual for OS, appliances, middleware, all tools, servers/devices, and all equipment. Any changes in the configuration manual need to be brought to the notice of the GoSL. The configuration manual should be updated periodically.

5.11.2.14 Software License Management

The MSI shall be responsible for software license management. MSI shall maintain data regarding entitlement for software updates, enhancements, refreshes, replacements, and

maintenance.

- Licenses should be under GoSL's name
- GoSL should be able to renew software licenses at the end of the contract.
- License coverage MUST be for the entire duration of the contract
- Cost of all licenses should be covered with in the proposal and in the total contract price.

5.11.3 Software System (including MOSIP, Biometric, and all other components)

(i) The MSI will be responsible for continuous enhancement, maintenance, and management of the SL-UDI Software System for a period of the contract. SL-UDI Software System maintenance and management support includes, but not limited to, troubleshooting, addressing functionality/availability and performance issues and also implementing change requests etc. For the purpose of application maintenance and management, the MSI shall provide a team of full-time resources. Maintenance and management support shall be undertaken whenever any maintenance and enhancement activity need to be carried out as per the mutually agreed plan or change request. The MSI shall ensure compliance with SLAs as indicated in this RFP. Any upgrades/major changes to the software shall be planned by MSI while ensuring that the SLA requirements are met at no additional cost to the GoSL.

(ii) MSI shall be responsible for first L1, L2 maintenance and management of the MOSIP application suite. MSI to work with MOSIP to provide maintenance and management support of MOSIP application suite which can be utilized by MSI on need basis.

(iii) All components / deliverables should be compatible and updated with future updates (OS, platform, patches, etc.) during the contract period.

5.11.3.1 Annual Technical Support

The MSI shall be responsible for providing annual technology support for the COTS products supplied by respective OEMs during the entire maintenance and management phase.

It is mandatory for MSI to take enterprise level annual support over the entire contract duration, at minimum, for the software(s) as mentioned in the Bill of Material provided by the MSI.

5.11.3.2 Application Software Support

(i) The MSI shall provide continuous support through on-site team/telephone/E-mail/Video Conferencing/installation visits as required.

(ii) The MSI shall address all the errors/bugs/gaps in the functionalities of the solution vis-à- vis the signed-off FRS and SRS at no additional cost during the maintenance and management phase.

(iii) All patches and upgrades from OEMs shall be implemented by MSI. Technical upgrades of installation to the new version, as and when required, shall be done by MSI. Any version upgrades of the software/tool/application will be done by MSI after seeking prior approval from the GoSL and submitting the impact assessment of any upgrade.

(iv) Any changes/upgrades to the software performed during the support phase shall be subject to comprehensive and integrated testing by the MSI to ensure that the changes implemented in the system meet the specified requirements and do not impact any other existing functions of the system. A detailed process in this regard will be finalized by the MSI in consultation with

the GoSL.

(v) An issue log shall be maintained by MSI for the errors and bugs identified in the solution as well as any changes implemented in the solution. The issue log shall be submitted to the GoSL monthly.

(vi) The MSI will inform the GoSL, as per the agreed plan, about any new updates/upgrades available for all software components of the solution along with a detailed action report. In case of critical security patches/alerts, the MSI shall inform the GoSL immediately along with any relevant recommendations. The report shall also contain the MSI's recommendations on update/upgrade, benefits, impact analysis etc. The MSI needs to execute updates/upgrades and update all documentation and Knowledge databases etc. The MSI will carry out all required updates/upgrades by following a defined process at no additional cost.

5.11.3.3 MOSIP Support

(i) MSI shall be responsible for the first level and second level (L1 and L2) maintenance and management of the MOSIP application suite.

(ii) MOSIP will provide maintenance and management support of MOSIP application suite at OEM Level which can be utilized by MSI on a need basis. MSI to work with MOSIP in regard to this.

(iii) The process for escalation of support tickets will be specified in consultation with the GoSL.

5.11.3.4 Biometric Solution Support

Following includes, but not limited to, the various activities to be performed by the BSP during the maintenance of the solution:

(i) When an upgrade in applied algorithm is available, the BSP shall evaluate the need to re-template the biometric gallery. Upon analysis, the BSP shall submit a report clearly specifying the advantages of new algorithm, time needed for re-template creation, additional infrastructure needed for re-template creation, plan for rollback in case of error, etc. The analysis should be done keeping in mind that the system downtime is either zero or minimal during this exercise. The GoSL will scrutinize the analysis presented by the BSP and may approve the exercise of re-template creation. Upon approval from the GoSL, the BSP should undertake this exercise and submit a periodic progress report to the GoSL.

(ii) The BSP shall provide support and maintenance for biometric solution for the duration of contract, commencing from the date when the system goes "live". The support and maintenance should include that the solution supplied under this contract shall have no defect arising from design or workmanship or from any act or omission of the successful MSI that may develop under normal use of the supplied solution.

(iii) During the O & M period, BSP shall be completely responsible for defect free functionality of the biometric solution and shall resolve any solution related issues including bug fixing, etc. as per service level defined in the contract. This shall include request-based services (defects/issues), enhancements, configuration management and post release support.

(iv) BSP shall provide the latest updates, patches, bug fixes, enhancements, and version upgrades relevant for the biometric solution at no extra cost to the GoSL. The GoSL should be informed of all version upgrades (minor & major), patches, releases and enhancements along with impacts to the biometric solution. The GoSL will review the impact of the change and will at

its own discretion decide if the change should be implemented. The BSP will install, test and configure the changed solution in various environments.

(v) BSP shall be responsible for software version management, software documentation management reflecting current features and functionality of the solution.

(vi) For support, the BSP may decide on an appropriate onsite-offsite model to meet the service levels

(vii) For bug-fixes and end-user problem resolution, the stakeholder support would include all activities related to resolving the bugs/defects reported by the users. Every bug/defect should be logged and should be categorized on the severity levels. BSP should identify the solution and take necessary approvals from the stakeholders and release the patch for User Acceptance Testing (UAT) after fixing the defects. BSP should document defects /bugs encountered as well as document the resolution of the same.

