THE GOVERNMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

Ministry of Technology

BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS

Volume 02 of 03

Single Stage Two Envelopes Bidding Procedure

FOR THE

PROCUREMENT OF A MASTER SYSTEM INTEGRATOR (MSI) FOR DESIGNING, DEVELOPING, SUPPLYING, DELIVERING, INSTALLATION, IMPLEMENTING, SUPPORT AND MAINTAINING THE SOFTWARE, HARDWARE AND INFRASTRUCTURE FOR SRI LANKA UNIQUE DIGITAL IDENTITY (SL-UDI) PROJECT OF GOVERNMENT OF SRI LANKA

INVITATION FOR BIDS No: **ICTA/SLUDI/IS/2022/01**

May 07, 2023

Table of Contents

List of Tables

List of Figures

Disclaimer:

If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are not authorized to and must not disclose, copy, distribute, or retain this message or any part of it.

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.

ICTA is the apex ICT institution of the Government. In terms of the Information and Communication Technology Act No. 27 of 2003, (ICT Act) ICTA has been mandated to take all necessary measures to implement the Government’s Policy and Action Plan in relation to ICT. In terms of Section 6 of the ICT Act, ICTA is required to assist the Cabinet of Ministers in the formulation of the National Policy on ICT and provide all information necessary for its formulation.

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 as the key stakeholder of the project.

By now, ICTA as the implementation / execution agency of the SL-UDI project 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, ICTA intends to expedite the implementation of the SL-UDI through an accelerated time period.

ICTA 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.

DRP intends to carry out the circa 17.5 million citizen registrations, through circa 1,600 enrolment centres, within a 1.5 year time period.

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.

Further, currently there is no such government initiative intending to issue digital identifiers to citizens. This fact emphasizes the timely need for rapidly executing the proposed project.

1.3 Objectives of the Project

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

The ICTA 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, please refer to Annexure-6. 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) Supply, installation, commissioning and maintaining the 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 a 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

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

#	Department / Agency	Role
1	Department of Registration of persons (DRP)	• Overall owner and data custodian of the SL-UDI project.
2	ICT agency of Sri Lanka (ICTA)	• Technical leaders for SL-UDI project. • Design, implementation, and execution owner for the SL-UDI program.
3	Department of Immigration and Emigration	• Association of SL-UDI number for citizens obtaining citizenship by the respective DRP Act.

#	Department / Agency	Role
5	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.
6	Department of Elections	• Verification of Voter Registry
7	Ministry of Home Affairs	• Verification of Householder Registry
8	Master System Integrator (MSI)	• For the provision of services as described in this document.
9	Managed Service Provider	• Work collaboratively with the 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 ICTA/DRP after the OAT • Operate and maintain the components transitioned to it by the MSI
10	Audit agency	• Independent audit agency for the SL-UDI program
11	Relying parties	• Organizations that are leveraging the authentication services of the SL-UDI program

Table 1 : Stake Holder Responsibilities

1.5 Adopted Standards (Demographic, Biometric, etc.)

Following are the standards adopted but not limited to,

S. No.	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 ICTA and DRP
11.	Date Formats	
12.	Location Names and Codes	
13.	Address Formats	
PKI Infrastructure		
14.	Digital Signature Standard	FIPS 186-4
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

S. No.	Description	Proposed Standard
18.	Public Key certificates	ITU-T X-509, ISO 9594-8
19.	XML Digital Signature	W3C / ETSI XAdES
Unique Digital Identity Number		
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	ISO/IEC 18004:2015— Quick Response (QR) code and PDF417 / QR code
Other Standards[1]		
29.	Security	ISO 27001, 27002, NIST Cybersecurity Framework
30.	Privacy	ISO/IEC 27701, 29100, 27018, 29184, NIST Privacy Framework
31.	Management	ISO/IEC 24760 Series
32.	Risk Management	ISO/IEC 31000, 27005
33.	Quality Management	ISO/IEC 25010, 9001, 9004
34.	ID Federation	OIDC + OAuth (RFC 6749) / SAML (SAML v2 – 2005)

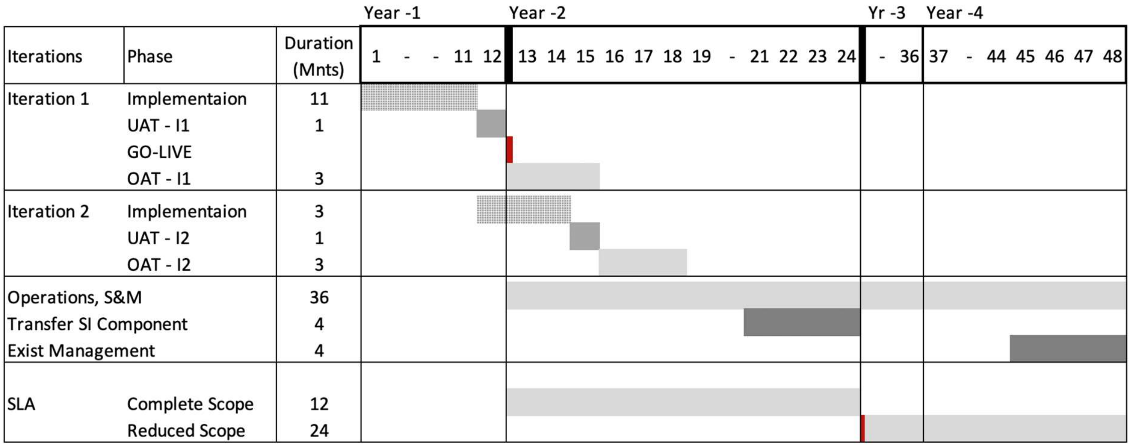
Table 2 :standards adopted

[1] Source: World Bank (https://documents1.worldbank.org/curated/en/707151536126464867/pdf/129743-WP-PUBLIC-ID4D-Catalog-of-Technical-Standards.pdf)

1.6 Targeted Performance Parameters (Throughput, Accuracy, Availability)

The SL-UDI should be designed considering the 10-year scale (2023 – 2032) i.e., population size of 26 million citizens. In addition, the SL-UDI number should be designed considering the population scale of 100-year and extendibility of this number to corporates, and other entities. For the duration of the project, the following targeted performance parameters are expected to be adhered to: *Refer the annexure 5 demand capacity.*

1.7 Project Duration



Iterations	Phase	Duration (Mnts)
Iteration 1	Implementaion	11
	UAT - I1	1
	GO-LIVE	
	OAT - I1	3
Iteration 2	Implementaion	3
	UAT - I2	1
	OAT - I2	3
Operations, S&M		36
Transfer SI Component		4
Exist Management		4
SLA	Complete Scope	12
	Reduced Scope	24

Figure 1 : SL-UDI Project Duration

The TOTAL duration of the project is the SL-UDI framework implementation period plus 3-year support and maintenance. The overall duration of the project implementation is 48 months. Within the aforementioned timelines, first 11th 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 be commencing from the 12th month upon Go-Live of iteration 1. Within the period between Release_1 and Release_2, the stabilization, and Operational Acceptance Test (OAT) needs to be completed. After the Release_2, the remaining 30 months (also referred to as "steady state operations period") for steady state operations within this period last 4 months will be allocated for comprehensive knowledge transfer and exit management.

1.8 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 entire hosting infrastructure and security infrastructure.

(ii) The MSI will be responsible for biometric (enrolment and authentication devices) as well as biometric software (ABIS, SDK, Manual Adjudication, etc.) and corresponding hosting infrastructure (server, storage, tape library, etc.)

(iii) The MSI will be responsible for registration kits (excl. the components brought by BSP and excl. the existing components available with DRP).

(iv) The MSI will be responsible for colocation space of primary site and secondary site including the interconnection link.

The MSI will be responsible for providing the field network at registration centres, wide-area network, and other network connections required under this project.

The ICTA 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.

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)

The key elements of procurement and their corresponding providers are provided in the table given below, the detailed minimum technical specification is provided as Annexure-3:

#	Solution Component	Provider
Software		
1.	Pre-registration Application (based on MOSIP)	MSI
2.	Registration Software (based on MOSIP)	MSI
3.	Identity Management System (based on MOSIP)	MSI
4.	Unique Identity Generator (based on MOSIP)	MSI
5.	Authentication Solution (based on MOSIP)	MSI
6.	Partner and Device Management (based on MOSIP)	MSI
7.	Integration Middleware	MSI
8.	Biometric SDK	BSP

#	Solution Component	Provider
9.	Automated Biometric Identification System	BSP
10.	Portal Solution	MSI
11.	Customer Relationship Management	MSI
12.	BI & Reporting Solution	MSI
13.	Document Management System	MSI
14.	Fraud Management System	MSI
15.	Service Billing System	MSI
16.	Knowledge Management System	MSI
17.	Learning Management System	MSI
18.	Trusted Service Provider (TSP) and User Agency (UA) Software	MSI
19.	Enterprise Service Bus	MSI
20.	API Gateway	MSI
21.	Business Rules Engine	MSI
22.	Business Process Management Suite	MSI
23.	Application Server and Container	MSI
24.	Web Server	MSI
25.	Distributed Caching	MSI
26.	Program / Project Management Tool	MSI
27.	Version management	MSI
28.	Virtualization Software	MSI
29.	Operating System	MSI
30.	Database Solution	MSI

#	Solution Component	Provider
31.	Performance Testing Tool	MSI
32.	Messaging Platform - Publish/Subscribe Queues	MSI
33.	Large-Scale Random-Access Storage	MSI
34.	IT Service Management Tools	MSI
35.	Enterprise Management System	MSI
36.	Replication and Backup Solution (Note: MSI and BSP may bring same solution or their separate solutions)	MSI and BSP
37.	Network Access Controller	MSI
38.	Email Solution	MSI
Data Centre Space		
39.	Data Centre Hosting Space (Primary Site)	MSI
40.	Data Centre Hosting Space (Secondary Site)	MSI
Hardware (Server Side)		
41.	Blade Servers (Biometric Solution)	BSP
42.	Blade Chassis (Biometric Solution)	BSP
43.	Rack Server (Biometric Solution)	BSP
44.	Server Rack (Biometric Solution)	BSP
45.	SAN (Biometric Solution)	BSP
46.	SAN Switch (Biometric Solution)	BSP
47.	Tape Library and Tapes (Biometric Solution)	BSP
48.	Blade Servers (Other than Biometric Solution)	MSI
49.	Blade Chassis (Other than Biometric Solution)	MSI

#	Solution Component	Provider
50.	Rack Server (Other than Biometric Solution)	MSI
51.	Server Rack (Other than Biometric Solution)	MSI
52.	SAN (Other than Biometric Solution)	MSI
53.	SAN Switch (Other than Biometric Solution)	MSI
54.	Tape Library (Other than Biometric Solution)	MSI
55.	Virtual Tape Library (Other than Biometric Solution)	MSI
56.	Internet Router (For entire infrastructure)	MSI
57.	MPLS Router (For entire infrastructure)	MSI
58.	Global Load Balancer (For entire infrastructure)	MSI
59.	Application Load Controller - Server / Application Load Balancer (For entire infrastructure)	MSI
60.	Core Switches (For entire infrastructure)	MSI
61.	Access Switch LAN (For entire infrastructure)	MSI
62.	Data Center Access Switches (For entire infrastructure)	MSI
63.	Enterprise Management System	MSI
64.	Replication and Backup Solution	MSI
65.	Network Access Controller	MSI
Network Connectivity		
66.	Data Centre – Interconnection Network	MSI
67.	Data Centres (DC & DR) – Internet Links	MSI
68.	WAN Connectivity at field offices (fixed registration centres)	MSI
69.	Internet Connectivity for mobile registration centres	MSI
70.	Data Centres (DC & DR) – NOC	MSI

#	Solution Component	Provider
71.	Data Centres (DC & DR) – SOC	MSI
72.	Data Centres (DC & DR) – Contact Centre	MSI
73.	Data Centres (DC & DR) – Technical Helpdesk	MSI
74.	Data Centres (DC & DR) – DRP Hosting Infrastructure	MSI
75.	Data Centres (DC & DR) – DRP Head Office	MSI
76.	Data Centres (DC & DR) – ICTA Head Office	MSI
Field Infrastructure		
77.	Location, Civil and Electrical Work	DRP
78.	Fingerprint Scanner (enrolment and authentication)	Please refer to 5.3field Infrastructure.
79.	Iris Scanner (enrolment and authentication)	
80.	Web Camera (enrolment)	
81.	Digital Camera (authentication)	
82.	Laptop for mobile registration kits	
83.	Desktop for fixed registration kits	
84.	Additional Monitor	
85.	Scanner	
86.	Printer	
87.	USB Hub	
88.	Background Screen	
89.	Flashlight	
90.	Enrolment Kit Container for mobile registration kits	
91.	USB Storage Device for mobile registration kits	
Security Component (Software)		

#	Solution Component	Provider
92.	DLP Solution	MSI
93.	Network Vulnerability Scanner	MSI
94.	Anti-Advanced Persistent Threat (APT)	MSI
95.	Privilege Access Management	MSI
96.	Two Factor Authentication	MSI
97.	Web Gateway with content Filtering & Proxy Solution	MSI
98.	Web Vulnerability Scanner	MSI
99.	Code Review Tool	MSI
100.	Anti-Virus Solution	MSI
101.	Virtual Desktop Infrastructure Solution	MSI
102.	Identity and Access Management	MSI
Security Component (Hardware)		
103.	Hardware Security Module	MSI
104.	Anti-DDoS solution	MSI
105.	Security Information and Event Monitoring (SIEM) Solution	MSI
106.	Patch Management Solution	MSI
107.	Email Gateway (Security Solution)	MSI
108.	Database Activity Monitoring	MSI
109.	SSL VPN	MSI
110.	External Firewall	MSI
111.	Internal Firewall	MSI
112.	Web Application Firewall	MSI
113.	Host Intrusion Prevention System	MSI

#	Solution Component	Provider
114.	Network Intrusion Prevention System (NIPS) and NIDS	MSI
115.	Intrusion Detection System / Intrusion Prevention System	MSI
116.	Security Racks (same as other racks)	MSI
117.	Security Testing Solution	MSI

Table 3 : Elements of procurement

1.9 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 purpose. In addition to this, please read the entire RFP to clearly understand their roles and responsibilities.

S. No.	Item	Responsibility
Knowledge Transfer and Support		
1.	MOSIP KT	MSI can access the relevant documentation from MOSIP's website. MOSIP team will provide a detailed training and knowledge transfer to the MSI's project team for a period of about 4 to 6 weeks. The MSP can also join the KT sessions along with MSI.
2.	L3 Support	MOSIP will provide technical (L3) support for its components. The MSI will be responsible to raise the ticket in the MOSIP's website and coordinate with MOSIP for the resolution. As part of ticket, the MSI will 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 to obtain enterprise support, as available, for the technology stack[2] (tools and technologies) based on which MOSIP has been developed.

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

S. No.	Item	Responsibility
Enrolment (Field Aspects)		
4.	Biometric SDK	BSP will provide the Biometric SDK and MSI will integrate the registration client and other components of MOSIP
5.	Registration Client	MSI will provide the registration client software (customize MOSIP and undertake necessary integrations), install it in the registration kits, maintain the software and provide technical support
6.	Biometric Capture Devices	The MSI will provide the biometric captures devices, deploy them with biometric registration kit, should be integrated with MOSIP, provide its technical support & maintenance, provide replacement devices (using spares), and provide comprehensive onsite warranty (troubleshooting, pickup of devices with issues from registration centres, and drop of working devices to registration centres) The MSI has to provide the device management server as well as foundation trust module.
7.	Registration Kit (other than Biometric Capture Devices)	MSI will provide the registration kit hardware, provide maintenance and warranty for the corresponding components it supplies under this project. The staff at registration centres will be equipped with basic diagnosis (as per training by MSI) and thereafter they may raise the tickets on helpdesk for repair/replacement of any faulty devices/components. MSI will provide the technical helpdesk (incl. tickets management), provide remote support, provide on-site troubleshooting, escalate, and monitor the tickets to the respective agencies, provide warranty claim/replacement, etc. For the components provided by DRP, the escalation will be done to the DRP team who will in-turn be responsible for warranty claim or replacements.

S. No.	Item	Responsibility
8.	Queue Management Software and Hardware.	The DRP will be responsible to provide the queue management software, provide television displays for tokens, etc. The DRP will setup necessary network wiring at registration centres. The DRP 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 centres.
9.	Registration Manpower	DRP 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 to plan training, develop training content, conduct trainings, conduct certification examination, and provide certificates to the registration manpower.
11.	Registration related issue identification and resolution	**Self-Diagnosis:** The staff at registration centres will be equipped with 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, MSI, 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 issue. First level of remote diagnosis will be performed by MSI. In case of issues with biometric devices, the next level of remote diagnosis 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/DRP. The

S. No.	Item	Responsibility
		necessary software for remote support should be provided by the MSI. **Onsite Troubleshooting:** For issues unresolved through remote support, the MSI will do the first level of on-site troubleshooting. If issue remains unresolved, then escalate it to the concerned agencies (MSI software, BSP, DRP, etc.). For issues concerning the biometric capture devices, the BSP will be responsible to resolve the issue by operationalizing the device at registration centre (if feasible) or provide spare as replacement, picking up the device from registration centre, repairing it in its service centre, and dropping the operational device at the registration centre and connecting it to the registration kit. Similar process will be followed for the other non-biometric components of registration kits by the MSI. **Management, Monitoring and Reporting:** The MSI will be responsible to manage the tickets, monitor their resolution (including timely escalations), and submit 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, and Integration Middleware)	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 1.8)	MSI will provide software (customize COTS/OTS, develop the bespoke software and undertake necessary integrations), finalize requirements for central infrastructure, install it in the central infrastructure, operate & maintain the software, and provide technical support.

S. No.	Item	Responsibility
14.	Biometric Components (ABIS and Manual Adjudication)	BSP will provide software (customize COTS and integrate with MOSIP with assistance from MSI), provide infrastructure and install software on it, operate & maintain the software, and provide technical support.
15.	Quality Assurance	The DRP will provide the manpower for review and approval of the enrolment packet as per their processes. The MSI will require to develop the necessary software-based workflow to support these requirements. Please refer to the annexure for details.
16.	Manual Adjudication	
17.	Unique Number Generation and Allocation	Refer 'Components based on MOSIP'
Personalization, Issuance and Activation of Card		
18.	Card Personalization and Issuance	DRP 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 DRP. 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 DRP to undertake necessary customization in the card personalization software for integration with the aforementioned APIs.
19.	Card Management and Workflow	The DRP 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.
20.	Card Activation	At the time of issuance, the card is in inactive state and before usage of card, it needs to be activated. MSI needs to build and provide the functionality to activate the cards in both online and offline manner.

S. No.	Item	Responsibility
		• Facility to activate the Card through DPR head office. • Facility to activate the Card at GN Office • Facility to activate the Card through internet. • Facility to activate the Card through SMS • Facility to activate the Card when card is used for the first time at an instance of the electronic transaction (E.g.: Bank)
Authentication		
21.	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 applications in all these languages (Java, PHP, JavaScript (NodeJS)). The MSI will provide necessary documentation and technical support for the TSPs and UAs to deploy this software at their end.
22.	Onboarding of Authentication Partners	MSI will extend necessary technical support to the Authentication Partners for onboarding them as TSPs, and/or UAs.
Grievances		
23.	Grievance Management	MSI will provide necessary solution for end-to-end grievance management.

Table 4 : Key Considerations

2 Functional Overview

The enrolment process has four major stages i.e. (i) pre-enrolment stage, (ii) enrolment stage, (iii) enrolment processing stage, and (iv) card personalization, issuance, and activation stage. The list of steps in these stages are identified in Annexure 1: DRP Flow.