(viii) For New development and enhancements, BSP in consultation with the GoSL is expected to define a formal process (change management process) to manage the requirements changes as defined in the Change management process Section 8.

(ix) For Configuration management and Version Control, BSP should adhere to the configuration management process defined in conjunction with the stakeholders. This will ensure that all versions' updates in the application are tracked and approved after due scrutiny. BSP may be required to ensure that a copy of the production environment is backed up and stored in the repository before the new/modified components are copied to Production.

(x) For test management, procedures should be defined in conjunction with the stakeholders to ensure smooth transition of the application changes from test environment to production environment. As part of the release management, BSP should perform the following activities:

a. BSP should group the related change requests, assess their development progress and accordingly prepare a schedule for their release to production.

b. BSP should, in consultation with the stakeholders, prepare a detailed release plan for every release. This plan should include the release number and date of release. It should also contain details about the change request to be released.

(xi) In case the performance of the biometric solution is not as per defined service level parameters, the OEM (BSP) will be required to conduct more performance tunings such that the necessary parameters are met.

5.11.3.5 Issue Identification and Resolution

(i) Errors and bugs that persist for a long time, impact a wider range of users and are difficult to resolve in turn lead to application hindrances. The MSI shall resolve all the application problems through implementation of the identified solution (e.g., system malfunctions, performance problems and data corruption etc.).

(ii) Monthly Issue Logs on problems identified and resolved would be submitted to the GoSL & MSP along with recommended solutions.

5.11.3.6 Change Control

(i) All planned or emergency changes to any component of the system shall be carried out through the approved Change Control Management process. The MSI needs to follow all such

processes (based on industry ITSM framework) at all times. For any change, MSI shall ensure:

a. Detailed impact analysis is conducted.

b. All change plans are backed by roll back plans.

c. Appropriate communication on change required has taken place.

d. Requisite approvals have been received.

e. Schedules have been adjusted to minimize impact on the Production environment.

f. All associated documentation is updated post stabilization of the implemented change.

g. Version control is maintained for all software changes.

(ii) The MSI shall define the change control process through change control process software. For any changes to the solution, the MSI has to prepare detailed documentation including proposed changes and impact to the system in terms of functional outcomes/additional features added to the system etc. The MSI shall ensure that software and hardware change control is carried out for the entire contract duration.

5.11.3.7 Release Management

(i) Release Management is used for the release of software of software, upgrades, and patches. This ensures the availability of licensed, tested, and version-certified software, which will function as intended when introduced into the production environment.

(ii) In the context of SL-UDI Information System, release management is required to be handled at two levels:

a) Troubleshooting of core MOSIP related issue may result into modification or update of the existing SL-UDI system deployment in production environment. The modifications required to be done in MOSIP would be carried out by MOSIP or its nominated agency. The tested patch or upgrade/update of MOSIP version 1.x would be made available to MSI. It will be the responsibility of MSI to obtain the modified software and carry out user acceptance test, if required, and then deploy it in the product environment.

b) Software incidents related to support application or other enhancements would require change in the respective modules. It will be the responsibility of MSI to test the modified software (including UAT, if required) and then deploy it in the product environment.

c) If any downtime is required, prior approval should be taken from the GoSL in compliance with the SLA.

d) The overall release management and version control of the SL-UDI Information System will be the responsibility of MSI.

(iii) The MSI shall carry out following activities in the release management process:

a) Plan releases as per the requirements for the approved changes.

b) Build release packages for the deployment for approved changes (one /many) into QA / Staging / Production.

c) Design, test and implement procedures (mechanisms) for the distribution of approved changes to QA / Staging / Production environment.

d) Effectively communicate and manage expectations of the customer / internal stakeholders/end customer during the planning and rollout of new releases.

e) Monitor, Control, and Report the distribution and installation of changes to all concerned stakeholders.

f) Deploy the release as per guidelines.

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

a) Release Planning Process.

b) Release Building Process.

c) Release Testing Process.

d) Release Deployment Planning Process.

e) Release Deployment Process.

f) Client Release Management Process.

g) Server Release Management Process.

(v) The MSI shall document the above processes and submit them to the GoSL for sign-off.

5.11.3.8 Maintain System Documentation

(i) The MSI will maintain at least the following minimum documentation but not limited to:

a) High level design of whole system

b) Low level design for whole system/module design level

c) Updated System Requirements Specifications (SRS)

d) Traceability matrix

e) Compilation environment

(ii) The MSI will also ensure that any software system documentation is updated with regard to the following:

a) Source code is documented.

b) Functional specifications are documented.

c) Application documentation is updated to reflect on-going maintenance and enhancements including FRS and SRS in accordance with the defined standards.

d) User manuals and training manuals are updated to reflect on-going changes/enhancements.

e) Standard practices of version control and management are adopted and followed.

(iii) In addition to the above documents, the documents that are mentioned in the deliverable schedule (Reference Section 6 Implementation Schedule) need to be maintained and provided. During the change management/ Change implementation all impacted documents should be updated accordingly.

5.11.3.9 Support during System Audits

(i) The GoSL may get the system audited by 3rd party auditors. The MSI shall provide necessary

support and co-operation for the audit and close the findings of the audit.

(ii) The GoSL may arrange for the ISO 27001 audit to be conducted for the SL-UDI Information System. The MSI shall cooperate, provide necessary support, and close the findings of the audit.

5.11.3.10 Patch Management

Patch management helps to acquire, test, and install multiple patches for all components of the SL-UDI platform.

(i) This involves updating the relevant system, software, applications, OS, Firmware patches after qualifying the same in the Test / Pre- Production environment before moving to production. Notify all storage users of an impact on their applications and assist them in testing their applications with new patches or upgrades.

(ii) Security and Vulnerability patches should be accorded a higher priority than other patches.

5.12 Project Reporting

The MSI will report to the GoSL on various aspects of the project. The MSI will prepare a draft reporting plan containing the area of reporting, type of reports and reporting frequency. Upon GoSL's approval, the recipients of these reports will be identified.

For the reports having an impact on the payment, service levels and penalties, the MSI will submit a signed hard copy of reports. The other reports can be sent on email to the recipients decided by the GoSL.