3 Project Scope

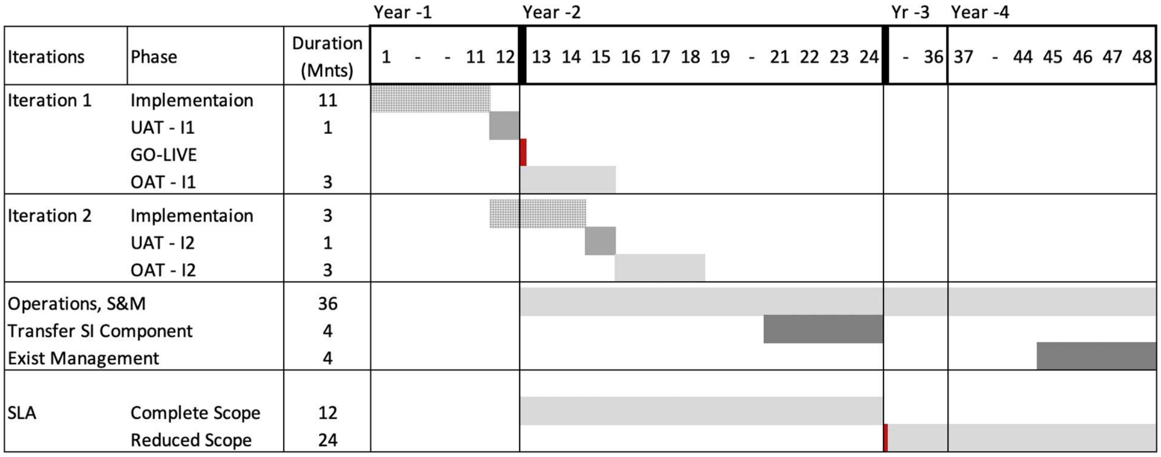
3.1 Introduction

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	Implementation of Systems Infrastructure, including the Data Center and Disaster Recovery Sites. Includes Co-location services and connectivity to and between DC/DR sites.	
2	Implementation and maintenance of the Automated Biometric Identification System solution (ABIS).	
3	Leverage the MOSIP platform to design and implement a foundational Identity platform solution for GoSL, back-office solution for the Department of Registration of Persons, and related integrations, in order to carry out citizen enrolment and issuance of digital identity.	
4	Supply and maintain enrolment and authentication devices for fingerprint, dual iris scanner, face including device management server together with microphone, speakers and signature pads.	
5	Implementation of Commercial off-the-shelf (COTs) products	
6	Implement the biometric SDK solution, the Manual Adjudication solution and related integrations.	
7	Implement and operationalize the operations and support centers – IT Help Desk, Network Operations Center, Security Operations Center.	The building and physical infrastructure will be provided by GoSL.
8	Operationally support, Support and maintain the above components for 3-years.	

Table 5: Key Components

The MSI will be the lead party responsible for providing end to end solution for the SL-UDI project. The MSI is required to design, develop, supply, deliver, install, implement, support and maintaining 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 is proposed to implement the Minimum Viable Product (MVP) of the SL-UDI framework (as Iteration 1) within 12-months, and support and maintain the SL-UDI framework for 3-years from the launch (go-live).



Iterations	Phase	Duration (Mnts)
Iteration 1	Implementaion	11
	UAT - I1	1
	GO-LIVE	
	OAT - I1	3
Iteration 2	Implementaion	3
	UAT - I2	1
	OAT - I2	3
Operations, S&M		36
Transfer SI Component		4
Exist Management		4
SLA	Complete Scope	12
	Reduced Scope	24

Figure 2 : SL-UDI Project Duration

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 MVP 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.

c. 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 OAT. Therefore, the Operational Acceptance (OAT) 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.

3.2 SL-UDI Operations, Support and Maintenance

i. Citizen's biographic, demographic and biometric information which are 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.

ii. Therefore, it is of critical importance that the citizens data are securely managed. Key considerations for the implementation of the SL-UDI includes following.

a. Privacy by design and Security by design consideration for the implementation of the SL-UDI framework.
b. The SL-UDI designed in accordance with the guidelines of the Personal Data Protection Act No 9 of 2022.
c. The SL-UDI data ownership clearly defined.
d. The SL-UDI design demands data being encrypted wherever possible.
e. User Access to SL-UDI confined within the Country.
f. The SL-UDI framework design leveraging on a Modular Open-Source Identity Platform (MOSIP) framework to enable GoSL to administer, access control and operationally manage the SL-UDI framework.

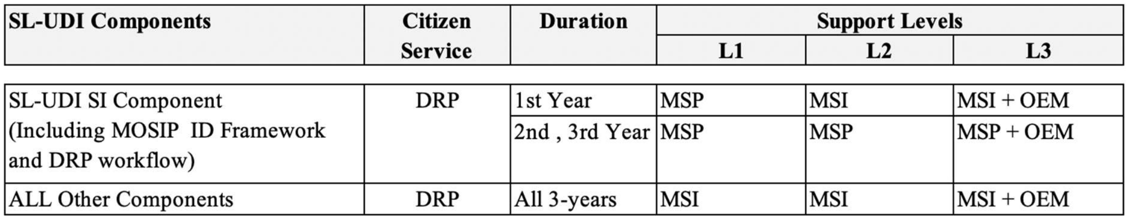
iii. Service providers responsible for implementing and operationally managing the SL-UDI framework.

a.	The Master Systems Integrator (MSI) – An Indian firm procured through competitive procurement by GoSL, funded through the GoI grant assistance.	1. Responsible for Implementing 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	2. Managed Service Provider for ICTA, responsible for the overall operations, audit, and governance of the SL-UDI. 3. Responsible for administration, access control and operations management of the SL-UDI Framework. 4. Responsible for taking over the SL-UDI MOSIP ID Framework and DRP workflow including related COTS from the MSI at the end of the 1st year support time period. 5. Providing Level 01 support for selected key components.

iv. Following control aspects of the SL-UDI Framework will be managed by ICTA or entrusted with the Managed Service Provider (MSP) as mentioned in the table below. MSP and MSI Shared responsibility Matrix

	#	**Description**	**From go-live onwards**	**OAT Acceptance (Iteration 1) onwards**	**1 year after go-live onwards**
	SL-UDI Administration, access control and operations management.				
1	Privileged Access Management/ Identity Access Management/ SSL VPN and remote access management / Database Activity Monitoring/ Required Perimeter level Access.				
	i	Access Control and Administration, Operational Management	MSP		
	ii	Fully Ownership including update/upgrade, enhance, availability, etc.		MSP	
2	Hardware Security Module (HSM)				
	i	Fully Custody (Access Control and Administration, Operational Management, Fully Ownership including update/upgrade, enhance, availability, etc.)	MSP		
3	MOSIP, DRP workflow, Related COTS				
	i	Access Control and Administration, Operational Management via item no 1 above mentioned.	MSP		
	ii	Fully Ownership including update/upgrade, enhance, availability, etc.			MSP
4	Access to Infrastructure and Core Data (Including all DBs and Objects Storages)				
	i	Govern and Monitor via Item #1 (mentioned above)	MSP		

v. SL-UDI Support arrangement.



SL-UDI Components	Citizen Service	Duration	Support Levels		
			L1	L2	L3
SL-UDI SI Component (Including MOSIP ID Framework and DRP workflow)	DRP	1st Year	MSP	MSI	MSI + OEM
		2nd , 3rd Year	MSP	MSP	MSP + OEM
ALL Other Components	DRP	All 3-years	MSI	MSI	MSI + OEM

Figure 3 :SL-UDI Support arrangement.

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

b. Support Levels for SL-UDI components (including the MOSIP IF Framework and the DRP workflow):
    - During the 1st year Support and maintenance time period, the MSP 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, DRP workflow and related COTS from MSI. MSI will no longer have access to this component. Therefore from 2nd year onwards, the MSP will be responsible for L2 and L3 support.

c. Support Levels for all other components of the SL-UDI:
    - MSI is required to provide L1, L2 and L3 support.
    - The MSI is expected to provide the support services through Sri Lankan based local organization in accordance with the sub-contractor criteria specified.

4 Solution Overview

SL-UDI Software system shall contain the 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.

5 Scope of Services

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

1.1. The MSI is responsible for the design, develop, deploy, support, and maintain the of the foundation ID platform in line with the given timeline.

1.2. The MSI's scope of work includes procuring, commissioning, configuration, implementation, integration, deployment, and maintenance of the entire SL-UDI system and it's components.

1.3. The MSI should conduct a system requirement study of the processes and review and understand the scope and functionalities required to implement the SL-UDI Foundational ID platform. Deviations 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 to ICTA.

1.4. The MSI should provide detail cutover plan and pilot roll out plan. Upon providing the plan the approval must be taken by ICTA/DRP.

1.5. On completing the above, a Detailed Software Requirements Specification (DSRS) and a Detailed Software Technical Design (DSTD), including the proposed solution architecture document, should be submitted. Accordingly, the MSI shall prepare and submit a detailed design and solution architectures such as server architecture, network architecture, database architecture, security architecture, deployment architecture.

1.6. If any COTS / OTS components are proposed as a part of the proposed design, the MSI shall conduct a detail requirements phase and produce a detailed functional specifications and design specifications, system architecture design, design principles/considerations, etc.

1.7. If any COTS components are proposed as a part of the proposed design, the MSI shall clearly indicate the resultant commercial impact (like software, license, enterprise level annual support, etc.) both for initial delivery and during subsequent operations in the bid submission. Further, a cost-benefit analysis should be provided to ICTA. Also, the MSI should facilitate and support in assisting ICTA to finalize agreement with Original Equipment Manufacturer (OEM) for all COTS licenses. The MSI shall obtain a certification from the OEM that the quoted products are not End of Support (EoS) and not End of Life (EoL). The OEMs whose products are offered must have their own Support Center. The MSI is responsible for coordinating with all Technical Assistance Center (Support Centres) for all issues. It should be noted that if any commercial expenses arising as a result of the detailed requirement study should be borne by the MSI.

1.8. MSI shall be responsible for operations, maintenance, and support of COTS/OTS solution as part of the Application Maintenance and Annual Technical Support from OEM including associated updates and upgrades.

1.9. All patches and upgrades from OEMs shall be implemented by the MSI where it's subject to 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.

1.10. Upon obtaining approval from the committee appointed by ICTA for the above, the MSI should design and develop the Foundation ID platform.

1.11. The implementation shall span across the following stages of software development lifecycle.

a) Requirement verification
b) Development and customization
c) Set-up of environment (refer Section 0) including required tools
d) Unit Testing, System Testing, Integration Testing, Performance Testing
e) UAT, OAT
f) Release management
g) Continuous build (Continuous Integration, Continuous Deployment)
h) Deploy
i) Audits – Compliance Audits, Information Security, Process Audits
j) Enhancement
k) Change request.
l) Technical Support, Troubleshooting, Identification and Resolution
m) Change and version control.
n) Patch management
o) Documentation
p) L1, L2 and L3 support for all applications

1.12. The MSI shall use MOSIP to satisfy the requirements for the core modules. The MSI shall be responsible for configuring, customizing, and modifying, deploying, maintaining the MOSIP application suite to comply with given requirements. The MSI is required to provided enterprise licenses for MOSIP tools and technologies, wherever available.

1.13. The MSI shall re-assess the requirement of MOSIP components and suggest customization of the application as per the country requirement, if any.

1.14. The MSI is compelled to use open-source applications (other than MOSIP) with enterprise support/license in all possible scenarios, wherever available, for the SL-UDI system with the consent of ICTA. The MSI is expected to estimate the number of licenses required and all the licenses/subscriptions purchased should be under ICTA.

1.15. The MSI should submit all deliverables (an iterative/phased manner) as specified in the below Section 6: Implementation Schedule, Final outputs, Reporting Requirements, Time Schedule for Deliverables'.

1.16. The MSI should obtain approval from the committee appointed by ICTA for all the deliverables.

1.17. ICTA intends to develop and launch the proposed Foundational ID platform in 12 months (iteration 1) then complete second iteration within next 3 months. Upon completion of iteration1 will be considered as Go-Live, From Go-Live till the end of contract will be the 3-year time period of operations and maintenance, this include some period of knowledge transfer and exit management.

1.18. 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.

1.19. The MSI should study existing integrations with organizations and carry out any enhancements needed for the proposed solution in order to provide a more comprehensive service, as per the design document and user-acceptance testing approved by DRP.

1.20. 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, and COTS, etc.

1.21. The MSI should study and implement a mobile application which supports integrations where native/hybrid mobile application development to facilitate digital ID services to the stakeholders.

1.22. The MSI should study and implement a Citizen portal to facilitate digital ID services to the stakeholders.

1.23. The MSI should study and build foundation ID platform APIs that are required to integrate to external systems to facilitate Digital ID life cycle.

1.24. The MSI should propose the most suitable solution to securely exchange data using APIs primarily for the authentication and e-KYC use-cases.

1.25. The proposed Foundational ID platform shall be compatible with the latest technological components and best practices, and which will be reviewed by ICTA.

1.26. The MSI should follow the proper coding standards and maintain project source code in the in a GIT system and upload all the relevant documents to the Document Management which should be established by MSI.

1.27. The MSI may leverage own environments for development and end-user application training in order to achieve the delivery timelines.

1.28. The proposed platform (citizen portal, mobile application, etc.) shall be able to integrate with multiple payment gateways and bank wallets proposed by the ICTA to facilitate online payments.

1.29. The proposed services/modules offered/interfaced to/with the public (eService interfaces) should be available in tri-languages (Sinhala, Tamil, and English).

1.30. Adopt a proper application release procedure to release the applications to the environments during the deployment in the staging/production environments at the SL-UDI Infrastructure.

1.31. An issue management system should be established for SLUDI. An issue log shall be maintained by the MSI for the errors and bugs identified in the Foundational ID platform as well as any changes implemented in the Foundational ID platform. Issue log shall be submitted to the ICTA monthly.

1.32. The MSI should understand and ensure 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 transforming these data to the new solution.

1.33. The Foundational ID platform should adhere to Web 2.0 concepts, open standards, and micro service architecture and industry standards.

1.34. The proposed Foundational ID platform should be browser independent and able to access with less configuration in the client workstation.

1.35. The MSI should carry out end-to-end security assessments prior to the Foundational ID platform launch and fix any issues found. Further, ICTA / a ICTA nominated party will conduct security assessments periodically post implementation phase, and the MSI should fix any vulnerability issues identified during assessments.

1.36. The MSI should follow templates if provided by ICTA for deliverables.

1.37. The MSI should derive the UAT test cases in collaboration with ICTA.

1.38. The MSI shall undertake benchmark exercise before Go-live. Validate the application and infrastructure performance benchmarks and undertake enhancement/augmentation, if required.

1.39. Obtain User Acceptance and Operational Acceptance for the implemented Foundational ID platform collaboratively with the committee appointed by ICTA.

1.40. 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.
e) Documenting, implementing, as well as obtaining certifications.

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

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

1.43. The MSI should provide support and maintenance services from the date of launch to the agreed time period. Moreover, the MSI should adhere to the Service Level Agreement (SLA), during the support and maintenance (S&M) phase (Refer Annex 9 – Service Level Agreement for Support and Maintenance Services).

1.44. 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 all components of the Foundational ID platform.

1.45. 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 designate offices by ICTA.

1.46. During the support and maintenance period, the MSI shall attend to any issue reported and carryout 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.

1.47. 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.

1.48. All planned or emergency changes to any component of the system shall be carried out through the approved Change Control Management process by ICTA. The MSI shall always follow standard industry processes.

1.49. The MSI shall provide proper application training and knowledge transfer for all designated offices by ICTA regarding technical aspects.

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

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

1.52. The MSI has to ensure that the training sessions held are effective and that the attendees would 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 ICTA.

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

1.54. Adhere to ICTA project management practices, please refer to the *annexure-7 (Project Management and Governance).*

1.55. Participate in Project Review Committee meetings and Project management committee Meetings as a member and present the status of the project when necessary.

1.56. The MSI who engages with the assignment should sign a Non-Disclosure Agreement (NDA) where applicable.

1.57. The intellectual property rights of the Foundational ID platform and all artifacts should be under ICTA.

1.58. The MSI to adhere to the data protection ACT 9 of 2022 in all components of SL-UDI.

1.59. The MSI to collaboratively work with the project stakeholders (i.e., ICTA's team, Management Consultant (MC), Independent Project Management Consultant (IPMC), MSP (Managed Service Provider), suppliers, departments, certification bodies, etc) designated or proposed by ICTA.

1.60. The MSI to work with the "Management Consultant (MC) and Independent Project Management Consultant (IPMC)", of the SLUDI project and accommodate the policies, procedures, recommendations, and the practices proposed.

1.61. The MSI to facilitate & provide technical guidance to set up the registration centres.

1.62. 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, ICTA reserves the right to deploy its own team including the Management Service Provider (MSP) appointed by ICTA, for operations and maintenance alongside the MSI team.

1.63. The MSI to carry a risk assessment in collaboration with the ICTA, appointed MC and IPMC and take necessary precautions to manage the risk as instructed by ICTA.

1.64. The MSI to facilitate a smooth transition without disruption of operations to the ICTA designated team upon completing the maintenance period where ICTA team is able to self-sufficient in managing the operations.

1.65. The following items (not limited to) should be reviewed, improved, and implemented by the MSI under the guidance of the Management Consultant (MC), Independent Project Management Consultant (IPMC) and ICTA,

a) RACI Matrix
b) Access Control Policy and Procedure
c) Business Continuity Management Plan
d) Capacity Management Policy and Procedure
e) Change Management Policy and Procedure
f) Development and Maintenance Policy and Procedure
g) Dispute Resolution Policy and Procedure

h) Governance Policy
i) Incident Management Policy and Procedure
j) Information Backup Management Policy and Procedure
k) Information Security Policy and Procedure
l) Release Management Policy and Procedure
m) Log Management Policy and Procedure
n) Patch Management Policy and Procedure
o) Service Level Management Procedure
p) Stakeholder onboarding Policy and Procedure
q) Vulnerability Management Policy and Procedure
r) Risk Management Policy & Plan

1.66. 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 Centre Site / Citizen Services Centres (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 Centre

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

1.67. Refer following Annexes, which form part and parcel of the Schedule of Requirements.
a) Annexure 1: High Level Process Flow
b) Annexure 2: Non-Functional Requirements
c) Annexure 3 – Minimum Technical Specifications
d) Annexure 4 - Software Engineering
e) Annexure 5 - Demand Capacity
f) Annexure 6 - Transition and Exit Management
g) Annexure 7 - Project Management and Governance
h) Annexure 8 - Biometric Device Certification
i) Annexure 9 – Service Levels
j) Annexure 10 – Manpower
k) Annexure 11 – Overview of Technology
l) Annexure 12 – List of Enrolment Centres

1.68. The scope of work of the MSI, spans the implementation, commissioning, and maintenance of the foundational ID platform at the Primary Data Centre, and Disaster Recovery Site sites.