The MSI will be required to broadly prepare and submit reports under the 5 categories – (i) ABIS, (ii) Data Quality, (iii) Incident and Issues, (iv) SLA and (v) Other reports. The detail about these categories is provided below:

5.12.1 ABIS Reports

While the SLA reports will focus on ABIS related performance levels on a monthly basis. The ABIS reports will be more frequent and will be used to ascertain the need to improve the performance of ABIS on a continuous basis.

5.12.2 Data Quality Monitoring & Reporting

The quality of captured data is related with accuracy of matching. It is therefore very important that the BSP should continuously monitor the data quality and publish reports, generating exceptions in case quality goes below the threshold. Data quality monitoring is complementary to benchmarking and helps to analyse and correct the problems with the capture process. The primary objective is to identify the sources of the quality problems and to implement corrective actions. The functionality will be implemented in the analytics module using the functionality provided by Biometric SDKs.

The BSP will report on the following:

- **Quality of Data Capture and Matching**: Analysis of captured quality and accuracy of matching on weekly basis
    - **Data Mix-up**: Weekly reports regarding mix-up of the particulars relating to one applicant with those of others, if any. The mix-up may be in any of the demographic or biometric data.
    - **Biometric Exception:** The Enrolment Software may allow the biometrics to be not captured in exceptional circumstances such as children, old persons, persons with one or no hands,

technological issues, etc. The BSP should submit a report about such biometric exceptions.

- **Quality of Operators and Devices**: The quality of data is also dependent upon the operator, enrolment center facility and device. Thus, to ensure the good quality of enrolment, the BSP should submit a statistical and quality analysis for operators, enrolment centers, and devices.

  It is assumed that the

  a) Data quality of capture would be received with the image. Image would be received in raw form.

  b) Original captured images may be appropriately compressed using published loss-less compression algorithm for optimization of storage and transmission. Compression will not alter the quality of the image.

In summary, the BSP should provision for following scope of work related with Data quality monitoring and reporting:

a) The BSP should centrally administer Image level quality checks and thresholds.

b) The BSP should implement a process which generates automated exceptions, if despite best efforts image captures do not meet quality standards. The BSP should design and implement a mechanism which would provide direct feedback of quality and capture related shortfalls to registrars.

c) The BSP should implement a process which implements Image enhancements techniques to enhance biometric feature extraction to acceptable levels.

d) The BSP should implement a process for achieving consistency across capture devices and, in the case of iris, distance from camera and lighting conditions, by applying variable image enhancement based on known issues of a specific device.

e) The BSP would present the statistical data to GoSL authority on a monthly basis. This will help GoSL to take a decision in case threshold value needs to be adjusted based on inputs from field.

f) The BSP should implement a mechanism to remote update of threshold value of capturing process in SL-UDI data capturing application. The patch should be automatically pushed when capture application connects next to SL-UDI data center for data upload.

g) The BSP should implement a mechanism for automated exception marking if despite best efforts image captures do not meet quality standards.

5.12.3 Incident and Issue Reporting

The incident and issue reporting shall be done by MSI after Go-Live. The scope of these reports will include:

1) Log of preventive / break-fix maintenance undertaken

2) Summary of changes undertaken in all the data center including major changes like configuration changes, release of patches, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.

3) Summary of incidents reported like application down, components down, overall downtime, security vulnerabilities detected, hacker attacks/security threats, peaking of utilization, etc.

4) Bug/defect resolution reports including the analysis of bugs/defects resolved, pending, completion time, responsiveness, concern areas, etc.

5) Change Request Logs with their resolution status.

6) Incident Reporting (as and when it occurs)

   a) Complete system down – with root cause analysis

   b) Peaking of resource utilization on any component

   c) Bottlenecks observed in the system and the possible solutions and workarounds.

7) Security Incident Reporting (as and when it occurs)

   a) Detection of security vulnerability detection with the available solutions/workarounds for fixing

   b) Hacker attacks, Virus attacks, unauthorized access, security threats, etc. – with root cause analysis and plan to fix the problems.

5.12.4 SLA Reporting

The MSI will submit system generated reports, to ensure minimal error in data on all the SLA parameters defined in the contract.

5.12.5 Other Reports

The MSI and BSP will propose the reports to GoSL and finalize the reporting requirements in consultation with them. The MSI and BSP will be responsible to prepare and submitting the reports in the approved format and frequency.

6 Implementation Schedule

6.1 Project Duration

			Year-1												Year-2												Year 3	Year 4											
Task	Activity	Duration (months)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25-36	37	38	39	40	41	42	43	44	45	46	47	48
Iteration 1 (SL-UDI application)	Design, development & implementation	11																																					
	UAT	1																																					
	Go-Live																																						
	Opration Stabilisation Period																																						
Iteration 2 (SL-UDI application)	Design, development, integration & implementation	3																																					
	UAT	1																																					
	Operation Stabilisation Period	3																																					
Operation, Support & Maintenance		36																																					
Exit Management		3																																					

Figure 3: SL-UDI Project Duration

The total duration of the project is the SL-UDI solution implementation period plus 3-year support and maintenance. The overall duration of the project is 48 months. Within the aforementioned timelines, first 11 months (also referred to as "implementation period") are planned for system design, development, and rollout (Release_1 in 12 months and Release_2 in 15th months), the operation and maintenance period will commence post Go-Live of iteration 1. The last 3 months of the contract period for this project shall be considered as Exit Management Period.

The MSI will be solely responsible for providing end to end solution for the SL-UDI project. MSI is

required to design, develop, supply, deliver, install, implement, support and maintain the software, hardware and infrastructure for SL-UDI as described in the Schedule of Requirement. The TOTAL duration of the project is the SL-UDI framework implementation period and 3-year support and maintenance. [Refer section 1.8 Project Duration]. The MSI shall implement the SL-UDI solution (Iteration 1) within 12-months, and support and maintain the SL-UDI solution for next 3-years from the launch (go-live).

The SL-UDI implementation consists of 2 iterations.

a) **Iteration 1:** Proposed duration 12 months from the project kick-off. This includes 11-months for the implementation of the iteration 1 and 1-month for the UAT (User Acceptance Testing)

b) **Iteration 2:** Proposed duration 4 months from the Iteration 01 implementation completing date. This includes 3-months for the implementation of the remaining requirement scope and 1-month for the UAT.

The proposed total implementation time duration for both iterations 1 and 2 is 15 months, as depicted in Figure 1. Each iteration will consist of a 3-month OSP. Therefore, the User Acceptance (UAT) of the SL-UDI complete solution (both iteration 1 and 2) is proposed to be within 18 months from the date of project kick-off. Further, the biometric-related operations will be rolled out with UAT in Iteration-1 but their advanced testing (such as biometric tests, benchmarking, acceptance) will be done along with Iteration-2.

6.2 Implementation Schedule

Note: *T – Date of signing of contract*

Note*: for actual Project Duration Refer Figure 2: SL-UDI Project Duration in Section 3 Project Scope of this document.*

#	Milestone	Duration (in Months)	Timeline (in Months)
1.	Kick-Off, Planning and Set up of Project Management Office (PMO)	0.5	T + 0.5
2.	Requirement Gathering and Initial Design	1.0	T + 1.5
3.	Detailed Design (Iteration_1)	1.0	T + 2.5
4.	Setup of Hosting Infrastructure	8.5	T + 11
5.	Software Development and Testing		
6.	First Software Release (Iteration_1), Benchmarking		
7.	User Acceptance and Go-Live (Iteration_1)	1	T+ 12
8.	Operational Stabilization Period (Iteration_1)	3	T + 15
9.	Detailed Design (Iteration_2) {Commence After T+11}	3	T + 14
10.	Second Software Release (Iteration_2)		
11.	User Acceptance and Go-Live (Iteration_2)	1	T + 15

#	Milestone	Duration (in Months)	Timeline (in Months)
12.	Operational Stabilization Period (Iteration_2)	3	T + 18
13.	Operations and Maintenance. {Commence After T+12}	36	T + 48
14.	Transition and Exit Management {Commence After T+ 44}	4	T + 48

Table 33: Implementation Schedule

6.3 Implementation Milestones

Note: *ED – Effective Date as specified in Volume 1*

#	Milestone	Output
1.	**Kick-Off and Planning/ Setup of PMO and Advance Payment Security**	1) Kick-Off Meeting Presentation 2) Setup of Project Management office in Sri Lanka within the one month of signing Contract. 3) Upon submission of Advance Payment Security. 4) Inception Report 5) Detailed Project Plan 6) MOSIP Takeover Plan 7) Manpower Deployment Plan (Monthly) 8) Manpower Compliance Report 9) Manpower Escalation Matrix 10) Template for Risks and Issue Tracker and Periodic Status Reports 11) Launch of project management tool (on public cloud) with project management plan 12) Launch of task management features on the project management tool 13) Signed contracts with Service Providers (Data Center, Network, etc.) and OEMs 14) Acceptance criteria for deliverables
2.	**Requirement Gathering and Initial Design**	1) Template for capturing requirements and system documentation. 2) Detailed plan for requirement gathering. 3) Identification of stakeholders for requirement gathering in accordance with detailed plan 4) Detailed Application, Data, and Infrastructure Architecture Definition Document

#	Milestone	Output
		5) Metadata Standards 6) Demographic Data Standards 7) Biometric Standards 8) Minimum baseline security standards 9) Infrastructure requirements of the project (as per scope of work) 10) Network architecture, storage architecture, security architecture, compute architecture, component architecture, integration architecture, data architecture, application architecture, API architecture, virtualization, and container platform architecture, deployment architecture. 11) High-level design and architecture documents for DC/DR infrastructure, platforms, software, security solutions, NOC/SOC, Network, etc. 12) Implementation plan of Data Centers, Contact Center, IT Helpdesk, Network Operations Center, Security Operations Center, Service Center, etc. 13) Documentation for COTS Applications 14) Detailed document on the model registration center 15) SL-UDI SLA methodology creation 16) Risk Assessment (Business and Technical) 17) RACI Matrix 18) Detail Cutover Plan and pilot rollout plan
3.	**Detailed Design (applicable for Release_1 as well as Release_2 components)**	1) Functional Requirement Specifications (FRS) 2) Use Case Design Document (UDD) 3) End to End Software Requirement Specification (SRS) 4) High-Level design specification document including the UML use cases, UML designs, Conceptual Data Model, Logical and Physical Data Model for different application modules, API Specifications (Signature /Contract), Stored 5) Procedures Specifications etc. 6) Low Level design document, with detailed algorithms and logic of the important API's stored procedures etc. 7) Low-level design and architecture documents for DC/DR infrastructure, platforms, software, security solutions, NOC/SOC, Network, etc., (covering Network architecture, storage architecture,

#	Milestone	Output
		security architecture, compute architecture, component architecture, integration architecture, data architecture, application architecture, deployment architecture, API architecture, virtualization, and container platform architecture) 8) UI/UX Style Guide 9) Traceability matrices with updated design features against the requirements
4.	**Setup of Hosting Infrastructure**	**Site Setup** 1) Establishment of co-location space within the hired data centers 2) Plan for commissioning of Primary Data Center and Disaster Recovery 3) Site Survey Report for Primary Data Center and Disaster Recovery 4) Detailed plan for site set-up 5) Rack Plan 6) Data Back-up strategy 7) Disaster Recovery Strategy and Procedures **IT Infrastructure** 1) Strategy, Approach, Design, Architecture, and Plan for commissioning of Primary Data Center and Disaster Recovery 2) Supply, 3) Installationand Commissioning of IT Infrastructure (among others hardware, software, appliances, platforms, security, network connectivity etc.) 4) Deployment Plan (among others overall DC/DR deployment, server deployment, storage, network, virtualization, enterprise container platform, security etc.) 5) Creation of environments relevant for this stage in DC and DR sites. 6) Test Plan and Commissioning Report 7) Supply, install and establish the network connectivity to and between DC, DR, NOC, SOC and IT Help desk, facilitate and configuring network connectivity extend from enrolment centers to DC, DR 8) BCP and DR test plan and report.
5.	**Software Development and Testing**	1) Setup of DevSecOps environment in the DC and DR 2) Solution Implementation Plan (including integrations) 3) Updated design documents (if any)