#	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 (Annexure-5) • 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	5.1 Software Solutions	**MOSIP Components MOSIP Application 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 • Integration Middleware

#	Scope	Sections	Brief Scope Description
			COTS/OTS Components (5.1.3 OTS/COTS Application) MSI shall be responsible for application development and customization of following, but not limiting to, COTS/OTS applications: • Business Intelligence and Data Analytics • Customer Relationship Management • Document Management System • Identity and Access Management • Knowledge Management Solution • Learning Management Solution **Bespoke Components** (5.1.4 Support Application) MSI shall be responsible for application design, development, and implementation of following, but not limiting to, applications: • Citizen Portal • Mobile Application • TSP and UA Application • DRP back-office workflow solution • Fraud Management **Biometric Solution** (5.1.5 Biometric Solution Implementation) BSP shall be responsible for biometric solution design, customization, integration, and implementation of following, but not limiting to, applications: • Automated Biometric Identification System • Biometric SDK • Manual Adjudication **Integration of MOSIP with 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 with

#	Scope	Sections	Brief Scope Description
			the information system. Biometric solution shall also be provided by BSP. **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 (Annexure-4)** The MSI will be responsible for: • Preparation of Delivery Plan • Requirements Gathering • Design • Development and Customization • Testing • Continuous Build • Change and Version Control • Maintain System Documentation • Issue Identification and Resolution • Support and maintenance Note: The MSI must utilize the agile methodology and DevSecOps approach.
3.	Supply, installation, commissioning of hosting infrastructure	Section 5.2	The MSI is responsible for providing hosting space in the two Tier-III data centres i.e., Primary Data Centre and Disaster Recovery sites. MSI shall assess the site(s), prepare a site plan and rack plan for approval of ICTA. As per approved plan, MSI will be responsible to supply, install and commission the IT infrastructure. The MSI is responsible for supply, install and commissioning of the IT hardware, software systems and peripherals required for the Data Store in the Primary Data Centre and Disaster Recovery for implementation.

#	Scope	Sections	Brief Scope Description
			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 centres • 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 DRP provided network at Citizen Services Centres (CSCs) for enrolment • Spares and Maintenance of Enrolment Kits
5.	Enrolment Centres/ Citizen Services Centres (CSC)	Section 5.4	MSI is responsible for preparing design document. In addition, MSI is responsible for establishing, operating, and maintaining the enrolment kits.
6.	Identity Cards	Section 5.5	DRP 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

#	Scope	Sections	Brief Scope Description
			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) • Ensuring Training Effectiveness • Managing Continuous Learning
8.	Benchmarking, Commission, Acceptance and Go-Live	Section 5.7	• Set up benchmark environment in DR site. • Undertake benchmark exercise before Go-live. • Validate the Application and Infrastructure performance benchmarks and undertake enhancement/augmentation, if required • Performance benchmark should be met in both production and DR sites.
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) • Security and Governance Audits, reviews and periodic testing, fixing and remediation. • Fraud Management **Business Continuity (Section** 5.8.3**)**

#	Scope	Sections	Brief Scope Description
			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 Centre and IT Helpdesk)		**Contact Centre (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 centre 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
11.	Security and Network Operations	Section 5.9	**Security Operations Centre (Section** 5.9.1**)** The MSI is responsible to SOC Setup, SOC Integration and running the SOC services. **Network Operations Centre (Section** 0**)** The MSI is responsible to NOC Setup, NOC Integration and running the NOC services
12.	Business and Technical Services	Section 5.10	MSI has to perform the following activities: **Business Services (Section** 5.10.1**)** • Conduct a initial rollout and undertake impact assessment of Enrolment Services to identify learnings • Authentication Services (Partner Onboarding and Device Management) • Ecosystem Partner Management • Authentication Services Management • Manual Adjudication Services • Enrolment Validation Services • Enrolment Officer Certification Program

#	Scope	Sections	Brief Scope Description
			Technical Services (Section 5.10.3**)** • IT Asset Management • Cell and Non-Cell Management • Field Network Assessment • IP Address Management • Warranty and AMC management • Software Management • SMS Services Integration • Biometric Solution Management • Biometric Device Audit and Certification Program
13.	Warranty, Operations and Maintenance	Section 5.11	**Warranty Services (Section** 5.11.1**)** The MSI is required to provide the warranty 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 Centre 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 • Network Monitoring • Security Management • Event Correlation • Incident Management • Configuration Management • Patch Management

#	Scope	Sections	Brief Scope Description
			• Change request Implementation Management of license agreements and system manuals and documentation. Note: ICTA 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 • Support during System Audits • Patch Management **Field Infrastructure (Section** 5.3**)** The MSI is required to do the following: • Issue Identification and Resolution • Repair services through service centre • Spares for timely resolution of issues • Software Updates

#	Scope	Sections	Brief Scope Description
14.	Project Reporting and Project Management	Section 5.12	**Project Reporting (Section** 5.12**)** • MSI is responsible for effective reporting during SL-UDI Implementation phases as well as during the SL-UDI operational phase (Support and maintenance). • This may include, among others Project Implementation status and progress reports including risk assessments. Further should also include reporting about the ABIS, data quality monitoring, incident & issues, service levels, and other key aspects of the project. • Progress reporting related to Transition Management and Exit Management should also be included. **Project Management (Annexure-7)** MSI shall be responsible for managing the engagement and ensure that the deliverables meet the satisfaction of the ICTA. MSI shall be responsible for, but not limited to, the following activities: • Set-up of project management office (PMO) • Preparation of a tool based detailed project plan including key project activities and milestones. • Manpower deployment in accordance with the plan • Define an Escalation Matrix • Change Control Management • SLA Management, Monitoring, and Reporting (Annexure-9) • Project Status Monitoring and Reporting • Risk and Issue Management • Transition Management • Exit Management

#	Scope	Sections	Brief Scope Description
15.	Transition and Exit Management	Annexure-6	**Transition Management (Annexure 6)** • 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: o Preparation and execution of the transition management plan, in cooperation with ICTA o Transfer of Deliverables and Documents o Transfer of Agreement and Licenses o Knowledge Transfer **Exit Management** 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 6 :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 offshore development model wherein, a dedicated core team comprising of Application Manager, Business Analyst, Business Process Specialist, etc. shall be stationed at the ICTA’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 the 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 ICTA.

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

(i) Application development as Release_1 of the SL-UDI Software System.

(ii) Application development as Release_2 of the SL-UDI Software System.

(iii) 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 ICTA 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:

(ii) **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 (Annex 12) . Release_1 of the SL-UDI Software System is proposed to primarily consist of the Pre-enrolment Software, Enrolment Software, Identity Management System (IDMS), 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.

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

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

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	• SL-UDI Portal • Fraud Management System

Implementation of SL-UDI Software System	
Release_1 (T + 12 Months) (MVP)	**Release_2 (T + 15 Months)**
• Enrolment Software • Identity Management System (IDMS) • Authentication Solution • Integration Middleware • Unique Identity Generator • Partner and Device Management **Biometric Solution Provider (BSP) Applications***** • Biometric Software Development Kit (SDK) • Automated Biometric Identification System (ABIS) • Manual Adjudication **Support Applications and Other Applications** • SL-UDI Portal (basic aspects for pre-enrolment and enrolment) • Business Intelligence and Data Analytics (basic reporting for the purpose of pilot) • Customer Relationship Management (CRM) • Document Management System • Identity and Access Management • TSP and UA Software • Project Management Tool • Fraud Management System (basic aspects) **Solutions for Training** Application training solutions/ platforms in accordance with the agreed training schedule. <Put reference to training plan>	• Business Intelligence and Data Analytics • SL-UDI Mobile Application • Knowledge Management System • Learning Management System • Service Billing System

Table 7 : 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: In case some components of Release_2 become necessary for Release_1, the MSI should be able to provide them at no extra cost.

Note: As part of the Release_1, the MSI should provide at least 75% infrastructure of the DC/DR (Infrastructure/Platforms/Security/SOC/NOC) to provide and maintain required SLAs for MVP.

Note: The above timelines including 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 adaption plan including, but not limited to, the following activities:

- Study the existing architectures 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 ICTA 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. country 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 ICTA 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 OTS/COTS Application

Note: The MSI should obtain the Developer support for COTS items, wherever concerned OEM offers this service

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

5.1.3.1 Business Intelligence and Analytics

(i) ICTA is seeking the capability to analyse large quantities of business data, transform the data into intelligence and insight, and deliver this intelligence and insight to the ICTA's processes and users. In a move aimed towards digital economy in Sri Lanka, the ICTA has taken up a Data Analytics and Business Intelligence initiative for SL-UDI Information System. SL-UDI Information System would help increase efficiency and improve savings in resources and availability of reliable data in a timely manner. ICTA desires to build enterprise-level DA and BI system with definition of Key Performance Indicators (KPI) for SL-UDI Information System. The KPIs need to be viewed from a Division, Function, Process, and user's perspective. The ICTA believes that data mining and 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 an enterprise level 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. The mechanism would also allow for alerts, reminders, etc. to be sent through a unified dashboard that will let the user control their procurement or supply.

(i) 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.

(ii) 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.

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

a. Propose, design, and implement an integrated BI and Data Analytics system.
b. Quality assurance test for BI and Data Analytics system
c. Provide documentation for BI and Data Analytics system.
d. Perform integration with internal and external systems' data sources for BI and Data Analytics system.
e. Master Data Management for all applications
f. The solution must have self-service client services such as system and data status dashboards, electronic data dictionaries, and manual data upload.

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

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

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

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

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

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

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

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

(iii) The proposed solution should meet the minimum technical specifications [Annex 3] 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

ICTA 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 ecosystem, such as CSC, IT Helpdesk, SOC, NOC, Partner Management, etc. which includes integrations and other components which cover the entire eco system.

The MSI's scope of work includes:

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

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

(iii) The CRM solution should be a single window to record and address queries of citizens and partners. MSI shall be responsible to undertake any customizations of the CRM solution as per ICTA's requirements, SRS, and associated Software Lifecycle Services.

(iv) 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.

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

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

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

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

(ix) DRP on behalf of ICTA, shall provide the MSI with a toll-free number(s) for contact centre.

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

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

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

(xiii) 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.

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

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

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

(xvii) The CRM solution shall support IVR, Voice, Email, FAX, letter and Web based complaint lodging, resolution, and response features using channels such as Voice, SMS, Email, FAX, WhatsApp and Web.

(xviii) The CRM solution should provide special functionality of handling handwritten letter as a part of grievance redressal. The letters shall be scanned and maintained in the CRM solution.

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

(xx) The solution should support call routing functionalities.

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

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

(iv) 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 either on the internet or intranet. 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 based on Role based access where after login to portal using SSO, the ability to invoke a particular application would depend if the role is authorized to access the application.

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

The proposed 55eaturd 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 Web Portal (Enrolment Partner Portal, Authentication Partner Portal, Public Portal, Private Portal, Citizen Services Portal and Developer Portal.)

(ii) SL-UDI Mobile Application

(iii) TSP and UA Software

(iv) Fraud Management

(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 Web Portal, SL-UDI Mobile application and TSP and UA software is given below:

5.1.4.1 SL-UDI Web Portal

A web portal shall be implemented as part of SL-UDI Information System. The SL-UDI Web Portal would be available to all stakeholders (residents, internal users, contact centre 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 internal users will be able to access applications like manual quality check, adjudication. The contact centre will be able to use applications such as CRM, Partner Management. The TSPs will be able to use the applications such as Partner Management. MSI shall be responsible for the following:

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

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

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

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

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

(vi) Implement a "Content Management" framework and solution to allow authorized users of ICTA 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 ICTA on the following:

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

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

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

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

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

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

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

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

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

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 Centres 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 all major platforms such as Android and iOS etc.

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

(x) Mobile Apps should work flawlessly across different platforms, including but not limited to all OS's widely used.

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

(xii) Should provide Role Based Access control.

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

(xiv) Should support in-device authentication.

(xv) 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.

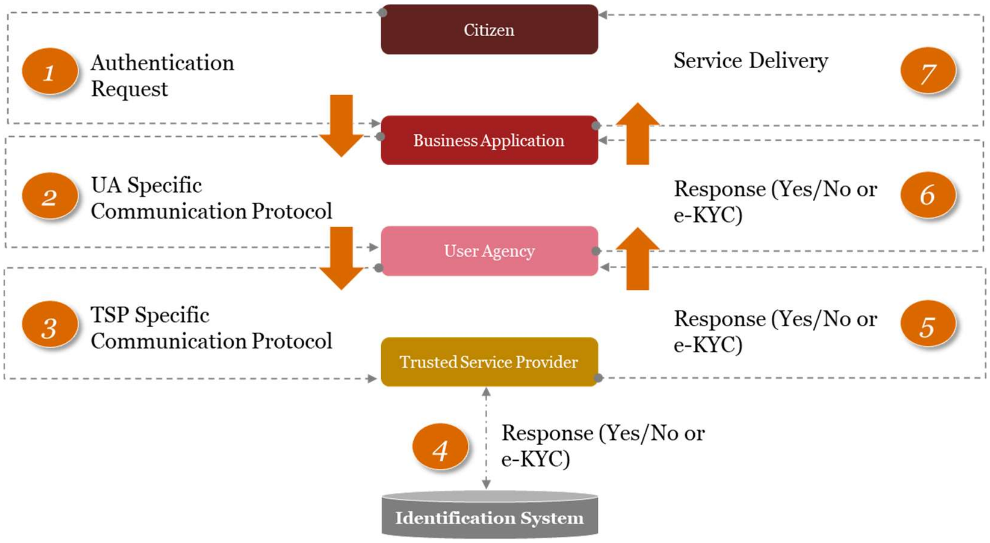

Citizen
1
Authentication Request
Service Delivery
7
Business Application
2
UA Specific Communication Protocol
Response (Yes/No or e-KYC)
6
User Agency
3
TSP Specific Communication Protocol
Response (Yes/No or e-KYC)
5
Trusted Service Provider
4
Response (Yes/No or e-KYC)
Identification System

Figure 4 : TSP and UA Applications

(ii) For TSP, there will 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 request, 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 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. As part of handling request, the UA application will log requests, validate request, append wrapper information in request, sign, and encrypted request, and forward the request to SL-UDI Information System. As part of handling response, the UA application will log response, validate response, decrypt the response, and forward the response to concerned UA.

5.1.4.4 Fraud Management

(i) The objective of the fraud detection system is to ensure that fraudulent enrolment/authentication are detected and prevented. In the context of SL-UDI Information System, fraud means ‘an intentional attempt by person or organization to gain illegal access to SL-UDI data and fraudulently benefit from the access.’

(ii) A fraud management solution is required to detect and reduce identity related fraud.

(iii) The fraud management solution should be able to detect frauds such as the following:

a. Misrepresentation of information.
b. Multiple enrolments by same citizen.
c. Enrolments for non-existent residents; or
d. Identity theft such authentication as someone else.
e. Enrolment and Authentication outside Sri Lanka.
f. Enrolment and Authentication during unusual hours of the day.
g. Replay attacks using stored biometrics.
h. Multiple authentications within very small-time durations.
i. Fraudulent Enrolment Centres.
j. Same individual authenticating from different locations using biometric.

(iv) MSI shall be responsible for creation of fraud scenarios including the above indicative list of frauds.

(v) The fraud management solution must have, among others, the following characteristics:

a. It is important to ensure secure access to the fraud information. For example, the DBA should not be able to read the list of residents who have committed fraud or even delete a record of a citizen who has committed fraud.
b. The fraud detection system architecture should have a well-defined API for interfacing with other components of SL-UDI Information System.
c. The fraud could be detected during enrolment and authentication. Frauds detected during enrolment should result in process for prevention of SL-UDI generation as well as NIC personalization / issuance.
d. The fraud management solution should have a high capacity to handle multiple transactions simultaneously.
e. A fraud engine should allow setup, configuration, and modification of fraud detection rules.

f. The fraud engine should update itself based on the frauds detected.

g. The following detection mechanism but not limited to, should be supported.

- Graph based.

- Fuzzy matching
- Biometric scores
- Authentication patterns

5.1.4.5 Knowledge Management System

The KMS delivery scope should include among others the following.

(i) MSI shall be responsible for design, develop and maintain 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.

5.1.4.6 Learning Management System

The LMS delivery scope should include among others the following:

(i) MSI shall be responsible for design, develop and maintain the Learning Management System (LMS).

(ii) MSI shall be responsible for preparation of training material and uploading all the training material prepared for training on the LMS.

(iii) MSI shall integrate LMS with the SL-UDI portal, KMS, DMS, etc.

(iv) The LMS must be designed in a flexible manner so that learning features can be added for various types (self-paced, one-time, etc.) of learning and media (audio, video, textual, etc.).

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

5.1.4.7 Queue Management System (QMS)

DRP will provide the QMS and MSI will be responsible for its integration with other components of SL-UDI solution.

5.1.4.8 Service Billing System

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

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

a. Should be integrated with the payment gateway provided by ICTA to enable various types of payments, their reconciliation, and their refund.
b. Support billing for G2C and G2B scenarios
c. Manage customer profile, metering and pricing configurations, invoicing and receivables, collections, notifications, reporting, etc.
d. Should be integrated with Authentication Solution, Pre-Enrolment Application, Enrolment Software, Web Portal, Mobile Application, BI & Analytics Solution, etc.
e. Should support create payment transaction records, record an audit trail of all actions, payment refund, payment status tracking, etc.

5.1.4.9 Single Sign On (SSO) Module

The ICTA 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 (Oauth 2.0). The SSO module should provide the 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 ICTA. For the period of the contract, the MSI will also be expected to extend technical support to government department 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 centres 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, unfettered, unlimited right to uses the licenses and the rights to deploy the solution anytime anywhere.

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

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

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

e) Adjudication stations 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 the BSP 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 BSP are operating system, systems software (e.g., virtualization), database, application server software, etc. The BSP 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 BSP 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.) being provided by the MSI.

In addition to installing and tuning its own software, the BSP will also be responsible 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 1. Rollout of Biometric Solution

(i) The BSP will 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 rule and application-level policies related to de-duplication and verification in consultation with ICTA.
   d) Perform de-duplication checks (1: N) for enrolment for a gallery size of capacity size provided in the RFP
   e) Assist MSI in 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 rollout 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 ICTA for their review and acceptance.

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

5.1.5.3 Integration Service

The BSP and MSI 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)

The BSP should extended necessary, adequate, and timely support to the MSI to achieve the integration and thereafter to monitor and management the requirements and service levels.

The MOSIP is working on micro-services architecture where integration with components is performed using RestfulAPIs. 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.

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**	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.

S. No.	Testing	Description
		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 ICTA. The MSI shall maintain the integration test plan along with test results and defect statistics and provide the same to ICTA, if desired so. The MSI shall submit report on integration to ICTA for review.
2	**System Test Planning & Testing**	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 ICTA. MSI shall submit a report on testing to ICTA for review.
3	**Performance Testing**	As part of the testing, MSI shall carry out Performance testing of the biometric solution to ensure that it meets the performance requirements.
4	**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.

S. No.	Testing	Description
		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 ICTA. The ICTA 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.
5	**User Acceptance Testing**	The objective of this testing is to determine whether the solution meets the ICTA'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 ICTA. 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 ICTA for the purpose of testing. ICTA 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 ICTA 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 is retested by the end user group. The testing shall be done in iterations till the specified

S. No.	Testing	Description
		requirements are met. At the decision of ICTA, 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 ICTA for solution UAT. The MSI shall be required to demonstrate all the services 67eature / functionalities as mentioned in the agreement. The prerequisite for carrying out UAT activity shall be: • Submission of a detailed test plan by MSI and approval of this plan by ICTA • The training requirements as mentioned should be completed before the final acceptance test • Licenses / manuals / brochures / Data Sheets / CD / DVD / media for all the supplied components have been provided to ICTA. • Software release note that contains stepwise instructions for ICTA on how to install the software. The instructions shall include information on creating the directory structures, installing source and executables, loading data needed for installation and so on. • All documentation related to solution and relevant acceptance test document should be completed & submitted before the final acceptance test to ICTA. 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. 5 User Acceptance Test Plan 6 Testing Reports 7 Necessary modification in software for passing the UAT
6	**Partial Acceptance Testing (after initial rollout)**	This testing will be carried out once a minimum number of datasets (nearly 50,000) are collected as part of the rollout. The data collected so collected will act as an input for this partial acceptance.