#	Milestone	Output
		4) GUI wireframes 5) Prototypes 6) Data Model Descriptions 7) Software Development and Customization 8) Technical and product related manuals 9) Source code of the applications with version control mechanism in the source code repository provided by GoSL 10) Change management histories. 11) Testing Strategy and Test Plan for various types of testing (automation testing, integration testing, system testing, performance testing, security testing and user acceptance testing) 12) Testing Cases, Testing Data, Testing Scripts, Testing Results and QA release notes (integration testing, system testing, performance testing, security testing, VAPT testing, and user acceptance testing) 13) For BCP and DR testing the test report, recovery logs and learnings report. 14) Draft documentation for relevant components on installation guides, user manuals, system administrator manuals, Toolkit guides and troubleshooting guides. 15) Draft Training Plan 16) Release management plan
6.	**First Software Release (Iteration_1 components), Benchmarking**	**Software** 1) Iteration 1 release and deployment on relevant environments (including production environment) 2) Source code of the applications with version control mechanism in the source code repository provided by GoSL 3) Secure source code review **System Documentation** 1) Updated design documents (FRS, SRS, UDD, etc.) if any 2) Updated documentation (as applicable) for relevant components on installation guides, technical and product related manuals, frequently asked questions, user manuals, system administrator manuals, toolkit guides and troubleshooting guides, SOPs, procedures, policies, processes, etc. 3) Documents revised after previous milestones.

#	Milestone	Output
		4) SOPs, procedures, policies, processes, etc. 5) Frequently asked questions guide. **Performance Testing (PT)** 1) Confirmation of readiness of system for PT 2) Formal submission of final versions of system (incl. ABIS/SDK) to be tested for PT and confirmation about the same. 3) Creation of PT environment, as per required specifications, 4) Installation of PT tools (includes development of logging tools for passive tests within the production environment) 5) Integration of PT suite with system 6) Generate artificial test data, if necessary, and acceptance of sample data 7) Participate and monitor the conduct of tests and review of test logs provided after the tests. 8) Investigate system results to determine deficiencies in performance of system and performing analysis of test logs. 9) Performance test report in the format specified by GoSL 10) Identify the gaps between current infrastructure and requirement infrastructure to meet the performance requirements. 11) Prepare the differential bill of material as per the gap. 12) Supply, install, and commission the material as per differential bill of material. 13) Repeat the relevant activities for re-test. **Note:** The environment will be the real environment wherein all applicable components including security components will be deployed as per the approved deployment architecture. **Audits** 1) Carry out a Complete software audit for the Iteration 1 release and ensure Iteration 1 is complaint. 2) Carry out an Information Security audit for the complete end-to-end Iteration 1 release, including infrastructure, platform, etc. ensure Iteration 1 is complaint. 3) Facilitate the third-party independent Information Security audit carried out by GoSL to ensure the Iteration 1 is complaint. **Training**

#	Milestone	Output
		1) Final Training Plan 2) Training Material, Training Manual, Training Content, Conduct of Trainings, and Satisfactory assessment reports for Trainings. 3) Approved online tutorials, videos, presentations loaded on KMS. 4) Process for Manual Adjudication 5) Training plan and material on manual adjudication 6) Training Reports and Certifications for Enrolment Offices **Field Infrastructure and Enrolment Center** 1) Plan for deployment, testing and commissioning of enrolment kits. 2) Commissioning Report and deployment of enrolment software on registration kits 3) Onboarding of enrolment operators 4) Operational internet for mobile registration centers **Network Connectivity** 1) Supply and Provisioning of connectivity from Data Centers (DC & DR) to NOC, SOC, Contact Center, Technical Helpdesk 2) Supply and Provisioning of internet connectivity links in Data Centers (DC & DR) **Contact Center and Technical Helpdesk** 1) Setup of Technical Helpdesk 2) Deployment of approved software (CRM, Helpdesk, etc.) 3) Preparation of documents i.e., SOPs, FAQs, etc. 4) Deployment of manpower and certificate of their training **Network Operations Center (NOC) and Security Operations Center (SOC)** 1) Setup of NOC and SOC 2) Design of operations model including detailed technical design 3) Undertake integration of tools and architecture and prepare a process for reporting requirement. 4) Deployment of manpower and certificate of their training 5) Switch-over Strategy 6) Emergency response procedures

#	Milestone	Output
7.	**User Acceptance and Go-Live (Iteration_1)**	**Acceptance Testing** 1) Confirmation of readiness of system 2) Formal submission of final versions of system (incl. ABIS/SDK) to be tested for Acceptance Testing and confirmation about the same. 3) Creation of Acceptance Testing environment, as per required specifications 4) Integration of test suite with ABIS/SDK 5) Development of logging tools for passive tests within the production environment 6) Generate artificial test data, if necessary 7) Acceptance of sample data 8) Participate and monitor the conduct of tests and review of test logs provided after the tests. 9) Investigate all errors discovered in system results to determine accuracy of test data. 10) Performing analysis of test logs and suggestions of re-test 11) Making necessary changes in the system as per the GoSL observations 12) Repeat the relevant activities for re-test 124. **Final Acceptance** 1) Deployment of the differential bill of material as per the Gap 2) Acceptance plan 3) Acceptance test cases and scenarios 4) Acceptance Test Plan 5) Acceptance Test Schedule 6) Acceptance Test Environment Inventory 7) Acceptance Test Summary Report 8) Acceptance Test Final Report
8.	**Operational Stabilization Period (Iteration_1)**	90 days period
9.	**Detailed Design**	1) Updated Functional Requirement Specifications (FRS)