S. No.	Testing	Description
		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 ICTA at the start of this phase of testing. For the purpose of this test, the ICTA and DRP shall form the Acceptance Test Governing Committee as well as the Test Teams (Test Data Team, Test Suit Team and Test Team). The ICTA 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. 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.

S. No.	Testing	Description
7	**Biometric Quality improvement testing**	Biometric solution (ABIS/ Biometric SDK) should be optimized to cater the requirement identified. Further finetuning of the biometric solutions should be done to improve the accuracy efficiency and effectiveness. This should be carried out after defined number of records are available and consultation with ICTA as agreed timeframe based on the implementation plan.

Table 8 : 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
- h. Integration Middleware

(ii) ABIS, Manual Adjudication, and Biometric SDK

(iii) Support Applications
- a. BI & Analytics
- b. Fraud Management
- c. Customer Relationship Management (CRM)
- d. Document Management System (DMS)
- e. Knowledge Management System (KMS)
- f. SL-UDI Portals and Mobile Applications
- g. 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 IDMS SEDA components on the middleware platform (certified to be supported by the MOSIP provider) 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 purpose.
f. Integration of SEDA workflow with NIC APIs for purpose of validation.
g. Integration of SEDA PIN generator with Civil Registration System API’s.
h. 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 Server, extraction component on the extraction server, extraction workflow composites on the Middleware (BPM/ESB), Extraction MQ etc.
b. Integration of extraction workflow on middleware with Biometric SDK Server, HSM, PIN Master and Biometric PIN databases.
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 in the Middleware layer.
g. Deployment and integration of Authentication and KYC workflows on middleware with proxy services on the ESB.
h. 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.
i. Deployment of APIs on API Gateway and integration with OTP server, Middleware and SMS gateway.
j. Deployment of SMS gateway and integration with Middleware.

(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 with ESB and DMS.
c. Integration of Pre-Enrolment Application with Integration Middleware and API Gateway.
d. Integration of Citizen Portal and other portals.

(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.
e. Integration of DMS with Pre-Enrolment Application.
f. Integration of DMS with IDMS.
g. Integration of Fraud Management with IDMS.
h. Integration of Fraud Management with Authentication Solution.
i. Integration of Fraud Management with SL-UDI Web Portal and Mobile Application.
j. Integration of ESB with Partner Management applications, DMS, KMS,CRM ,BI & Analytics, Fraud Management system.

(vii) Integration of BI & Analytics

a. Setup of Data Store, ETL, Analytics Software, Reporting and Visualization software.
b. Integration of ETL with Data Store.
c. Integration of Analytical Software with Data Store.
d. Integration of visualization software with Data Store and BI & Analytics Software.
e. Integration of ETL with sources such as IDMS and Authentication Solution.
f. Integration of analytical models for real time analytics on BI & Analytics Software.

(viii) Integration of Enrolment Software with SL-UDI-DS

a. Integration of Enrolment Software with FTP servers for upload of completed enrolment packets.
b. Integration of Enrolment Software with Partner and Device Management.
c. Integration of Enrolment Software with API gateway for Download of Master data, Download of pre-enrolment information, etc.

(ix) Existing DRP Applications such as:
a. Indexing System (System that stored ID Previous ID Images)
b. IC Inquiry System (System that stored current ID information)
c. ICAO Photo Capturing – Photo Storing Server
d. Card personalization System (track master)
e. Card management System
f. Call centre Integration

5.2 Hosting Infrastructure

5.2.1 Data Centre Site Set-up

5.2.1.1 Data Centre Strategy of Project

ICTA has decided to utilize 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 entire duration, a mechanism for storage and safe keeping of backup tapes, a remote site will be utilized.

ICTA shall utilize the co-location model for hosting IT Infrastructure in Primary Data Centre and Disaster Recovery. The Primary Data Centre and Disaster Recovery sites should be in two separate data centres. The MSI needs to hire the colocation space in the reputed Tier-III data centres in Sri Lanka. MSI shall undertake assessment of the data centres, prepare a site plan and rack plan.

The MSI should provide a fibre-based connectivity for data replication between the two sites. The MSI shall undertake a capacity assessment and undertake capacity augmentation to meet the required requirement and performance levels mentioned in the RFP.

The other requirements w.r.t. the Data Centres should be as follows:

(i) Tier III certified data centre and uptime should be 99.982% in Sri Lanka

(ii) Should provide incident reporting facility.

(iii) Allow termination of the links provided by the ICTA via any service provider. If telecom junction box / multiplexers of these links are not available, commissioning the same should also be allowed. Further, laying of cables and associated works in their premises should be allowed.

(iv) Should provide Access cards, Gate passes to the ICTA personnel /ICTA appointed system integrators as and when they require visit the site. (Such access should be provided 24 X 7 and will not have any time restriction).

(v) Should regularly monitor the access to the provided space (cage with necessary physical security) by means of access control system, physical security, biometric access, and CCTV (Closed-circuit television) and should always make sure that they are functional 24X7 days.

(vi) If required, the bidder should provide details of people accessing ICTA own space/cage sharing the entries made in the security registry, reports from access control system, CCTV video clips etc.

(vii) Shall conduct periodic security audits of the data centre and report by annually.

(viii) Access to ICTA demised space is restricted to authorized persons only. Other than emergency conditions requiring extreme urgency (e.g., fire, injury), entry into the demised space requires coordination and approval by ICTA prior to any person being granted access to the space.

5.2.1.2 Site Set-up

MSI shall provide the physical space for hosting IT Infrastructure in Data Centre and Disaster Recovery. Data Centre Service providers, procured by the MSI shall be responsible for civil works including provision of cooling and power facilities in these sites. Upon availability of space for each of the Data Centre sites, the MSI shall set-up the site for hosting of SL-UDI Information System. The MSI, in consultation with ICTA 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 to the ICTA.

(iii) Prepare a detailed plan for site set-up and obtain a sign-off from the ICTA.

(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. as to align with the facilities of Data Centre as per the requirements of the infrastructure.

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

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

(x) MSI should arrange for all the facilities in the data centre sites, 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 9 : 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 in Primary Site as well as Disaster Recovery Site
Quality Assurance	The necessary testing & quality assurance environment for solution should be created in Primary Site as well as Disaster Recovery Site
Training*	The necessary training environment for solution should be created in Primary Site and Disaster Recovery Site. However, for initial training before Release-1, the MSI will have the option to use the appropriate environment aligned with the timelines.
Service Creation	The necessary service creation environment for solution should be created in Primary Site as well as Disaster Recovery Site
Benchmarking	Disaster Recovery Site will act as the testing environment for Benchmarking exercise
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

*Note: It should be noted that for the immediate requirement of training citizen enrolment staff prior to the formal launch of the project SL-UDI that the MSI is required to provide the necessary training environments (public or on premise) free of charge in addition to above training 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 Centre 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 network, 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 behaviour, 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 production environment. It should be capable to provide visibility across 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 centre level, commissioned by MSI as per the specifications mentioned [Refer Annex 3] 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. Design of servers will be done based on the final sizing requirements arrived, 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 the 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 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. Design of network will be done based on the final bandwidth requirements arrived, 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 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 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 against 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 centre 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 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. 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. Post completion of build for non-production environment, middleware team will be asked to perform installation and carry out test activities. After conformation from middleware team, setup will be provided to performance test team to validate server configuration and sizing. 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 Ius 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 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 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 centre 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 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 is described in the section. The SL_UDI network proposing 3 different type of networks i.e., WAN, Data Center to Data Center (P2Plinks) Network, Internet Network.

The network connectivity encompasses the following:

S. No.	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	The first TSP will be implemented by MSI where segregation of networks should be implemented. For the additional TSPs' which may come on board in the future, the TSPs' will bring their own secured network from their data centres to SL-UDI DC and DR. The MSI will accommodate and provide necessary provisions and 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 and DR sites.
SL-UDI Wide Area Network			
3.	Data Centre – Interconnection Network	P2P	MSI will be required to provide secure and reliable connectivity.
4.	Data Centres (DC & DR) – NOC	MPLS/SDWAN	MSI will be required to provide secure and reliable connectivity.
5.	Data Centres (DC & DR) – SOC	MPLS/SDWAN	MSI will be required to provide secure and reliable connectivity.
6.	Data Centres (DC & DR) – Contact Centre	DRP IPVPN	MSI will be required to provide secure and reliable connectivity.
7.	Data Centres (DC & DR) – Technical Helpdesk	MPLS/SDWAN	MSI will be required to provide secure and reliable connectivity.
8.	Data Centres (DC	DRP IPVPN	DRP will provide secure and reliable

S. No.	Link	Type	Remarks
	& DR) – DRP Hosting Infrastructure		connectivity, MSI shall work collaboratively work with DRP their network service provider
9.	Data Centres (DC & DR) – DRP Head Office	DRP IPVPN	DRP will provide secure and reliable connectivity, MSI shall work collaboratively work with DRP their network service provider
10.	Data Centres (DC & DR) – ICTA Head Office	Lanka Government Network (LGN)	ICTA will provide secure and reliable connectivity, MSI shall work collaboratively work with ICTA their network service provider
11.	Connectivity at field offices (fixed registration centres)	DRP IPVPN	DRP has its own IP/VPN with Sri Lanka Telecom secure network to connect their fixed registration centres. DRP will provide the secure connectivity (including registration centre 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 DRP. The MSI should provide necessary network provisioning to terminate the connection.
Internet Connectivity			
12.	Data Centres (DC & DR) – Internet Links	Internet	MSI will be required to provide reliable connectivity for open access of the services provided by SL-UDI
13.	Internet for mobile registration centres	Internet	MSI will be required to provide secure and reliable internet dongles for connectivity of mobile registration centres with the DC and DR

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 network

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, ICTA 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 (Fibre Channel) interface and bandwidth, Security products, etc
3. MSI should provide certified hardware/devices to proposing 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 24 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 ICTA 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 3-years from the date of signing of contract with ICTA. 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 ICTA 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 Centres. 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 type of disks. Buffer at storage disks also need to be taken for global hot spares within the storage solution, providing redundancy and high availability at disk levels.

(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 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 of 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 ICTA/DRP. 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, VTL, disks 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. The sizing of VTL is done on the basis of amount of backup and the inline deduplication and compression that is estimated based upon the file type. It would be defined that for which type of data LAN based backup would be done and for which SAN based backup would be configured. Normally backup can be classified into agented or agentless. Depending upon the data type, the same should be configured. Deduplication can again be source based or target based which is also contingent upon data type. Depending upon the backup policy, it would then be decided which data has to be kept for how much duration on the virtual tape library before taping out can happen. 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 tool. 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 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 centre-wide network aggregation.

3. Virtualization solution should provide monitoring and management of virtualized infrastructure with configurable, customizable operations dashboards to provide real-time insight into infrastructure behaviour, and for capacity analytics. It should provide 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 centre

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 limit 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 has to be part of solution.
6. The platform shall support multiple technologies as runtime platforms for applications such as – Java, PHP, Python, Ruby, Perl, Node.js etc.
7. The platform shall provide auto scaling capability for automatically running appropriate number of container instances as per load requirements.
8. The platform shall provide container instance auto healing capability.
9. 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 earlier version.
10. The platform shall provide deployment strategies support such as for ensuring no/minimum downtime for application updates / upgrades.
11. The platform shall provide centralized logging capability (including applications logs from container instances) for audit, logs analysis & ease of management purpose.
12. The platform shall provide integrated container native persistent storage capabilities.
13. Generic/Shared Components as per the Solution Architecture Blueprint can be on 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:

Number	KIT Item	Provider
1	Desktop PC and other components	DRP
2	Dual Display Monitor (Touch)	DRP
3	Document Scanner	DRP
4	Printer	DRP
5	Multi-Functional Printers (Fax)	DRP
6	IP Phones	DRP
7	Power Extension	DRP
8	Flash Light	DRP
9	Background Screen	DRP
10	Web Camera	DRP
11	QR Reader (Scan PRN included QR)	DRP
12	USB Hub	DRP
13	Enrolment – Fingerprint Scanner (4-4-2)	MSI
14	Enrolment – Iris Scanner (Dual)	MSI
15	Enrolment – Microphone	MSI
16	Signature Pad	MSI
17	Speakers	MSI
18	Auth – Facial Scanner	MSI
19	Auth – Iris Capture Device	MSI
20	Auth- Fingerprint scanners	MSI
21	Mobile Units	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 below KIT items.

Number	KIT Item
1	QR Reader (Scan PRN included QR)
2	Laptop
3	Document Scanner
4	Printer
5	Enrolment – Fingerprint Scanner (4-4-2)
6	Enrolment – Iris Scanner (Dual)
7	Web Camera

8	Signature Pad
9	UPS
10	USB Hub
11	Internet Dongle
12	Flash Drive
13	Flash Light
14	Background Screen
15	Container
16	Speaker
17	Microphone

Table 12 : Mobile Kits

It is expected that the registration software (based on MOSIP) developed by the MSI shall be compatible/interoperable with biometric capturing devices (Fingerprint, Iris, and Face,) of at least three leading and reputed OEMs. In order to ensure this, MSI is expected to provide biometric capturing devices from three different OEMs. The volume of biometric capturing devices from three OEMs will be as per the table given below:

Type	Qty. (MSI)	OEM-1	OEM-2	OEM-3
Fingerprint Registration Device	Please refer BOQ [Put the proper referencing]	60%	30%	10%
Iris Registration Device				
Fingerprint Authentication Device				
Iris Authentication Device				
Face Authentication Device				

Table 13 :volume of biometric capturing devices

Note:

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

(2) In addition to above quantity entrusted to MSI for the entire kit as well as biometric capture devices, the MSI needs to maintain spare biometric devices which the MSI will have to procure and manage. However, additional stock for spare parts may be maintained by MSI, at its own cost, to comply with the SLA requirements.

(3) The MSI is required to provide the Virtual Device Manager (VDM) along with the biometric capture devices.

(4) The certification and documentation related to the device management server environment and foundation trust module provisioning environment are as follows:

a. ISO 27001:2013 certification
b. FIPS 140-2 Level 3 HSM certification
c. VAPT conduct and report.
d. Disaster recovery plan
e. Architecture Diagram
f. Demonstration of compliance to requirements (audit frequency to be decided by ICTA)

5.3.2 Supply, Installation and Commissioning of Enrolment Kits

(i) To enrol the individuals under SL-UDI program, facilities for enrolments shall have to be created. The ICTA envisages reusing existing enrolment centres as well as setting up new enrolment centres across the country that would be equipped with enrolment kits for biometric enrolment. At present, it is estimated that fixed and mobile enrolment centre 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 ICTA and MSI. In such 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 warranty 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 ICTA and DRP.

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).
Packaging and marking	Unless specified otherwise, biometric devices shall be securely and properly packed, and every precaution taken to avoid loss or damage during transit. The packing shall be all weather-proof and sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit and open storage. Packing case size and weights shall take into consideration, where appropriate, the remoteness of the goods' final destination and the absence of heavy handling facilities at all points in transit. Each package should be clearly marked to indicate Description and Quantity of material, Name and Address of the delivery, Gross weight of the Package, S.O. No., and Date and the Name of the MSI. The packing, marking and documentation within and outside the packages shall comply strictly with such special requirements as shall be provided for in the work order and in any subsequent instructions ordered by the ICTA and DRP.
Dispatch Instructions and Notification	Unless otherwise specified, supplies will be available from the date of Contract commences. It is essential that full and clear instructions regarding dispatch are given in the Work Order. Any changes in dispatch or delivery instructions should be notified to the ICTA and DRP. Receipts/ invoices / delivery note, Packing Notes must be submitted to the ICTA and DRP sufficiently in advance of the actual arrival of biometric devices at destination failing which the MSI shall be held responsible for any subsequent discrepancy between actual receipt and the materials detailed in the receipts/ invoices / delivery note received later. The biometric devices will be delivered free at sites / project sites end including fright. It will be responsibility of MSI for safe arrival of items in full and good conditions at specified destination and ICTA/DRP will not pay separately for transit insurance, if any. The supplied items shall confirm to standard guarantee/warranty effecting as per terms and conditions of this RFP.

	The timelines for supply, installation, testing and commission of the equipment is provided in relevant section of this RFP.
Delivery Documents	Within 24 hours of shipment, the MSI shall notify the ICTA & DRP, by cable/telex/Fax the full details of the shipment including Contract No., Receipt No., Date, Description of Goods, quantity etc. The dealer shall submit, among others, the following documents to the ICTA and DRP: • Soft copy of the invoice showing goods description, quantity, unit price, and total amount. • Transport (Air, Railway, Truck, etc.) receipt • Factory Inspection Report • Manufacturer's Guarantee Certificate
Factory Inspection Report	The MSI shall provide the copy of the factory inspection report having details of the equipment and specimen signature of the quality officer of OEM. The quality officer shall physically inspect the equipment supplied and check the list of items and their physical state. During the inspection, the OEM should check the biometric devices for compliance to specification, adherence to OEM's quality standards, and other parameters specified in the RFP. For both Box/es with broken seal or signature on seal not matching with that on inspection report, the equipment shall not be accepted by the ICTA and the same shall have to be taken back by the MSI at his own risk and cost. All equipment will have to be supplied with all the detailed operational and maintenance manuals free of cost.
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 ICTA) where the basic checks and testing have to be performed. Thereafter, at its own cost the MSI will be responsible to safely package and transport the devices to the enrolment centres. A list of the locations of enrolment centres where such registration kits would be deployed has been given in Annexure 12 (Project sites / Sites)

5.3.2.3 Testing and Certification

The MSI is required to perform various types of testing for the biometric devices which includes Factory Inspection (quality report to be submitted), Installation & Integration Test, and User Acceptance Tests. The MSI to provide self-certification by the device manufacturer that the devices have been checked and found to be working as per requirement in OEM's factory premises. The MSI is required to propose a plan for other tests and obtain prior approval of ICTA. The MSI is also required to submit the test reports and obtain approval of ICTA.

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.

In a medium-long term basis (in the first two years), the MSI is required to utilize the services of the global lab(s) to perform this testing, audit, and certification which are approved by ICTA (List of labs to be provided by the MSI). For this purpose, SL-UDI will authorize one or more lab(s) under the MOSIP Advanced Compliance Program. For long term, please refer to the relevant sub-section under technical services section. [Annex 8] In case if a qualified local certification lab is available, ICTA will nominate the lab at an equal or lower cost, where the cost should be borne by the MSI.

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.
- In exceptional circumstances, the features which could not be validated should be fulfilled by the MSI by the way of undertakings, legal bindings, global certifications, or by enforcing liabilities.
- MSI should ensure the devices are certified under the MOSIP Advanced Compliance Program from the one global lab approved by ICTA. (List of global labs to be provided)

The additional aspects to be noted by the MSI are as follows:

- MSI will demonstrate compliance against the SL-UDI's systems before qualifying the devices as an approved make/model.
- There must be periodic audits on the eligible set of devices in the ecosystem devices that are not having a valid certification status, must be removed from production systems.
- MSI shall maintain a common repository of approved devices, foundation trust module, software checksums, etc.
- There will be requirement of periodic renewals, when necessary, at no additional cost.

5.3.2.4 Installation and Commissioning

To enroll the citizens under SL-UDI program, facilities for registration shall have to be created. The ICTA 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 of overall registration kit with pre-installed Enrolment Software to the specified enrolment kit, whereas the BSP will be jointly responsible for operationalization of registration kits. The MSI is expected to test, install, commission, and ensure the functioning of Enrolment Kits in accordance with the plan approved by the ICTA.

For successful deployment of registration kits, the MSI shall:

- Prepare an installation, commissioning, and testing plan of the Enrolment Kits at enrolment centres and obtain approval from the ICTA.
- Demonstrate successful operation of enrolment kits (integrated with biometric devices and all components) to the ICTA & DRP prior to supply of registration kits to enrolment centres.
- 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 centres.
- Follow the distribution plan approved by ICTA for supply, installation, and commissioning of registration kits. Safely transport kits at each enrolment centre in accordance with the distribution plan. Monitoring of safe transportation of enrolment kits at enrolment centres in accordance with the distribution plan.
- MSI should also check the network connectivity at each enrolment centres and provide feedback to DRP and suggestion to make improvements where necessary at enrolment centres.
- MSI is expected to commission and test the functioning of Enrolment Kits in accordance with the plan approved by the ICTA. The testing should also include integration testing for upload of the Enrolment packet from the Enrolment Kits to the Primary Data Centre and Disaster Site. Also, sample enrolments should be carried out for 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 the ICTA & DRP. The format of this report must be prepared in consultation with the ICTA & DRP.
- Note that the enrolment kit, registration kit terminology used above refers to both fixed enrolment kits used at enrolment centres / citizen service centres as well as the mobile enrolment kit.

5.3.3 Service Centres 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 perform levels to ICTA.

5.3.3.1 Service Centre

The MSI should either utilize its existing service centre or open a service centre for repair and maintenance of biometric devices. The location of service centre should be decided in consultation with the ICTA and DRP, preferably in Colombo.

5.3.3.2 Protection against risk of obsolescence

MSI 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. Thereafter, MSI will give at least twelve months' notice prior to discontinuation of support services, so that the ICTA & DRP may order its requirements of the spares if it so desires. If any of the components are not available or difficult to procure, or the procurement is likely to be delayed for replacement, if required, the replacement shall be carried out by MSI with state-of-the-art technology equipment of equivalent or higher capacity, at no additional charges to the ICTA & DRP.

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 with no additional cost to the ICTA.

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 a 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 Annex 9: SLA (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 ICTA. 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 Centres

The DRP is setting up a wide network of registration centres across the country. The citizens can do their biometric registration (and updates) in these registration centres. These centres 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 centres will be managed by the DRP. In addition, the seating arrangements for citizens as well as government staff (including furniture) will also be made by the DRP. DRP need 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 centre 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 DRP will issue a polycarbonate card to the citizens registered under the SL-UDI program. The DRP will do the procurement of such cards and card management system at their end and its own cost. The DRP has the necessary software, hardware and manpower for card personalization, quality assurance, dispatch, and activation of cards.

The DRP 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 needs to be updated accordingly.

- **Online Activation**: The card is planned to be activated both in online and offline manner. For the offline process, the card holder needs to visit the designated government office, and once card gets activated the status should get updated in the personalization workflow management. For online process, the MSI needs to develop the components for card activation and integrate the same with necessary interfaces (web, mobile, SMS, etc.) for activation and perform integration in the personalization workflow management for update of status.

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. Following shall be responsibilities of the MSI for training:

5.6.1 ***Training Needs Assessment***

MSI in consultation with the ICTA shall identify the training required to be imparted to ICTA team/ different stakeholders for successful implementation and operations of SL-UDI Information System. Both technical and support function training shall be identified by the MSI and approved by the ICTA. Manpower to be trained shall be identified by the ICTA in consultation with the MSI. Maximum batch size should not exceed 25. An indicative list of trainings is given below:

Type	Domain	Duration per batch	Outcome
Technical Training	Biometrics Solution (To be provided in partnership with Biometric Solution Provider)	2 weeks	Hands on understanding of the ABIS and IDMS, Software Development Kits, its integration and Troubleshooting guidelines
	Authentication (To be provided in partnership with Biometric Solution Provider)	2 weeks	Hands on understanding of the Authentication Services, Software Development Kits, and authentication Services
	Security	2 days	Understanding of security guidelines, risk, reporting and compliance. Understanding of access rights and policies, Dos and DONTs, and general awareness about cybersecurity and cyber-threats

Type	Domain	Duration per batch	Outcome
	Security	4 weeks	Advanced knowledge of network security architecture, data Centre security, threats and situation management, software security, etc.
	Technology	5 days	Database management, network management, virtualization, container platforms, server storage management, back up and replication management
	BCP	1 day	Awareness on disaster policy, disaster management and BCP
	BCP	2 weeks	Detailed knowledge about the Business Continuity Planning, Disaster Drill Management, Testing of Biometric Solution at DC Site, RTO & RPO Management and Backup & Replication Management
	Application (COTS and Bespoke)	2 days	Understanding of application development and maintenance, testing, portals management, user acceptance, release management
	MOSIP	5 days	Understanding of MOSIP Components, MOSIP Technology, Functionalities and Features, Support Mechanism, Service Levels, etc.
Support Functions Training	Enrolment Operations	2 days	Monitoring of the continuous enrolment process, upkeep and maintenance of the enrolment software, maintenance of the Enrolment Kits, coordination with and supervision of the Citizen Service Centres, etc.
	Quality Check	3 days	Understanding of Manual Adjudication and

Type	Domain	Duration per batch	Outcome
	Manual Adjudication	2 days	Quality Checks with relevant processes, procedures, systems, etc.
	Contact Centre	3 days	Understanding of Call Logging, Call Forwarding, Call Resolution mechanisms, FAQs, CRM etc.
	Solution core components and support systems	3 days	Understanding core components, functionalities and features, support mechanism, service levels, etc. Understanding Foundational ID platform support systems functionalities and features, support mechanism, service levels, etc.
	All day-to-day operations and processes	7 days	Monitoring of the continuous process, upkeep and maintenance of the SL-UDI, maintenance, coordination with and supervision
	Card Management System and Card Personalization Management System (in partnership with the card provider)	3 days	Understanding of CMS and CPMS functionalities and features, support mechanism, service levels, etc.
	Technical Helpdesk Support	15 days	Understanding of call/ticket logging, call/ticket forwarding, and resolution mechanisms, FAQs, etc.
Biometric Solution and Devices (Lead by BSP)	Biometric SDK	2 days	SDK Tool Kit (Development, Configuration, and Integration, management, etc.)
	Training on Biometric Solution	4 weeks	ABIS System Configuration and Administration (including backup and restoration), Manual Adjudication Configuration and Integration, Manual Adjudication Operation, SDK Tool Kit

Type	Domain	Duration per batch	Outcome
			(Development, Configuration, and Integration), ABIS quality and accuracy management, Input Data Quality Management, Monitoring, Performance Measurement, Overall Solution (configuration, usage, API, performance tuning and measurement and technical reports)
	Enrolment Devices	1 day	Handling, operations, maintenance of enrolment and authentication devices
	Authentication Devices		

Table 15 : Training Needs Assessment

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 the ICTA and DRP

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

(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 the ICTA and DRP. DRP. The actual bifurcation of the manuals to be printed in Tamil, Sinhalese, and English shall be obtained from the DRP. 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 ICTA. Upload the content on KMS post approval.

5.6.3 Impart 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 ICTA and DRP.

5.6.4 Ensure Training Effectiveness

(i) MSI has to ensure that the training sessions held are effective and that the attendees would 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 ICTA.

(ii) MSI is expected to design the test methodology in consultation with the ICTA and DRP. MSI shall also device a test for trainees, the test questionnaires must be approved by the ICTA and DRP. ICTA and DRP shall also supervise all trainings provided by the 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 ICTA 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.

5.6.5 Continuous Learning

At the end of each phases of the project such as requirement gathering, designing, development, quality assurance, deployment, etc., the training should be provided to the designated officers by ICTA in an iterative manner. Further, the designated officers from ICTA including MSP will participate and evaluate the key decisions made during project lifecycle.

The MSI should organize the refresher trainings for all key modules every three months so as to enable continuous learning by designated officials by ICTA enabling them to be ready for takeover at the end of contract. The course plan should be approved by ICTA, course material should be accepted by the ICTA prior to the training and training should clear the effectiveness parameters as defined in Section 4.5.4.

5.7 Benchmarking, Post Benchmarking, Acceptance and Go-Live

Prior to Go-Live of the SL-UDI Information System, MSI shall be responsible for undertaking a benchmarking exercise, commission the SL-UDI Information System and support the ICTA in User Acceptance testing as shown in the figure below.

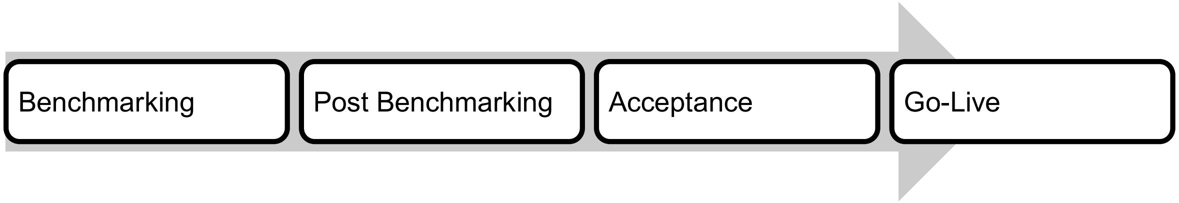


Figure 5 : Benchmarking, Post Benchmark, Acceptance and Go-Live

5.7.1 Benchmarking

(i) The Benchmarking exercise is intended to evaluate the ability of the proposed SL-UDI Information System to scale to the intended usage. It is envisaged to cover the entire SL-UDI Information System, including but not limited to its applications/software, other component solutions, SL-UDI Data Store, and all related interfaces. The Benchmarking process does not intend to simulate all the aspects of SL-UDI Information System however all design parameters, components and related interfaces shall be considered.

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

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

b. This exercise should include all relevant applications, software, and components.

c. The MSI will be responsible for creating the relevant benchmarking 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 ICTA.

d. The MSI shall assist the ICTA teams to benchmark the DR setup.

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

(iii) Benchmarking shall be in accordance with the production deployment and solution architecture proposed in the Technical Proposal of the MSI.

(iv) MSI shall be responsible to undertake the benchmarking of the SL-UDI Solution. The MSI shall:

f. Prepare benchmarking test cases and obtain sign-off on the test cases from the ICTA

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

h. Provide the tools (load generator), scripts for etc. for benchmarking. ICTA does not require licenses for such tools.

i. Create test data (combination of real, artificial, and duplicate data)

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

k. Fingerprint (1 or multiple), Iris (both), Face or any combination thereof will be used for benchmarking

l. The report will be measured on average as well as 90 percentile basis.

m. Undertake benchmarking 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
Basic	Basic Performance Test with proposed sizing and associated IT Hardware	10 million	4,000/Hr.	24 Hours	1
Advanced	Scalability with proposed sizing and associated IT Hardware	20 million	4,000/Hr.	24 Hours	1

Table 16: benchmarking 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
Basic	Basic Performance Test with proposed sizing and associated IT Hardware	10 million	0.1 Million per hours	12 Hours	800
Advanced	Advanced Performance Test with proposed sizing and associated IT Hardware	20 million	0.1 Million per hours	12 Hours	800

Where:

Request Rate – 70% of 1.75 million transactions spread over 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 1 to 3 seconds with 800 concurrent users during basic performance test

Authentication Request Rate (Advanced Performance) – 0.1 million Authentication Requests are expected per hour with a response service time of 1 to 3 seconds with 800 concurrent users during advanced performance test.

Test Duration – Duration in which 1:1 matching authentication completes as per expected SLA of 1 to 3 seconds in the entire test cycle.

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

n. Report the benchmarking output in the format specified by ICTA or its appointed agency. Key guidelines for reporting benchmarking 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 benchmarking with drill down of consumption by each equipment).

(d). The test results should also include the iterative configuration changes/tuning required to achieve the benchmark 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 benchmark results and SLA.

o. ICTA shall witness the benchmark or appoint an agency to verify and validate the benchmarking environment and certify the results of the benchmarking. Benchmark test report provided by the MSI shall be verified and certified by the ICTA

(i) 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 ICTA such that the benchmark performance is delivered by the solution proposed.

(ii) The MSI is expected to define parameters to measure performance of SL-UDI Information System in consultation with the ICTA.

5.7.2 Post Benchmark –

After successful benchmarking of SL-UDI Information system, the MSI shall commission the entire system in the ICTA's Primary Data Centre, and Disaster Recovery Site. Following shall be the key responsibilities of MSI for completion of post benchmark (applicable for both Release-1 and Release-2):

(i) Configuration of all the components of the hardware, software, devices, accessories, etc.

(ii) Integrated testing of all components

(iii) Tuning and testing of application at the Primary Data Centre, Disaster Recovery

(iv) Successful testing of the integrated solution.

5.7.3 Acceptance

Completion of activity of 5.7.2 (mentioned above) of the SL-UDI Information System, the ICTA/ DRP shall undertake a user acceptance of the entire system. Acceptance for the SL-UDI Information System can be divided into the following phases:

5.7.3.1 Pre-Acceptance phase

1. **Creation of Acceptance Plan**

(ii) 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.

(iii) 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

(c). Test plan including schedule, timeline, duration, test activities and due deliverable dates

(d). Detailed acceptance tests

(e). Format for acceptance reports

(f). Highlight any major test areas and reporting activities

(g). Key individuals and responsibilities

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

(v) The Acceptance of the solution shall be provided by the ICTA only after the following conditions have been met successfully to the satisfaction of the ICTA & DRP.

(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 the ICTA & DRP to their satisfaction.

(d). Installation and Configuration of all the components of the solutions including hardware, software, storage, accessories to the satisfaction of ICTA & DRP 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 ICTA within a timeframe of three months from the date of successful go-live from the Primary site

2. **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.

3. **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 ICTA. 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 ICTA.

4. **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 ICTA and DRP prior to submission of draft document
- Submission of draft document for ICTA & DRP review after sufficient internal review by the MSI
- Closure of review comments from ICTA & DRP within the timelines stated
- Acceptance of revised draft(s) by ICTA & DRP based on adequacy and quality of the final submission

5.7.3.2 Acceptance Phase

1. Execution of Tests

(ii) MSI shall assist the ICTA'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.

(iii) ICTA 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.

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

2. Resolution of issues identified during the acceptance testing

(i) All issues and defects identified by ICTA's acceptance test team will be recorded in 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 and document the same.

b. At agreed upon intervals, the ICTA'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 the 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 of the issues at no additional cost. The MSI shall support the ICTA's acceptance test team in re-executing the acceptance test procedures and retest each corrected defect. ICTA's acceptance test team can also undertake additional testing if required. If the incident does not re-occur the ICTA's acceptance test team shall recommend closure of the defect. In case incident continues to occur, the ICTA's acceptance test team shall inform the MSI and the defect shall remain open.

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

5.7.3.3 Post Acceptance Phase

1. Acceptance Documentation and Signoff

(ii) The MSI shall assist ICTA's acceptance test team in creating the reports for acceptance testing. The reports shall summarize the test activities and identify outstanding deficiencies and issues.

(iii) 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.

(iv) 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

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

5.7.3.4 OAT acceptance process

Operational Acceptance Testing (OAT) or Operational Testing is non-functional testing conducted before releasing an application to the production stage. It comes after the user acceptance testing. The primary purpose of this testing is to check the operational readiness of application software.

The process should ensure that all components meet the specified standards and optimum operational level. This needs to consider the benchmarking.

The whole process comprises of a series of tasks such as not limited to, the vender should propose the OAT plan.

- Installation testing
- Robustness of the app
- Data integrity
- Code analysis
- Security testing
- Infrastructure and systems testing
- Network installation, connectivity and required bandwidth
- Recovery testing
- Procedure verifications like security, support, alerts, and stress

Both the iteration 1 and 2 will be followed by OATs to ensure the operationality of the system.

5.8 Information Security and Business Continuity

5.8.1 Information Security

The ICTA is preparing the following but no 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 ICTA.

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

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 success of identity and authentication services for all stakeholders other than citizens. It helps establishing 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) Biometric device certification process: MSI shall assist the ICTA to create, review, enhance, and implement processes for obtaining security certification of all biometric devices deployed by SL-UDI. MSI shall ensure that the biometrics are encrypted as and when they are captured at the device itself. Registered devices shall be used for the same.

(vi) IT asset certification process: MSI shall review, enhance, and implement of 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.

(vii) Risk assessment and treatment process: MSI shall develop and implement processes for identification, estimation, assessment, and treatment of security risks as well as Fraud Management 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 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 centres, 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. All minimum baseline security standards shall be prepared in consultation with ICTA.

5.8.1.3 Security Components for Implementation

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.

(i) Firewall Management (Internal and External).
(ii) Web Application Firewall.
(iii) HIPS/NIPS/NIDS.
(iv) IPS/IDS.
(v) SSL VPN Solution.
(vi) HSM.
(vii) Access Control System and Directory Services.
(viii) Anti-DdoS.
(ix) DLP Solution.
(x) Email Gateway.
(xi) Web Gateway.
(xii) 2 Factor Authentication.
(xiii) SIEM.
(xiv) PIM/PAM.
(xv) Virtual Desktop Infrastructure.
(xvi) Database Activity Monitoring.
(xvii) Web Vulnerability Scanner.
(xviii) Code Review Tool.
(xix) Network Vulnerability Scanner.

(xx) Anti-APT.

(xxi) Security Orchestration Automation and Response (SOAR)

(xxii) Patch Management Solution.

(xxiii) Antivirus.

(xxiv) IDAM.

(xxv) Network Detection and Response

(xxvi) Other security solutions / tools / products and hardware and software components mentioned in RFP and/or proposed by MSI.

For reference, the requirement of solutions on end-points 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.

S. No.	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 centres)	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 centres)	Server hosting the centralized EDR console (In DC and DR)
5	Intrusion Prevention System/Intrusion Detection System (IPS/IDS)	Not Applicable	IPS/IDS is an appliance that will be placed in DC and DR
6	Data Loss Prevention (DLP)	Endpoint DLP – All 4000+ endpoints (Including endpoints to be used in enrolment centres)	Network DLP – All Servers / Network gateways in Data Center and DR across all environments (Prod/Staging/QA etc.)
7	Email Gateway	Not Applicable	On Email server in DC and DR

S. No.	Security Solution	Coverage	
		Endpoint (Desktops, Laptops etc.)	Servers
8	Security Orchestration Automation and Response (SOAR)	Not Applicable	DC and DR server hosting the SOAR setup + Agents (connection is established) are installed on all servers/databases/app servers etc. to integrate with SOAR
9	Web Gateway	Not Applicable	Deployed on the network at the gateways which provide access to the internet
10	SSL VPN (Ipsec)	All such endpoints that will be required to connect to SL UDI data centre remotely (i.e., employee official laptops, enrolment centre staff connecting to data centre)	VPN is an appliance that will be placed in DC and DR
11	2 Factor Authentication (2FA)	2FA sizing is generally done per user/account	Server hosting the 2FA tool (DC + DR)
12	Web Vulnerability Scanner	Not Applicable	Server hosting the web vulnerability scanner tool
13	Code Review Tool	Not Applicable	Server hosting the code review tool
14	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
15	Network Vulnerability Scanner	Not Applicable	Server hosting the network vulnerability scanner tool
16	Hardware Security Module (HSM)	Not Applicable	HSM is an appliance that will be placed in DC and DR
17	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

S. No.	Security Solution	Coverage	
		Endpoint (Desktops, Laptops etc.)	Servers
18	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)
19	Virtual Desktop Infrastructure (VDI)	VDI licensing is generally per user. In SL UDI only certain internal users will be requiring VDI capabilities as per business requirement (Exact number can be decided once the manpower strength is estimated)	Server hosting VDI infra (DC + DR)
20	Access Control System and Directory Services	All 4000+ endpoints (Including endpoints to be used in enrolment centres)	All Servers in Data Center and DR across all environments (Prod/Staging/QA etc.) + Standalone server hosting the tool
21	Database Activity Monitoring (DAM)	Not Applicable	DAM agent to be installed on all Database servers in Data Center and DR across all environments (Prod/Staging/QA etc.) + Standalone server hosting the tool
22	Anti-Advanced Persistent Threats (Anti-APT)	APT should cover all endpoints, to monitor endpoint behaviour, traffic etc.	Anti-APT is an appliance that will be placed in DC and DR
23	Anti-DdoS	Not Applicable	Anti-DdoS is an appliance that will be placed in DC and DR
24	Identity and Access Management	Not Applicable	Server hosting IDAM suite
25	Network Detection and Response	Not Applicable	Server hosting NDR/NDR server console

Table 17 : 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. Conduct source code review and vulnerability assessment of all the software brought by the provider.
3. 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.
4. 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.
5. Ensure access control configuration to support SL-UDI access control policies.
6. Apply Security patches as per SL-UDI policy.
7. Ensure compliance to other security policies of SL-UDI.
8. The SL-UDI Platform software shall conform to the highest level of assurance and shall provide different, multifactor authentication services.
9. Ensure API Security or Microservice in line with SL-UDI. (This should be fully encrypted).
10. Ensure system security when doing the system scalability and increase concurrent user and transaction at a time.
11. Undertake security test and reporting automation.