#	Milestone	Output
	(Iteration_2)	2) Updated Use Case Design Document (UDD) 3) Updated Software Requirement Specification (SRS) 4) Updated High-Level design specification document including the UML use cases, UML designs, Conceptual Data Model, Logical and Physical Data Model for different application modules, API Specifications (Signature/Contract), Stored Procedures Specifications etc. 5) Updated Low Level design document, with detailed algorithms and logic of the important API's stored procedures etc. 6) Updated Low-level design and architecture documents for DC/DR infrastructure, platforms, software, security solutions, NOC/SOC, Network, etc., (covering Network architecture, storage architecture, security architecture, compute architecture, component architecture, integration architecture, data architecture, application architecture, deployment architecture, API architecture, virtualization, and container platform architecture) 7) Updated UI/UX Style Guide 8) Updated Traceability matrices with updated design features against the requirements
10.	**Second Software Release (Iteration_2 components)**	**Software** 1) Enhancements in components in Iteration_1 as per the enhancement identified during pilot. 2) Release and deployment on relevant environments (including production environment) 3) Source code of the applications with version control mechanism in the source code repository provided by GoSL. 4) Secure source code review 5) Integration of remaining COTs Solutions 6) Optimize the authentication by among others adjusting biometric authentication parameters / quality scores using existing data. 7) Biometric tests, Benchmarking and Acceptance **System Documentation** 1) Updated design documents (FRS, SRS, UDD, etc.) if any 2) Updated documentation (as applicable) for relevant components on installation guides, technical and product related manuals, frequently asked questions, user manuals, system administrator manuals, toolkit

#	Milestone	Output
		guides and troubleshooting guides, SOPs, procedures, policies, processes, etc. 3) Documents revised after previous milestones. 4) Design of fraud management process **Audits** 1) Carry out a Complete software audit for the Iteration 2 release and ensure Iteration 2 is complaint. 2) Carry out an Information Security audit for the complete end-to-end Iteration 2 release, including infrastructure, platform, etc. ensure Iteration 2 is complaint. 3) Facilitate the third-party independent Information Security audit carried out by GoSL ensure the Iteration 2 is complaint. **Training** 1) Updated Training Plan 2) Updated Training Material, Training Manual, Training Content, Conduct of Trainings, and Satisfactory assessment reports for Trainings. 3) Approved updated online tutorials, videos, presentations loaded on KMS. **Technical Helpdesk, NOC, SOC** 1) Deployment of additional manpower and certificate of their training as required
11.	**User Acceptance and Go-Live (Iteration_2)**	**Acceptance Testing** 1) Confirmation of readiness of system 2) Acceptance of remaining COTS Solutions. 3) Creation of Acceptance Testing environment, as per required specifications 4) Development of logging tools for passive tests within the production environment 5) Generate artificial test data, if necessary 6) Acceptance of sample data 7) Participate and monitor the conduct of tests and review of test logs provided after the tests. 8) Investigate all errors discovered in system results to determine accuracy of test data.

#	Milestone	Output
		9) Performing analysis of test logs and suggestions of re-test 10) Making necessary changes in the system as per the GoSL observations **Final Acceptance** 1) Deployment of the differential bill of material as per the gap 2) Acceptance plan 3) Acceptance test cases and scenarios 4) Acceptance Test Plan 5) Acceptance Test Schedule 6) Acceptance Test Environment Inventory 7) Acceptance Test Summary Report 8) Acceptance Test Final Report
12.	**Operational Stabilization Period (Iteration_2)**	
13.	**Operations and Maintenance** **(After Iteration 1 GO Live)**	**General** 1) Reports as per scope of work. 2) Methodology and Plan for undertaking a preventive maintenance (PM) 3) Monthly Support and Maintenance Report 4) Relevant documentation updates as required. 5) Report on proof of renewal of OEM support for all IT infrastructure i.e., hardware, software, etc. 6) Comprehensive reports on enrolment and authentication services on a daily, weekly, and progressive basis 7) Daily and weekly tracker of issues logged and rectification measures. **Project Management** 1) Project Management Weekly status review reports 2) ABIS and Data Quality Report 3) Incident Management Report 4) SLA monitoring report **Enhancement and Maintenance of SL-UDI Software System**

#	Milestone	Output
		including MOSIP Components 1) Continuous update and modification of the technical manual to align it with the GoSL's and GoSL's decision on releases on software system. 2) Monthly Issue Log for the errors and bugs identified and changes implemented in the solution. 3) Recommendations for improvement of enrolment software, ABIS, quality checks, manual de-duplication, and fraud management functions 4) Patch Release Management Process **Data Centers** 1) Data Centers Hosting Infrastructure 2) Policies for management of Primary Data Center and Disaster Recovery, backup and archival policy, and updated security policy 3) Continuous performance tuning, storage, network, virtualization, container platform performance benchmarking 4) Path management 5) Monthly Issue Log for the errors and bugs identified and changes implemented in the solution. 6) Configuration manual for OS, appliances, middleware etc. **IT Helpdesk** 1) Periodic Root Cause Analysis report **Business and Technical Services** 1) Forecast of demand of required assets 2) Asset management report containing assessment of required inventory, gaps and forecast of required asset. 3) Report on renewal of support for all IT infrastructure products and other system software's taken from OEMs. 4) Process for change and configuration management. 5) Storage management policy 6) Database administration guidelines 7) Backup and archival policy 8) Configuration manual for all software 9) Schedule of infrastructure augmentation requirements

#	Milestone	Output
		10) Detailed security architecture for the authentication services 11) IP Address Management Plan **Partner Management** 1) One-time creation, validation, update, and modification of technical manual for on boarding of enrolment officer. 2) Report on enrolments (center-wise, enrolment officer-wise reports, etc.) and on data quality. 3) Report on authentications. **Operations and Continuous Improvements** 1) Undertake necessary operations and coordination. 2) Identification and rectification of issues on continuous basis 3) Assessment reports 4) Logging of enhancements in hardware, software, security, network, etc. **Information Security and Business Continuity** 1) First time within 3 months of Go-live and review on a half- yearly basis subsequently, the following: a. SL UDI Security and Privacy Policy review and update b. Designing of Security and Privacy Procedures c. Minimum Baseline Security Standards (or referred as Hardening standards) d. Access management review e. Asset management review f. Change management review. g. Patch management review. h. Encryption review i. Backup review j. Biometric deduplication review k. Personnel security review l. Physical security review m. Security Operations Center (SOC) review n. BCP-DR drills