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.

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. Conduct source code review and vulnerability assessment of ABIS software and biometric device drivers.
8. 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.
9. Enable secure logging and support integration with security solutions.
10. Deploy and integrate security solutions with the ABIS solution and biometric devices.
11. Apply security patches as per SL-UDI policy.
12. Backdoors and other vulnerabilities should be checked in a sandbox environment prior to installation.
13. **Ensure multimodal biometrics** compatibility.
14. Ensure device and security compliance compatibility. (Sri Lankan Laws, Policies, and International Compliance).
15. 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.
16. Bring in a proven record of technology in national-scale projects, like passport issuance and voter deduplication, etc.
17. Ensure fast matching in verification, identification, and deduplication modes. E.g., million comparisons per second on **each node** of the system.
18. Support scalable, modular architecture with high availability and fault tolerance.
19. Ensure that customization is possible for specific project needs.

20. 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. Perform periodic Vulnerability assessment and penetration testing on all infrastructure components.
3. Maintain a comprehensive asset register for all infrastructure components with CIA rating as per SL-UDI policy.
4. Ensure security configuration of the infrastructure components as per SL-UDI policy or industry standards such as CIS benchmarks.
5. Ensure access control on the infrastructure components as per SL-UDI policy.
6. Conduct source code review and vulnerability assessment of the software deployed on the infrastructure.
7. Enable security logging and support integration with Security solutions.
8. Provide BCP/DR provisions.
9. Ensure remote access security.
10. Ensure load balancing capability.
11. Ensure compatibility with software, security and device configurations, services, and architectures.
12. Support/conduct infrastructure system audit (internal and external)
13. Deliver physical security report of the infrastructure. (ex: Power/ Air Condition / Fire Protection / Access Control)
14. Apply security patches as per SL-UDI policy.
15. Backdoors and other vulnerabilities should be checked in a sandbox environment prior to installation.
16. 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.

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 analysing, detecting, preventing, and responding to cyber security threats and incidents.
6. Provide BCP/DR provisions and maintain compliance to ISO 22301 standard.
7. Maintain compliance to ISO 27001 standard.
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.
12. Support other service providers to deploy and integrate Security solutions.
13. Develop at least 20 or more response playbooks and runbooks and integration plugins, including the emerging attacks.

5.8.1.8 Threat Intelligence

The MSI to procure threat intel feeds. The MSI shall ensure that the source entity/organization from which Threat Intelligence (TI) is procured meets the following criteria:

1. The team which prepares, analyses & monitors the threat feed must have at least 50 researchers (The researchers must be working on TI sources such as threat intelligence gathering / dark web / deep web / other threat sources).
2. Threat intelligence feed shall also capture targeted attempts using deception technology.
3. At least 150K sensors monitoring networks; At least 2 billion emails per day; At least 1 billion web requests a day.

4. Proposed threat feeds should be mature with either industry experience of at least last 5 years in the security domain with or should be in the leader's quadrant of Gartner / Forrester Reports / similar for Threat Intel.

5. The threat intelligence interface should include complete threat visibility i.e., End-to-end details of threats from attack surface vulnerabilities to malware and actors behind the attacks.

6. Offer the ability to visualize indicator-of-compromise (IOC) relationships between multiple IOCs, threat actors, intelligence reports and, if applicable, first-party endpoint security product detections.

7. Offer the ability to visualize **Indicators of attack (IOA)** focus on detecting the intent of what an attacker is trying to accomplish, regardless of the malware or exploit used in an attack. Just like AV signatures, an IOC-based detection approach cannot detect the increasing threats from malware-free intrusions and zero-day exploits.

8. Provide custom, highly contextualized, analytical intelligence, proactively delivered based on threat intelligence collections.

9. TI feeds should be sourced from actual attacks including inspection of the decrypted TLS network traffic (as opposed to synthetic environments or honeypots) happening on Threat Intelligence Feed Provider's sensor network.

10. The threat intelligence report included in subscription must cover the following which is relevant to the SL UDI (indicative) – (a) Malware analysis; (b) Threat actor profiles; (c) Daily security news analysis; (d) Trending and forecasting; I Country risk profiles; (f) Industry risk profiles; (g) Futures scenarios; (h) Vulnerability analyses; (i) Vulnerability exploitation tracking; (j) Alerting on significant threat developments; (k) Integration of Indicators of Compromise (IOCs) & Indicator of Attack (IOA); (l) Crime ware, ransomwares; (m) Advanced persistent threats; (n) Financially, ideological, state-sponsored and strategically motivated actors; (o) Threats to emerging technologies, (p) MITRE ATT&CK Framework with TTP Integration - Common Platform Enumeration (CPE), Common Weakness Enumeration (CWE), and Common Vulnerabilities and Exposures (CVE)

11. Asset Intelligence: The Asset Intelligence service shall deliver regular profile updates for faster and more accurate anomaly detection. It helps focus efforts and reduce mean-time-to-respond (MTTR)

5.8.1.9 IT Hygiene

Common IT misconfigurations continue to be the root cause of many security breaches. Groups with too many permissions, unpatched systems, unprotected endpoint devices and excessive administrative rights are frequently exploited by hackers. The MSI shall conduct IT hygiene assessment to cater to areas such as week IT settings, common IT misconfigurations, excessive access rights, amongst others.

5.8.1.10 Security Processes and Procedures

The MSI shall ensure the **end-to-end design, 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. Some of the indicative and non-exhaustive security processes and procedures that shall be developed, documented, implemented, and maintained by the MSI are listed and described below:

(i) **Personnel security process**: MSI shall develop a process and apply security for resources employed in the SL-UDI ecosystem, prior to employment, throughout an individual's employment, as well as post-employment within SL-UDI.

(ii) **Physical and environmental security process**: MSI shall apply security controls for secure sensitive information processing facilities by defining security perimeters with appropriate security barriers and entry controls, along with equipment security within SL-UDI offices, data centres, and all other locations.

(iii) **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.

(iv) **Process for securing network components**: MSI shall develop processes to secure devices/ products/ solutions that provide secure storage, processing, and transmission environment in the SL-UDI data and management network.

(v) **Process for ensuring device level encryption**: MSI shall ensure that the biometrics are encrypted as and when they are captured at the device itself. Registered devices shall be used for enrolment and authentication.

(vi) **Key management process**: MSI shall develop processes for securing cryptographic keys in SL-UDI ecosystem. Key management is crucial to success of identity and authentication services for all stakeholders other than residents. It helps establishing 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.

(vii) **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.

(viii) **Processes to manage security solutions and devices**: MSI shall develop and implement process for management of each SL-UDI security solution.

(ix) **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.

(x) **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.

(xi) **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.

(xii) **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.

(xiii) **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.

(xiv) **Enrolment packet quality check process**: MSI shall develop processes and undertake quality check for enrolment packets which will contain citizen PII such as biometric and demographic information.

(xv) **Process for blacklisting of enrolment officers**: MSI shall develop and implement processes for blacklisting of enrolment officers involved in misconduct or non-compliance of SL-UDI policies.

(xvi) **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.

(xvii) **Process for de-duplication checks**: MSI shall develop and implement a Multi-level process for checking deduplication of biometric details.

(xviii) **Process for distribution of enrolment software**: MSI shall ensure secure and official distribution of enrolment software. The enrolment software shall be licensed.

(xix) **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.

(xx) **Secure login process**: MSI shall develop and implement processes for secure login, authentication, and access to SL-UDI systems.

(xxi) **New installations and maintenance process**: MSI shall ensure appropriate security controls are incorporated by design in all SL-UDI applications.

(xxii) **Change management process**: MSI shall ensure a comprehensive change management process by implementation of changes to application systems in a controlled manner, which shall be inclusive of recording of changes, impact assessment, testing and execution, rollback processes, and documentation of changes.

(xxiii) **Security incident management process**: 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, Business Impact Analysis (BIA), and incident closure.

(xxiv) **Secure SDLC process**: MSI shall apply security assurance activities such as penetration testing, code review, and secure architecture analysis of all SL-UDI applications, portals, etc. as an integral part of the development effort.

(xxv) **System hardening process**: MSI shall develop a process for hardening of all SL-UDI systems such as OS, desktops, servers, network devices, storage devices etc. MSI shall ensure that OEM guidelines are followed for such hardening.

(xxvi) **Biometric device certification process**: MSI shall develop and implement processes for obtaining security certification of all biometric devices deployed by SL-UDI.

(xxvii) **IT asset certification process**: MSI shall review, enhance, and implement of 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.

(xxviii) **Application certification/ onboarding process**: MSI shall ensure development and implementation of necessary security guidelines and measures before introduction or deployment of an application in SL-UDI network. MSI shall also evaluate and minimize impact to other existing processes, applications, devices, etc. affected by introduction of the new application.

(xxix) **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.

(xxx) **Application security testing process**: MSI shall identify and document security requirements in application software. MSI shall ensure security risk assessment on user specifications, secure information architecture, proper role-based access, secure code training to developers, change management, peer code review for security, external source code review, exhaustive security testing, secure implementation guidance, secure configuration of applications, etc.

(xxxi) **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.

(xxxii) **Vulnerability assessment and penetration testing process**: MSI shall develop and implement processes for quarterly internal and external vulnerability assessment and penetration testing of all SL-UDI applications.

(xxxiii) **Risk assessment and treatment process**: MSI shall develop and implement processes for identification, estimation, assessment, and treatment of security risks as well as Fraud Management in SL-UDI's applications, systems, office, and DC/DR locations, etc. basis SL-UDI's risk management framework. International standard ISO 27005 shall be followed for security risk assessments.

(xxxiv) **Security aspects in API specifications**: MSI shall develop API specifications for SL-UDI applications with security implemented in them.

(xxxv) **Security Exception Process**: MSI shall establish a security exception management process. MSI shall identify and report information security exceptions against SL-UDI security policies and processes. Security exceptions shall be tracked.

(xxxvi) **Third Party Management Process**: MSI shall establish processes for management of SL-UDI's third parties, service providers, etc. MSI shall provision for escrow agreements third parties for proprietary software provided.

(xxxvii) **Training and Awareness process**: MSI shall develop and implement processes for security training and awareness of all personnel employed with SL-UDI. Training and awareness shall include development of automated tool for training, mass security awareness sessions, posters, workshops, meetings, etc.

(xxxviii) **Data Backup and Restoration Process**: MSI shall develop, implement, and periodically review the process for data backup and restoration in line with the SL-UDI Business Continuity and Disaster Recovery plan.

(xxxix) **Secure Configuration Management**: MSI shall develop and implement processes for secure configuration of systems, solutions, devices etc. MSI shall ensure integration of security devices/ solutions etc. with existing or new SL-UDI infrastructure.

5.8.1.11 Security Control–s - Enrolment related Security

(a) 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

(i) All biometric devices shall be certified for security by a reputed agency and shall have liveness detection feature.

(ii) Enrolment software shall be provided by SL-UDI in signed binary form.

(iii) Every machine shall be uniquely identified via online registration.

(iv) Enrolment software shall only run-on systems that have been sufficiently hardened as per SL-UDI specifications.

(v) All officers shall have SL-UDI number, shall be trained, and certified, and registered with SL-UDI.

(vi) Every enrolment packet shall be biometrically signed by the officer.

(vii) Resident data including raw biometrics shall be encrypted at run time.

(viii) Every enrolment packet shall be encrypted. Encryption shall be done on the biometric capture device at hardware level (AES 256 and PKI 2048 bit).

(ix) Encrypted biometric packets shall not be stored at any other place other than enrolment packet.

(x) Enrolment software shall run an automated purging script to securely delete any enrolment packets older than the policy requirement.

(xi) Secure channel such as HTTPS shall be used to transmit the enrolment packer to SL-UDI DS.

(xii) Enrolment software shall be digitally signed, and signature shall be validated at server for every transaction.

(xiii) Enrolment software shall be developed in appropriate platform/programming language that prohibits reverse engineering of the software.

(xiv) GPS device 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.

(xv) Background checks shall also be conducted by DRP for all enrolment officers.

(xvi) Enrolment station (laptop, Desktop) shall protect with endpoint extended detection and protection solution.

(b) Security while transferring enrolment packets from Enrolment Devices

(i) Every enrolment data packet shall "always" be stored in PKI encrypted, tamper proof files.

(ii) Enrolment data shall "never" be decrypted in transit until it is reached SL-UDI.

(iii) 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.

(iv) The enrolment software having feature for secure upload of encrypted enrolment packets to SL-UDI shall be provisioned.

(v) All uploads shall happen only through registered upload stations which shall be initiated after a two-factor authentication.

(vi) Malware checks shall be done on the enrolment packets received in SL-UDI DS before processing the packet.

(vii) Enrolment software shall run a script to check the hygiene of the system such as EDR installed, patches are updated, OS is licensed etc.

(c) Security while storing enrolment packets in Identity Repository

(i) Validation of "all" enrolment packets for authenticity of source, authenticity of officers, overall validity of data, any tampering, viruses, etc.

(ii) Every sub-system including the biometric de-duplication systems shall be isolated and separated by firewalls.

(iii) Audits of access to sensitive data and audits of modifications shall be captured and analysed.

(iv) Additional metadata shall be collected as part of every enrolment packet for performance and fraud analytics.

(v) Enrolment packets shall be kept in encrypted format within SL-UDI.

5.8.1.12 Security Control–s - Authentication related Security

Following security controls shall be put in place by the MSI with respect to authenticatio**n)**

(a) Security while capturing Biometrics through Authentication Devices

(i) End to end encryption of identity data shall be enforced.

(ii) Only certified biometric devices, with liveness detection feature, shall be used for authentication.

(iii) Biometric Devices shall encrypt data at hardware level.

(iv) 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.

(v) HMAC within the authentication packet shall ensure no tampering is done.

(vi) Authentication requests shall be digitally signed by the UA to ensure authentication of the agency and non-repudiation.

(vii) Use of API license keys with built-in access and expiry controls shall ensure API endpoint authentication.

(viii) 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.

(ix) Background check shall be mandated for all officers of the authentication agency before providing access to authentication data or operations

(b) Security while transferring Authentication packets from Authentication server to Identity Repository

(i) Mandated channel security (device to UA server and UA to TSP server) shall be enforced.

(ii) TSP to Authentication Server connectivity shall be only over a leased/ MPLS network terminating the data centres along with IP filtering.

(iii) 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.

(iv) HMAC and DSC shall ensure end-to-end data integrity while 2048-bit encryption and SSL shall ensure end-to-end data confidentiality.

(v) Authentication packet shall be transmitted only on secure connection such as LAN, HTTPS or MPLS (if public network)

(vi) Encrypted biometric shall not be stored by the authentication agency post sending the authentication request to SL-UDI data store (DS)

(vii) Malware checks shall be done on the authentication packets received in SL-UDI DS before processing the packet.

(viii) Authentication packets that are rejected in the malware scan shall be securely deleted from the authentication server.

(c) Securing authentication packets in the Authentication Server

(i) 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.

(ii) Every authentication request shall be validated for authenticity of source (DSC), access control (License keys), structure (XSD), and integrity of identity data block (HMAC).

(iii) All encryption and digital signature handling shall be done via network HSM. All traffic requiring encryption/decryption/digital signature operation shall pass through the HSM at real time to fetch the keys/digital signature.

(iv) All responses shall be digitally signed and audited.

(v) All biometric/OTP authentication requests shall be notified to citizens/residents.

(vi) The Authentication database shall be encrypted all the time.

(d) Securing and monitoring authentication for all critical systems related to SL-UDI

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

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

5.8.1.13 Security Control–s - Security of SL-UDI data centres, data stores and administrative offices

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

Risk	Controls
Cyberattack from Internet	1. Security technologies for security by design 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 (Application front end hardware) g. HSM for secure storage of keys h. NG-SOC solution to monitor and prevent attacks

Risk	Controls
	2. Periodic vulnerability assessment and penetration testing 3. Periodic internal audits and external audits 4. Secure coding practices and checklists to ensure security of public portals applications 5. Process for onboarding of new applications and changes to applications to ensure security 6. Encryption of all data at storage and transmission to minimize the impact of cyber attack
Cyberattacks from Authentication partner network	1. Security technologies for security by design 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 (Application front end hardware) f. HSM for secure storage of keys g. NG-SOC solution to monitor and prevent attacks 2. Periodic vulnerability assessment and penetration testing 3. Internal audits 4. External audits for authentication partners 5. Secure coding practices and checklists to ensure security of public portals applications 6. Process for onboarding of new applications and changes to applications to ensure security 7. API based communication to ensure limited information exchange 8. 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	1. Virtual desktop infrastructure solution to ensure that data remains within the data centre. 2. DLP solution to prevent any data leakage. 3. HSM for secure storage of keys 4. PIM to control access to servers at OS level. 5. DAM to monitor access to databases. 6. SIEM to log internal activities and monitor real time violation of policies. 7. Encryption of data in storage and transmission to minimize the impact. 8. Federated databases and use of referencing to minimize loss of one single database.

Risk	Controls
	9. Web gateway and content filtering
Biometric data integrity within SL-UDI DS, and Demographic data integrity within SL-UDI DS	1. PIM to control access to servers at OS level 2. DAM to monitor access to databases 3. Encrypted raw packet is stored as it is and can be used to recreate the data 4. Federated databases and use of referencing to minimize loss of one single database

Table 18 : Security of SL-UDI data centres, data stores and administrative offices

5.8.1.14 Security and Governance Audits and reviews

Prior to go-live, the security audit is mandatory for each software release. After go-live, the security audit is to be carried out periodically (refer SLA). For the purpose of this security audit, the ICTA shall hire a third-party security auditor. As part of the security audit, the governance audit will also be carried out under this program through a third-party auditor.

MSI shall conduct independent audit and assurance assessments according to relevant standards by annually with ICTA nominated certified independent assessors including but not limited to GDPR, ISO, NIST, etc. standards annually. Further, MSI shall verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.