#	Milestone	Output
		o. Exception management review p. Internal security audit including vulnerability assessment and penetration testing. q. Risk assessment methodology design/review. 2) First time within 6 months of Go-live, and assessment on annual basis subsequently a. Risk assessment and treatment plan. b. Risk register. c. Privacy framework d. Privacy gap assessment and privacy impact assessment e. Privacy inventory 3) Annual a. Periodic secure source code review report 4) Half-Yearly Basis a. Periodic application security testing report b. Phishing simulation exercise report 5) Quarterly Basis a. Incident management review b. Data Leakage Prevention (DLP) and End Point Detection Response (EDR) review c. Periodic vulnerability assessment and penetration testing report d. Review and enhancement of existing fraud rules. 6) Monthly a. Comprehensive compliance dashboard (Monthly workshop / presentation to GoSL stakeholders every month with the updated tracker and dashboard) 7) Other frequencies a. Report on training and awareness (First time within 3 months of Go-live. Report on yearly basis subsequently) b. Security solution review and improvement report (First c. time 12 months after Go-live, and post this annually)
14.	**Transition and Exit Management**	1) Transition and Exit Management plan. 2) AMC support related documents, credentials for all OEM Products

#	Milestone	Output
		3) Inventory Details 4) Knowledge Management 5) Up-to-date source code 6) Up-to-date documentations 7) Final S&M report should consist of comprehensive knowledge transfer documentation.

Table 34: Implementation Milestones

Note: *This is an indicative list of deliverables the vender is expected to provide and deliver the entire SL-UDI solution.*

6.4 Transition to Managed Service Provider (MSP) –

The GoSL is planning to hire the services of a local partner, being referred to as the Managed Service Provider (MSP). This MSP will take-over the components in a gradual manner from the MSI. The MSI will be required to work collaboratively with the MSP to achieve the objectives of the project and to enable the MSP to operate and maintain the components transitioned to it by the MSI. **(Refer Annexure 6: Exit Management)**

~~7~~ Schedule of Requirements

An indicative Schedule of Requirements is given below. The MSI is expected to submit the complete Bill of material as per the schedule of requirements in Vol 1 during proposal submission.

(i) The devices mentioned in the tender is just indicative, the bidder is expected to provide the require no of devices, hardware based during the requirement analysis Phase.

(ii) During the validity period of the contract, if any of the machines/chips/parts becomes unavailable in the market, the MSI will be bound to supply the next higher version/configuration/family of the machines/chips /parts/devices/ another component with no additional cost to the GoSL.

#	Product and /or Service Item Description	Units	QTY
Software			
1.	Modular Open-Source Identity Platform (MOSIP)	Items	
2.	Biometric SDK	Items	
3.	Automated Biometric Identification System	Items	
4.	Portal Solution	Items	
5.	Mobile Application	Items	
6.	Queue Manangement System	Items	

#	Product and /or Service Item Description	Units	QTY
7.	Customer Relationship Management	Items	
8.	BI & Reporting Solution	Items	
9.	Document Management System	Items	
10.	Fraud Management System	Items	
11.	Service Billing System	Items	
12.	Knowledge Management System	Items	
13.	Learning Management System	Items	
14.	TSP and UA Software	Items	
15.	API Gateway	Items	
16.	Business Rules Engine	Items	
17.	Application and Web Server	Items	
18.	Application Performance Monitoring (APM) and full Stack Observability	Items	
19.	Version management	Items	
20.	Operating System	Items	
21.	Database Solution	Items	
22.	Performance Testing Tool	Items	
23.	IT Service Management Tools	Items	
24.	Enterprise Management System	Items	
25.	SLA Monitoring	Items	
IT Infrastructure			
26.	Blade Servers (Biometric Solution)	Items	

#	**Product and /or Service Item Description**	**Units**	**QTY**
27.	Blade Chassis (Biometric Solution)	Items	
28.	Rack Server (Biometric Solution)	Items	
29.	Server Rack (Biometric Solution)	Items	
30.	SAN (Biometric Solution)	Items	
31.	SAN Switch (Biometric Solution)	Items	
32.	Tape Library and Tapes (Biometric Solution)	Items	
33.	Blade Servers (Other than Biometric Solution)	Items	
34.	Blade Chassis (Other than Biometric Solution)	Items	
35.	Rack Server (Other than Biometric Solution)	Items	
36.	Server Rack (Other than Biometric Solution)	Items	
37.	SAN (Other than Biometric Solution)	Items	
38.	SAN Switch (Other than Biometric Solution)	Items	
39.	Tape Library (Other than Biometric Solution)	Items	
40.	Backup Media Storage Fire Safe at DC & DR location of needed capacity	Items	
41.	DNS, DHCP and IPAM	Items	
42.	Internet Router (For entire infrastructure)	Items	
43.	MPLS Router (For entire infrastructure)	Items	
44.	Global Load Balancer (For entire infrastructure)	Items	
45.	Application Load Controller - Server/Application Load Balancer (For entire infrastructure)	Items	
46.	SDN And Spine Switches (For entire infrastructure)	Items	
47.	Leaf Access Switches (For entire infrastructure)	Items	
48.	Replication and Backup Solution (Note: MSI and BSP may bring same solution or their separate solutions)	Items	

#	Product and /or Service Item Description	Units	QTY
49.	Network Access Controller	Items	
50.	Virtualization Solution	Items	
51.	Enterprise Container Application Platform	Items	
52.	Enterprise Grade Object Storage Solution	Items	
NOC / SOC			
53.	Laptop (for manager and L1 analysts)	Items	
54.	Desktops Monitors for NOC & SOC Agents	Items	
55.	IP Phone	Items	
56.	IP PABX	Items	
Field Infrastructure			
57.	Dual Screen Monitor	860	
58.	Enrolment Fingerprint Scanner (4-4-2)	860	
59.	Enrolment Iris Scanner (Dual)	1612	
60.	Signature Pad	860	
61.	Auth- Fingerprint scanners	100	
62.	Auth - Facial Scanner	100	
63.	Auth - Iris Capture Device	100	
64.	Enrolment Kit Container for registration kits	1612	
65.	Laptop for registration kits	1612	
66.	Web Camera	1612	
67.	Multi Function Device (Printer cum Document Scanner)	1612	

#	Product and /or Service Item Description	Units	QTY
68.	White Background Screen (4 ft X 3 ft)	1612	
69.	USB Hub 2.0/3.0 minimum 5 ports	860	
Mobile Registration KITS			
70.	Enrolment Kit Container for mobile registration kits	40	
71.	Laptop for mobile registration kits	40	
72.	Document Scanner cum Printer	40	
73.	Enrolment - Fingerprint Scanner (4-4-2)	40	
74.	Enrolment - Iris Scanner (Dual)	40	
75.	Web Camera	40	
76.	Signature Pad	40	
77.	+50000 MAH battery	40	
78.	USB Hub 2.0/3.0 minimum 5 ports	40	
79.	Internet Dongle	Items	GoSL Responsib ility
80.	USB Storage Device for mobile registration kits	40	
81.	White Background Screen (4 ft X 3 ft)	40	
Network Connectivity			
82.	Data Center – Interconnection Network	MSI to provide bandwidth sizing	GoSL Responsib ility
83.	Data Centers (DC & DR) – Internet Links	MSI to provide bandwidth sizing	GoSL Respponsi bility

#	Product and /or Service Item Description	Units	QTY
84.	Internet Connectivity for mobile registration centers	MSI to provide bandwidth sizing	GoSL Respponsibility
85.	Data Centers (DC & DR) – NOC / SOC/ Technical Helpdesk	MSI to provide bandwidth sizing	GoSL Respponsibility
Security			
86.	DLP Solution	Items	
87.	Network Vulnerability Scanner	Items	
88.	Anti-Advanced Persistent Threat (APT)	Items	
89.	Privilege Access Management (PIM/ PAM)	Items	15
90.	Two Factor Authentication	Items	
91.	Web Gateway with content Filtering & Proxy Solution	Items	
92.	Application Vulnerability Scanner	Items	
93.	Code Review Tool	Items	
94		Items	
95.	Identity and Access Management	Items	
96.	Hardware Security Module	Items	
97.	Security Information and Event Monitoring (SIEM) Solution (SOAR not to be included . This can be procured later via change control)	Items	
98.	Anti-DDoS solution as a Service from GoSL Telecom Service Provider	Items	GoSL Responsibility
Security Component (Hardware)			

#	Product and /or Service Item Description	Units	QTY
99.	Patch Management Solution	Items	
100.	~~Email Gateway (Security Solution)~~	~~Items~~	
101.	Database Activity Monitoring	Items	
102.	SSL VPN	Items	
103.	External Firewall	Items	
104.	Internal Firewall	Items	
105.	Web Application Firewall	Items	
106.	Host Intrusion Prevention System	Items	
107.	Network Intrusion Prevention System (NIPS)	Items	
108.	Security Racks (same as other racks)	Items	
109.		Items	
110.	Network Detection and Response	Items	
111.	Container Runtime Security and East west Traffic Inspection and Attack Mitigation Solution	Items	
112.	Extended Detection and Response Solution	Items	
Other Tools			
113.	Specify if any	Items	

Table 35: Bill of Martial

8 Change Request

Given below are details on the Change Request Process at a very high-level based on the Change Management policy.

#	Deliverables	Phase	Duration
1.	CR proposal including effort.	Estimation	-

2.	2.1 Proper maintenance of source code in repository provided by GoSL. 2.2 Updated Solutions installation guide (if applicable) 2.3 Updates User manual with enhancements (if applicable) 2.4 Functional Test Cases, Non-Functional Test Scripts and Test Results 2.5 UAT Test Cases & Successful UAT acceptance 2.6 User training for assignments (if applicable) 2.7 Updated Detailed Software Technical Documentation (DSTD) (if applicable) 2.8 QA Release Notes 2.9 User manuals (if applicable) 2.10 Administrator manuals (if applicable)	Implementation	Agreed duration for the CR

Table 36: Change Request

9 Compliance to Schedule of Requirements

The supplier shall provide the consent for the Schedule of requirements as described in Volume 2.

#	**Schedule of Requirement**	**Description**	**Compliance (Y/N)**	**Remarks**
1.	Volume 2 : Schedule of Requirements	Scope of Work		
2.	Annexure 1A : As-Is Functional System	Existing Functional System		
3.	Annexure 1: High Level Process Flow	DRP Process Flow		
4.	Annexure 2 : Non Functional Requirements	System Non-Functional Requirements		
5.	Annexure 3 : Minimum Technical Specification	Technical Specifications		
6.	Annexure 4 : Software Engineering	Software Engineering Practices		
7.	Annexure 5 : Demand Capacity	Demand Capacity for Enrollment		
8.	Annexure 6 : Exit Management	Exit Management		
9.	Annexure 7 - Project Management and Governance	Project Management Procedures		

10.	~~Annexure 8 Biometric Device Certification~~	~~Device Certification Process~~		**Deleted**
11.	Annexure 9- Service Level	Description of Service levels		
12.	Annexure 10 – Manpower Requirement	Manpower for the Project		
13.	Annexure 11: Overview of Technology	Technology Functional Specifications		
14.	Annexure 12: Project sites/sites	Project Enrollment Sites and Other Sites		
15.	Annexure 13: Card Printing and Personalization Technology	Card Printing and Personalization Facilities		
16.	Annexure 14: List of Indicative Trainings	Type of Indicative Trainings		
17.	Annexure 15: Transition Framework	Transition Framework		
18.	Annexure 16: RACI Framework	RACI Framework		

Table 37: Compliance Sheet

Note: *The MSI is expected to provide compliance of the Components of the Schedule of Requirements above item by marking 'Y/N' as mentioned in the respective table. And reasons for non-compliance can be provided in the remarks column. Further list down any deviations and out of scope components in the remarks column.*