3) Moreover, MSI shall comply and adhere to the laws and regulations applicable in Sri Lanka and shall specifically meet the legal standards oa) Electronic Transactions Act No. 19 of 2006 (as amended by Act No. 25 of 2017);
   b) EU GDPR and Sri Lankan Personal Data Protection Act of 2022

5.8.2 ***Fraud Management***

A fraud management system (FMS) is required to detect and minimize identity fraud. Fraud is defined here as ‘an intentional attempt by a person or organization to gain illegal access to resources and benefits of the SL-UDI’s Technology Solution’. The objective of the fraud detection system is to ensure that fraudulent enrolment/authentication are detected and prevented.

The fraud management system should be able to detect frauds such as the following:

1. The system should be able detect and keep track of all the residents attempting to register multiple times.

2. The citizen may attempt to register by providing incorrect address, or parents information.

3. The system should be able to detect any attempt to create invalid registrations of people who don't exist or use incorrect information.

4. Identity theft by authenticating as someone else.

5. Other potential frauds

The fraud management system must have the following characteristics:

(i) It is important to ensure secure access to the fraud information. For example, the DBA should not be able to read the list of residents who have committed fraud or even delete a record of a citizen who has committed fraud.

(ii) The fraud detection system architecture should have a well-defined API for interfacing with other components of the SL-UDI's Technology Solution. The fraud engine and action engine sub-components should also have well-defined, standardized, flexible interfaces to allow use of emerging algorithms. Each component should have well defined interfaces for the system.

(iii) The fraud detection system must operate within the constraints of privacy and policies that are outlined by the SL-UDI.

(iv) The fraud could be detected during the enrolment process or during authentication. Frauds detected during enrolment should result in immediate action such as prevention of SL-UDI number generation.

(v) The fraud management system should be capable of handling huge volumes of data coming from enrolment, authentication, logs, and BI data stores.

(vi) A fraud engine should allow setup and configuration of fraud detection rules. Users should be able to add new rules/modify existing rules into the rule's engine of the FMS. For all such changes, audit history should be maintained.

(vii) The fraud engine should be a learning system i.e., should update its knowledge based on detection of frauds.

(viii) The following detection mechanisms (not limited to), should be supported:

   a. Graph based

   b. Fuzzy matching

   c. Biometric scores

   d. Authentication patterns

(ix) The FMS should also have a scoring engine. Score engines are designed to flag suspicious transactions. The engine calculates a score based on the available information. Score gives the probability in the range from 0-1, higher the probability higher the propensity of being fraud. Scoring engine should be able to provide a base-level logistic model to predict the suspected frauds.

(x) Based on inputs from the scoring engine and the rules engine, the FMS should be able to categorize frauds into high potential fraud, medium potential fraud, or low potential fraud. The threshold for high, medium, and low potential frauds should be configurable.

(xi) FMS operators/investigators should be able to request for a possible fraud inspection based on data inputs.

(xii) The following points describe some examples of the potential frauds attempted and expected response from the fraud management system. **The list is just indicative of possible fraud scenarios and should not be construed as an exhaustive compilation of all the possible scenarios and responses.**

(xiii) Scenario: A citizen applies for a SL-UDI number with wrong information under his/her name.

a. **Action:** The verification process returns application to the applicant and presents the reasons for not issuing a number.

(xiv) Scenario: A citizen attempts to apply to get a second SL-UDI number in another name.

a. **Action:** The application should be rejected, with the reason. If the per'on's name was fraudulent for the first time the citizen has the option of re-applying with changes to the demographic data. If this fraud is attempted again, the person is added to a watch list for legal action.

(xv) Scenario: A citizen appears as himself and applies for a second SL-UDI number.

a. **Action:** Application returned, with reason provided. If attempted more than three times the person is added to the watch list.

(xvi) Scenario: Person appears as another existing person, registering the second per'on's information under his fingerprint.

a. **Action:** The victim can report identity theft to the SL-UDI's grievance office. SL-UDI will undertake an investigation, and take appropriate action if theft is confirmed.

(xvii) Scenario: Impersonation of a deceased individual is done with fake supporting documents.

a. **Action:** If the applicant passes the verification process, then he may be able to take on the stolen identity. However, he will not be able to change his demographic fields over his lifetime without due process.

5.8.3 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 Centre 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 with 1:1 capacity

(ii) There shall be zero data loss while switching from Primary Site to Disaster Recovery site

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

(iv) The MSI will be responsible to transport the tapes to 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 and Business Impact Analysis for BCP/DR.
2. Identify and review risks and gaps created by disruptive events that may impact the Foundational ID platform
3. From a cross-functional BCP/DR team covering all services including ICTA’s teams such as authentication, registration, platforms, COTs to review data replication strategy between primary DC, and secondary DC (DR site). The team should also review DC-DR connectivity and failover procedures and perform the necessary upgrade as per the identified gaps.
4. Execute the processes and procedures as per BCP/DR plan and conduct periodic BCP/DR drills (refer SLA). The MSI should coordinate with ICTA and other associated partners to ensure successful completion of the BCP/DR activities.
5. Create the functional Business Continuity working plans for ICTA’s approval.
6. Periodically review the BCP/DR plan and update to reflect newly identified risks and gaps.
7. Stay compliant to the latest ISO 22301 standard - international standard for business continuity management system.
8. Develop business continuity and disaster recovery processes and procedures for all the solutions, addressing both IT and non-IT aspects of an emergency, with an intent to

limit human impact, minimize capital loss and enable early restoration of SL-UDI operations.

9. 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.
10. 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.
11. Develop a crisis communication plan to address external and internal communication before, during and after a disaster, to be executed by the management team.
12. Develop a comprehensive cyber crisis management plan in order to ensure that the information assets are protected from damage, unauthorized alteration, leakage, and other cyber risks. The key objectives of this plan would include timely identification of cyber incidents, assessment of situation and organization of a systematic approach for response, providing support for the business recovery efforts being made in the aftermath of the cybersecurity incident by liaising with management, and ensuring appropriate learning and reporting for future.

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 to provide 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 facing applications, CRM, email, etc.) and Active-Passive mode (for other applications).

(iv) Both RPO and RTO will be discussed and agreed between SL-UDI and MSI during the design phase.

(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.

(viii) Once provisioned our service management framework with change control and incident management will ensure your IT infrastructure is professionally managed and maintained.

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 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 Centre for continuous operations.

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

(iii) Network connectivity required for replication.

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

5.8.3.1 Process/component wise Recovery Strategy

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

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

Table 19: indicative list of recovery strategy of processes

5.8.3.2 RPO and RTO

An indicative list of the RPO (data loss) and RTO (down time) of various components is given below. The MSI is expected to validate the list given below:

Process/Component	Criticality	RTO	RPO	Rationale for RPO and RTO
Enrolment (SFTP server, Master Database, other internal applications involved in SL-UDI number generation)	High	24 hours	~Zero	**RTO**: Enrolment is an offline process and officers are required to sync/upload packets at least once a day, hence 24 hrs. is affordable. **RPO (Enrolment Databases)**: It is a business requirement that no data shall be lost in the ecosystem.
Authentication (Authentication APIs, Authentication Database)	High	~Zero	~Zero	**RTO**: Authentication is a highly critical online process, and it is anticipated that this service will be used for all social programs. **RPO (Authentication databases including logs)**: It is a business requirement that no authentication data shall be lost.
Critical Portals (Public facing portals such as SL-UDI's main website, pre-registration portal etc.)	High	~Zero	~Zero	**RTO**: These portals could be citizen facing and any downtime could have major reputational impact. **RPO (Logs databases and enrolment, Authentication databases)**: It is a business requirement that no data is lost from the logs database. Authentication and Enrolment databases will also have ~Zero RPOs.
Customer Relationship Management (CRM) system	High	~Zero	~Zero	**RTO**: CRM is a citizen facing service and any downtime could have major reputational impact. **RPO (CRM database, call recordings etc.)**: It is a business requirement that no data is lost from the CRM databases and maintenance of the databases also may be necessary for compliance to legal requirements.
Security Operations Center (SOC)	High	~Zero	~Zero	**RTO**: SOC is a very important security operation for SL-UDI. SOC should never be down as logs from various devices are collected by SOC and it is important that logs are always available for investigation purposes. **RPO (Log's file system, SOC configuration etc.)**: It is a business and legal requirement that

Process/Component	Criticality	RTO	RPO	Rationale for RPO and RTO
				logs are always available.
Email	High	~Zero	~Zero	**RTO**: Email is a critical service as a lot of other services depend upon email such as email to residents when SL-UDI number is generated or when a citizen authenticates. **RPO**: Email is a very critical service, and a lot of internal and partner communications take place on email.
Other portals (non-critical portals such as knowledge management, training, BI, etc.)	Medium	6 hours	~Zero if data other than logs ~24 hrs. if only logs	**RTO**: It is understood that these portals are not intended for public, and criticality of these portals is medium. **RPO (Logs databases and enrolment, Authentication databases)**: It is a business requirement to ensure there is no data loss in case data other than logs is present.
Network Operations Center (NOC)	Medium	6 hours	~24 hours	**RTO**: It is understood that NOC is an important process to monitor the availability of service and extended downtime could have a major impact on the business. **RPO (Ticketing database etc.)**: Ticketing database is not a critical database and hence loss of 24 hrs. of tickets can be afforded.
SL-UDI Office Locations	Medium	~24 hours	N/A	**RTO**: Office locations will not store any data. Hence, an RTO of ~24 hours is affordable. **RPO**: RPO in case of office locations is not applicable as no data will be stored.
Fraud Management System	Medium	24 hours	120 hours	**RTO**: Data analytics would be run, and the system should be operational for 24 hours. **RPO**: FMS uses enrolment and authentication as primary data source. This data is stored in a separate database, which can be recreated.

Process/Component	Criticality	RTO	RPO	Rationale for RPO and RTO
IT Helpdesk				

Table 20 : RPO (data loss))and RTO

5.8.3.3 Data Backup

The MSI is required to finalize the data back-up strategy in consultation with the ICTA'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 MSI** to offsite location on Daily basis at a geographically separate location with appropriate physical security controls, at par with banking regulator of Sri Lanka for such secure transfer, arranged by MSI.

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

Table 21 : Type of data for backup

5.8.3.4 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 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 22: 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 and should have provision for scaling in future.

5.8.3.5 VPN Access

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

a. VPN facility to be kept enabled for key staff.

b. Key staff to run the operations from locations designated by ICTA, if data centre site is physically inaccessible.

c. Minimal staff may be present in the Data Centres as far as feasible for on ground support.

d. This facility could be used when movement of staff is restricted due to natural disaster such as floods, or strikes, or pandemic.

5.8.3.6 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 Centre facility is down	• Alternate Data Centre with 100% capacity capability • Active-Active or Active-Passive based on criticality of operations and feasibility
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 (near zero) of all critical data in DR site and vice versa • Worst case scenario if data is lost from both data centres (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 23 : 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 component down resulting in unavailability of a particular process.

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

g. Recovery from Tapes.

5.8.3.7 Testing of BCP/ DR

MSI shall perform the following testing exercises, ensuring simulation of all possible failures:

S. No.	Test Type	Frequency	Details
1.	Diesel generator and UPS maintenance	Quarterly	Quarterly maintenance of DG and UPS as per OEM specifications.
2.	Full load power testing	Monthly	Shut down the power from the main electricity switch and test the auto start of Diesel generators and UPS battery support.
3.	DC, DR failover for all services	Half yearly	Power shutdown in one of the DCs and running the entire operations from the other data centre.
4.	DC, DR failover tests for Enrolment	Half yearly	Enrolment services shutdown in one data centre and entire enrolment operations are run from the alternate data centre.
5.	DC, DR failover tests for Authentication	Half yearly	Authentication services shutdown in one data centre and entire authentication operations are run from the alternate data centre.
6.	DC, DR failover tests for portals	Half yearly	Portal services shutdown in one data centre and entire portals operations are run from the alternate data centre
7.	DC, DR failover tests for CRM	Half yearly	CRM services shutdown in one data centre and entire CRM operations are run from the alternate data centre (DR).
8.	Fire drill	Half yearly	Building evacuation
9.	VPN	Half yearly	Specific staff members operate from home through VPN.
10.	Sample restoration of data from backup tapes	Fortnightly	Good sampling method shall be used to select random tapes and attempt recovery. Also, testing shall be done for time taken to bring the tapes from offsite to data centres.

S. No.	Test Type	Frequency	Details
11.	Full Data backup from tapes	Half yearly for 2 years and then yearly	Full data restoration and reconstruction of the database shall be carried out from the tapes. Initially half yearly activity and once activity is stabilized, frequency can be changed to yearly.
12.	Simulated phishing activity	Half yearly	Half yearly phishing attack simulation / social engineering exploits for all SL-UDI staff.
13.	Simulated ransomware activity	Half yearly	Half yearly ransomware attack simulation within SL-UDI staff, along with testing of data recovery.

Table 24 : Testing of BCP/ DR

MSI shall develop and implement processes and response procedures for business continuity and disaster recovery. MSI shall develop, implement, and periodically review the process for data backup and restoration in line with the Business Continuity and Disaster Recovery plan.

5.8.3.8 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.

5.8.4 Deliverables for Information Security and Business Continuity

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

S. No.	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	**First time:** Within 3 months of Go-live. Review on an annual basis subsequently

S. No.	Deliverable	Description	Periodicity
		of land within Sri Lanka. Indicative list of processes is as follows - a) Personnel security process b) Physical and environmental security process c) Process for security of SL-UDI data repository d) Process for securing network components e) Process for ensuring device level encryption f) Key management process g) Logging and auditing process h) Processes to manage security solutions and devices i) Access management process j) Asset management process k) 2-factor authentication process l) Business Continuity and Disaster Recovery processes m) Biometric exception process n) Enrolment packet quality check process o) Process for blacklisting of enrolment officers p) Process for use of portable media q) Process for de-duplication checks r) Process for distribution of enrolment software s) Patch management process t) Secure login process u) New installations and	

S. No.	Deliverable	Description	Periodicity
		maintenance process v) Change management process w) Security incident management process x) Secure SDLC process y) System hardening process z) Biometric device certification process aa) IT asset certification process: ab) Application certification/ onboarding process ac) Internal audit process ad) Application security testing process ae) User Acceptance Testing Process af) Vulnerability assessment and penetration testing process ag) Risk assessment and treatment process ah) Security aspects in API specifications ai) Security Exception Process aj) Third Party Management Process ak) Training and Awareness process al) Data Backup and Restoration Process am) Secure Configuration Management an) Privacy Policy related procedures such Data Retention, Data Archival, Notice and Consent, Data Governance etc.	

S. No.	Deliverable	Description	Periodicity
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 ICTA.	**First time:** Within 3 months of Go-live. Review on an annual basis subsequently
5	Access management review	MSI shall design the process and implement the same to do review of access management of more than 4000+ devices of SL-UDI which includes but not limited to databases, servers, AD, LDAP, Security Devices, Network Devices, Applications and ’PI's, etc.	**First time:** Within3 months of Go-live. Review on a half-yearly basis subsequently
6	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	**First time:** Within 3 months of Go-live. Review on a half-yearly basis subsequently

S. No.	Deliverable	Description	Periodicity
		shall also evaluate and minimize impact to other existing processes, applications, devices, etc. affected by introduction of the new asset.	
7	Change management review	MSI shall design the process and implement the same to do review of changes introduced in SL UDI environment to validate the implementation of approved change management process and measures before introduction or implementation of any change in SL-UDI environment and make enhancements to the existing process. MSI shall also evaluate the security impact to other existing processes, applications, devices, etc. affected by introduction of the new change.	**First time:** Within 3 months of Go-live. Review on a half-yearly basis subsequently
8	Patch management review	MSI shall design the process and implement the same to do review of patches introduced in SL UDI environment to validate the implementation of approved patch management process and measures before introduction or implementation of any patch in SL-UDI environment and make enhancements to the existing process. MSI shall also evaluate the	**First time:** Within 3 months of Go-live. Review on a half-yearly basis subsequently

S. No.	Deliverable	Description	Periodicity
		security impact to other existing processes, applications, devices, etc. affected by introduction of the patch. MSI shall also identify and evaluate comprehensive list of applicable patches within SL UDI environment and highlight missing patches as part of Patch Management review	
9	Encryption review	a) Data Encryption Review MSI shall review, provide policy recommendations and facilitate implementation of identified controls with respect to Data Encryption technologies and processes implemented in SL UDI ecosystem. MSI shall review and report on the compliance level of encryption mechanisms (including encryptions of storage devices) implemented to ensure compliance with the IS policy. b) Key Management MSI shall review the Key management procedures and provide recommendations and facilitate implementation as a primary responsibility to ensure that only authorized users can access and decrypt all encrypted data using	**First time:** Within 3 months of Go-live. Review on a half-yearly basis subsequently

S. No.	Deliverable	Description	Periodicity
		controls that meet operational needs and comply with data retention requirements.	
10	Backup review	a) 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. b) 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 infrastructure including but not limited to databases, applications, application and device configurations, etc.	**First time:** Within 3 months of Go-live. Review on a half-yearly basis subsequently
11	Biometric deduplication review	a) Deduplication Processes MSI shall review and validate the entire deduplication process from an accuracy and performance point of view. MSI shall assist SL UDI in measurement of	**First time:** Within 3 months of Go-live. Review on a half-yearly basis subsequently

S. No.	Deliverable	Description	Periodicity
		accuracy and reliability of the multi-modal biometric data captured at enrolment centers so as to prevent false matches. Review of the algorithms/software and hardware infrastructure used for deduplication b) Review of BSP processes Review the process which is being followed by BSP to carry the Biometric De-duplication and conduct the POCs to measure the accuracy of results produced by BSP as an output of Biometric De-duplication process.	
12	Personnel security review	MSI shall assess the adequacy and effectiveness of personnel security measures in SL UDI ecosystem and its compliance with Information Security Policy. The objective of the assessment should be to highlight the information security risks from personnel who have access to SL UDI information and provide relevant recommendations to mitigate the same. Some of the important aspects include but not limited to conducting background verification checks, confidentiality or non-disclosure agreements signed by employees, Contract or third party user confidentiality agreement,	**First time:** Within 3 months of Go-live. Review on a half-yearly basis subsequently

S. No.	Deliverable	Description	Periodicity
		process of training provided to employees (and relevant third parties) on information security as well as knowledge and awareness of security incident reporting.	
13	Physical security review	MSI shall perform the physical Security Assessment for SL UDI ecosystem facilities including but limited to DC, DR, any other premises which house infrastructure/ information/ data related to SL UDI processes among others. MSI shall also evaluate effectiveness of physical security controls and environmental controls	**First time:** Within 3 months of Go-live. Review on a half-yearly basis subsequently
14	Security Operations Center (SOC) review	As part of Security Operations Center Review, MSI shall a) Review the implementation of SIEM solution in SL UDI including but not limited to review of integration process which is being followed to integrate more than 4000+ devices with SIEM, review of SOC alerts, review the process of handling an incident logged in SIEM, review the process followed to investigate the alerts. b) Design the use cases specific to functioning of SL UDI and implement the same in SIEM to capture the incidents.	**First time:** Within 3 months of Go-live. Review on a half-yearly basis subsequently

S. No.	Deliverable	Description	Periodicity
		c) Design the customized parsers for the in-house build applications including but not limited to enrolment, authentication, internal and external applications, standalone applications, etc. d) Review the logging level of all the devices present in SL UDI to ensure appropriate collection of logs from all the devices integrated with SIEM. e) Conduct an analysis of all known attacks that have happened nationally and internationally including attacks on National ID programs and provide a report on the various threat scenarios. These possibly could be scenarios such as phishing attack, SQL injection, malware propagation, ransomware, command and control of data center etc. Refer to all known sources of information to identify these attacks. f) Include new rules for existing or new components as communicated by function owners or as per function requirements. g) Identify new rules based on the threats feeds. Also new rules should be identified on the basis of current or previous attacks trends on others National Identity programs or any	

S. No.	Deliverable	Description	Periodicity
		other critical infrastructure. h) Identify new rules on the basis of any security incident reported internally or externally on security incident management portal or any other communication channel or forum i) Identify attack scenarios and possible correlation rules. j) Provide a report on the rules that are required to be created in SIEM to detect such attacks. Report should also include all issues reported by other stakeholders to MSI through any means.	
15	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	During operations and maintenance phase on a quarterly basis

S. No.	Deliverable	Description	Periodicity
		time to closure, business impact, and criticality among others.	
16	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
17	Exception management review	MSI shall establish and report compliance on security exception process for obtaining exception against security policy requirements including step by step documentation, approval and retention of the records. MSI shall review Security Exception Management Process in SL UDI against the Policy and Industry best practices.	**First time:** Within 3 months of Go-live. Review on a half-yearly basis subsequently

S. No.	Deliverable	Description	Periodicity
18	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 plan 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 will be approved by SL UDI. Internal audit scope shall include security policy, procedures, ISO 27001 standard and regulatory compliance requirements as well.	**First time:** Within 6 months of Go-live. Review on a half-yearly basis subsequently
19	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:	**First time:** Within 3 months of Go-live. Review on annual basis subsequently

S. No.	Deliverable	Description	Periodicity
		identify, analyze, plan, track, control, and communicate Risk methodology. MSI shall refer to international standards such as ISO 31000, 27005 for risk assessment processes.	
20	Risk assessment and treatment plan	Risk assessment and treatment plan of all SL UDI process–s - 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 plan 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	**First time:** Within 6 months of Go-live. Assessment on annual basis subsequently

S. No.	Deliverable	Description	Periodicity
		consequences on SL ’DI's operations. It will involve identification, assessment and management. b) Risk Treatme–t - 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	
21	Risk register	Risk Register The assessment should be reported and identified risks should be stored in“a "risk regis”er" 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
22	Privacy framework	Drafting Privacy Framework for SL UDI MSI shall design a Privacy framework for SL UDI based on international standards such as ISO 27701, ISO29100, BS10012, GAPP etc. Framework should include all necessary components for a successful privacy program in SL UDI.	**First time:** Within 6 months of Go-live. Assessment on annual basis subsequently

S. No.	Deliverable	Description	Periodicity
23	Privacy gap assessment and privacy impact assessment	a) Privacy Gap Assessment MSI shall conduct an assessment of the privacy posture of SL UDI (Governance, legal compliance, standards compliance – ISO 27701, ISO29100 or BS10012, NIST Privacy Framework, etc., privacy inventory, privacy impact assessments, privacy audits etc.). b) Privacy Impact Assessment Conduct periodic privacy assessments to ensure that privacy compliance is being maintained by SL UDI to various legal obligations and ISO 27701, ISO29100, NIST Privacy Framework or other privacy standards or frameworks etc.	**First time:** Within 6 months of Go-live. Assessment on annual basis subsequently
24	Privacy inventory	Privacy inventory: Prepare a Privacy inventory for SL UDI and keep it periodically updated with help from SL UDI.	**First time:** Within 6 months of Go-live. Assessment on annual basis subsequently
25	Comprehensive compliance dashboard	Comprehensive Compliance Dashboard (Findings closure tracker and management dashboard (including internal audit, risk assessment, process reviews, privacy reviews, security solutions review, etc.)) Effective information	Monthly (Workshop/Presentation to ICTA stakeholders every month with the updated tracker and dashboard)

S. No.	Deliverable	Description	Periodicity
		security cannot be achieved through single, point-in-time security assessments. Rather, to achieve true security, it is paramount that MSI reviews and finalizes strategic and an executive compliance dashboard which incorporates risks related to people, processes, and technology identified through various assessment and audit activities, across SL UDI ecosystem and to employ appropriate measurements to manage and improve overall compliance. Consolidating this information and gaining both a comprehensive view of compliance is critical to the ongoing management of overall SL UDI risks	
26	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

S. No.	Deliverable	Description	Periodicity
27	Vulnerability assessment and penetration testing before go-live	Vulnerability assessment of applications, servers, network, security devices etc. before go-li–e - Vulnerability assessment of all IT assets should be carried out before go-live. MSI shall discover the live hosts, take IP range from ICTA 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.
28	Periodic vulnerability assessment and penetration testing report	Perform Vulnerability assessment and Penetration testing of entire SL UDI netwo–k - Vulnerability assessment of all IT assets should be carried out at least once every quarter. Vendor should discover the live hosts, take IP range from ICTA every quarter and take information from asset management database to identify the scan range. MSI should discover the live hosts, take IP range from ICTA every quarter and take information from asset management database to identify the scan range.	During operations and maintenance phase on a quarterly basis

S. No.	Deliverable	Description	Periodicity
		MSI shall ensure vulnerability closure as per the vulnerability management process and ensure continuous vulnerability closure revalidation activity is performed.	
29	Application security testing before go-live	Application security testing of applications, servers, network, security devices etc. before go-li–e - All applications, APIs, shall undergo security testing before go-live. MSI shall gather list of applications, APIs etc. from the ICTA management before initiating the testing 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.
30	Periodic application security testing report	Perform application security testing of applications, servers, network, security devices et–. - Application security testing of applications, servers, network, security devices etc. should be carried out at least once every six months. MSI should discover the live hosts, take IP range from ICTA every quarter and take information from asset management database to identify the	During operations and maintenance phase on a half yearly basis

S. No.	Deliverable	Description	Periodicity
		scan range. MSI shall ensure vulnerability closure as per the vulnerability management process and ensure continuous vulnerability closure revalidation activity is performed.	
31	Secure source code review before go-live	Secure source code review of applications, APIs etc. before go-li–e - All applications, APIs, shall undergo source code review before go-live. MSI shall gather list of applications, APIs etc. from the ICTA management before initiating the testing 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 any applications / APIs
32	Periodic secure source code review report	Perform secure source code review of applications, APIs, et–. - Secure source code review of applications, APIs etc. should be carried out at least once every year. MSI should discover the live hosts, take IP range from ICTA every quarter and take information from asset management database to identify the scan range.	During operations and maintenance phase on an annual basis

S. No.	Deliverable	Description	Periodicity
		MSI shall ensure vulnerability closure as per the vulnerability management process and ensure continuous vulnerability closure revalidation activity is performed.	
33	Phishing simulation exercise report	MSI shall assess the effectiveness of training and awareness to SL UDI employees and its ecosystem partners on social engineering attacks and phishing schemes which can divulge confidential information. Assess information security awareness levels for the SL UDI staff and its ecosystem. Social engineering audits and assessments for staff across levels SL UDI shall consider social engineering attacks and phishing schemes such as Spear Phishing, Media Mailing, and Onsite Media Drop, Phone Pretexting (IT/Help Desk and End Users), Onsite Pretexting, Client Public Information Profiling, etc.	During operations and maintenance phase on a half yearly basis
34	Report on training and awareness	a) MSI should prepare a training calendar and shall ensure coverage through LMS portal / in-person training for all staff (ICTA, MSI and other ecosystem partners of SL-UDI) across all locations and data centers on Information Security and Privacy policy,	First time: Within 3 months of Go-live. Report on yearly basis subsequently

S. No.	Deliverable	Description	Periodicity
		procedures,'do's and don'ts etc. MSI is expected to conduct training and awareness exercises as per the approved training calendar and submit proof of training completion (such as training records, feedback forms, attendance list etc.) to ICTA. b) MSI shall be responsible for designing the training content for the SL UDI which shall be used by SL UDI for delivering information security trainings to its various resources. These resources shall include presentations, emails, flyer, posters and quizzes on various security related topics on a periodic basis. SL UDI would use these training content for delivering the trainings and promoting the culture of information security in SL UDI.	
35	Design of fraud management process	MSI shall review and monitor the Fraud Risk Management (FRM) process to identify and address the Fraud 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	One Time (Before Go-live)

S. No.	Deliverable	Description	Periodicity
		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.	
36	Review and enhancement of existing fraud rules	Indicate list of activities include - a) Fraud risk exposure should be assessed periodically by MSI to identify potential 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 appropriately and timely manner e) MSI shall recommend based on leading practices in fraud management. f) Identify frauds in Enrolment and	During operations and maintenance phase on a quarterly basis

S. No.	Deliverable	Description	Periodicity
		authentication and revise fraud rules accordingly	
37	Security solution review and improvement report	MSI shall conduct security review of security solutions implemented. The periodic implementation exercise shall cover (not limited to) - a. Review of the security solution for all aspects such as architecture, integration with other devices, effectiveness, coverage etc. b. Fine-tuning of security solution based on inputs received from other assessments (such as risk assessment, internal audits, third party audits, vulnerability assessments, etc.) c. Suggestions / Measures to improve the effectiveness of the security solution d. Successful closure of any identified gaps or detailed plan of action for improvement e. Submission of review and improvement report to ICTA for review and approval. f. Conduct workshop with ICTA stakeholders highlighting the output of	First time: 12 months after Go-live. Post this, annually.

S. No.	Deliverable	Description	Periodicity
		review and improvements for each security solution g. Any other activity included in the scope of work of this RFP For list of security solutions refer to the Scope of Work of this RFP. All the security solutions review should be completed within defined timeline.	
38	Any other periodic activity described in the scope of work in the RFP	Refer to the scope of work of this RFP	-

Table 25 : Deliverables for Information Security and Business Continuity

5.8.5 Support (Contact Centre and Helpdesk)

5.8.5.1 Contact Centre Setup and Administration

(i) The SL-UDI Information System will require a Contact Centre which will be facilitated by DRP. The Contact Centre 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) DRP will provide a toll-free number for the Contact Centre and will bear the operational cost of this number.

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

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

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

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

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

(viii) DRP 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 centre will provide support in Sinhalese, Tamil, and English languages.

5.8.5.2 Deployment of CRM Solution for Contact Centre Operations

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

5.8.5.3 Deployment of Infrastructure for Contact Centre Operations

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

(ii) DRP shall provide physical space for the Contact Centre 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 Centre

h. Desktop/Laptop

i. Monitor

j. LAN connectivity

k. IP Phones

l. Network Connectivity between Contact Centre and DC, and Contact Centre and DR

m. Communication Equipment such as IVR, Dialler, EPBX, etc.

n. Software such as Computer Telephony Interface connector to integrate CRM and IVR, Call barging and recording software, etc.

o. Automatic Call Distributor (ACD) for distribution of incoming calls to Contact Centre 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 Contact Centre staff based on their availability to take calls on first come first serve basis.

- Standard features like Call Transfer, Conference, Barge-in, Dialled Number Identification Sequence (DNIS), Automatic Number Identification (ANI), and Caller Line Identification (CLI) etc.
- System should announce the queue waiting time for the caller before getting attended by a Contact Centre.
- System shall support the ability to play customized announcements per queue as defined by the administration.

(iii) MSI should provide recommendation for DRP to establish the Contact Centre with requisite IT and other Infrastructure to support the project requirements.

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

5.8.5.4 Other responsibilities of MSI for Contact Centre Operations

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

(ii) Training is an important aspect of the Contact Centre agents. The MSI should impart proper training in soft skills like call handling, exposure to related application 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 centre including call handling processes, quality assurance and escalation management.

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

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

5.8.5.5 Reporting

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

(vi) MSI shall facilitate MSP to prepare and submit reports to ICTA 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 Centre staffing

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

5.8.5.6 Monitoring

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

(ii) MSI shall be responsible to assist the SL-UDI officials in monitoring of the contact centre agents and operations.

5.8.5.7 Key features of the proposed Contact Centre

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

No. of Sea	3 5 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 DRP
Features	Contact Centre 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 26 :key features of the proposed Contact Centre

An illustrative list of queries and grievances that may be posted with the SL-UDI Contact Centre 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.

5.8.5.8 Sample Queries at the Contact Centre

An illustrative list of queries and grievances that may be posted with the SL-UDI Contact Centre 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 fees 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 • 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	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 I use? • What is the procedure for registration of authentication devices? • What is the virtual identity, can I use it

Queries (Sample)	Queries (Sample)
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 enrol 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 27 :Sample Queries at the Contact Centre

5.8.6 IT Helpdesk (Service Desk)

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

The MSI will facilitate MSP to operate a 7x24 hour service desk for customers to report network connectivity, 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 network specialists 24 hours per day, 7 days per week (24x7);

(ii) As customers frequently require support outside regular business hours, the service desk must be staffed with network support specialists capable of performing network equipment upgrades and configuration changes at all times;

(iii) Respond and resolve all network connectivity issues reported to the service desk and;

(iv) 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. This helpdesk will act as first point of contact for the end users for any IT related issue (application, infrastructure or functional). UDI-SD is expected to provide

L1 support to all end users of SL-UDI's IT Systems. For any query landing on UDI-SD, it will try to provide basic services to the end users based on Standard Operating Procedure (SOP) provided. The application related queries which cannot be handled using the SOP (L2 and above) will have to be routed to the Application Support Teams. For infrastructure related queries, the L2 and above issues shall be routed to Operations and Maintenance Team along with issues related to the hardware or security components shall be routed to the corresponding team.

MSI shall be accountable and responsible for all the proposed components and shall adhere to Service Level Agreement provided as part of the RFP. The MSI shall provide comprehensive onsite support to ICTA at the Data Centres and Disaster Recovery site on a 24x7 basis.

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

5.8.6.1 Helpdesk Setup and Operations

(i) MSI shall be responsible for setting up an IT helpdesk operation for the Local Partner to support IT issue resolution.
(ii) MSI shall prepare a detailed plan for implementation of IT Helpdesk in line with overall project timelines. Plan shall be prepared in coordination with the ICTA.
(iii) MSI shall be responsible to prepare standard operating procedures (SOP) for the IT helpdesk. The SOP should include detailed process flow for issue logging, issue prioritization guidelines, problem security codes and escalation procedures, issue resolution etc.
(iv) SOP should also include predetermined restoration/resolution targets based upon Service Level Agreements defined as part of this RFP.
(v) MSI shall deploy CRM software/ Incident Management module of EMS for the helpdesk which shall be accessible to all users through the SL-UDI portal (Intranet) for logging issues.
(vi) The IT Helpdesk should provide support in Sinhala and Tamil.
(vii) In order to operationalize the IT Helpdesk, the MSI will ensure seamless connectivity of the application with the DC and DR site.
(viii) The IT Helpdesk should have provision for call backs which is expected to be utilized in limited cases

5.8.6.2 Deployment of Infrastructure for IT helpdesk

(i) ICTA will provide PRI lines and a toll-free number for the IT helpdesk and will bear the operational costs of these items.

(ii) ICTA 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

(iii) MSI should ensure that the IT helpdesk has requisite IT and other Infrastructure to support the project requirements. MSI shall be required to provide and maintain all IT and Non-IT infrastructure (excluding only those items mentioned in points given above) required for successful operations of the IT helpdesk including, but not limited to, the following:

a. Communication Equipment such as IP Phones, IVR, Dialler, EPBX, etc.

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

c. Software such as helpdesk software, computer telephony interface connector to integrate helpdesk and IVR, call barging and recording software, etc.

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

e. 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
- Standard features like Call Transfer, Conference, Barge-in, Dialled Number Identification Sequence (DNIS), Automatic Number Identification (ANI), and Caller Line Identification (CLI) etc.
- System should announce the queue waiting time for the caller before getting attended by a helpdesk.
- System shall support the ability to play customized announcements per queue as defined by the administration.

f. Integrate Ticketing System, Helpdesk, NOC, SOC, Contact Centre, other integrations with DC/DR.

(iv) MSI will be responsible to integrate the infrastructure provided by DRP/ICTA with infrastructure provided by MSI to make the IT helpdesk operational

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

5.8.6.3 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 etc. so as to prepare the ICTA or nominated service providers staff at the IT Helpdesk to answer and resolve issues/ incidents.

(iii) The MSI shall include the cost of training the resources for any new process, modules, etc.

(iv) MSI shall be responsible for periodic training of the ICTA or nominated service providers staff at the IT helpdesk. A detailed training calendar should be prepared and submitted by the MSI to the ICTA.

5.8.6.4 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. License of the Helpdesk application shall be in the name of the ICTA.

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

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

d. The IT Helpdesk application would maintain 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 record 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 or EMS solution as the case may be.

5.8.6.5 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	MSI will be required to train the Managed Service Provider (Local Partner) to resolve the L1 issues by themselves and if required can escalate for L2 support team. L1 issues/ incidents are the ones which have a minimal business impact. These issues/ 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	MSI will be required to train the Managed Service Provider (Local Partner) to resolve the L2 issues by themselves and if required can escalate for L3 support team, i.e., MSI. It could be required that some of the L2 issues are important in nature and thus MSI will be required to address them. 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 level problems are the ones which have a critical business impact. The IT helpdesk will record such incidents and if required inform the MSI directly to address the issue at the earliest. L3 issues would be resolved by MSI. These problems could have any of the following characteristics: • Entire or part of any service unavailable (including APIs) • Incorrect behaviour 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 28 : Level Definition

(ii) IT Helpdesk staff should have a provision to increase the severity levels, if required.

(iii) 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

e. Any Other

(iv) MSI shall analyse all the 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 ICTA.

(v) Track and route incidents/service requests and to assist end users in answering questions and resolving problems. Assign severity level to each ticket as per the SOPs.

(vi) Issues which cannot be resolved by the IT Helpdesk should be routed to the concerned team of the MSI for resolution.

(vii) Escalate the issues/complaints, if necessary, as per the escalation matrix.

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

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

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

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

(xii) 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.

(xiii) 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).

(xiv) Continuous Improvement: MSI shall ensure continuous improvement in the IT Helpdesk Operations. The MSI shall:

a. Prepare Knowledge base for frequently reported problems along with the resolution steps/solutions and publish on the portal.

b. On a quarterly basis, carry out the analysis of help desk tickets (open and closed) to identify the recurring incidents and conduct a root cause analysis on the same. MSI shall submit a report to ICTA with the analysis and provide inputs to ICTA on user training requirements, awareness messages to be posted on the portal, redesign recommendations and/or application enhancements (functional/design) based on help desk ticket analysis. The objective of the analysis should be to address the repeat incidents and enhance the delivery of services to the end users.

(xv) MSI shall prepare and configure end-user dashboards as per the mutually agreed reporting structure.

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

a. Incident logs (category, severity, and status of call etc.)
b. Incidents escalated
c. SLA compliance/non-compliance report with reasons for non-compliance
d. Detailed analysis of the calls containing opportunities of automation, trainings, FAQs, etc.
e. IT Helpdesk utilization reports benchmarked against industry standards for similar application/environment.

From the biometric solution perspective (except biometric capture devices), for L1 support the BSP can 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:

f) ICTA will classify the issue as Critical or Non-Critical
g) BSP will undertake troubleshooting and communicate the estimated resolution time to the ICTA
h) ICTA shall approve the estimated resolution time
i) For critical issues, the BSP will provide a work around solution as soon as possible in agreed timeline
j) For all issues, the MSI will provide a resolution solution in timeline approved by the ICTA.

5.8.6.6 Reporting

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

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

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

i. Incidents escalated

j. SLA compliance/non-compliance report

k. Problem Management

l. Key learning from similar previous experience

m. Escalation procedure for handling significant issues

n. Helpdesk staffing

(iv) MSI and ICTA will mutually agree on the format of the reports to be submitted to ICTA. MSI must provide at minimum the following reports:

n. Reports based on time period

o. Type of grievances/queries/demand/analysis

p. Repeat request or complaints analysis

q. Call waiting time

r. Lost calls

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

t. Hourly call details

u. Complaints pending for more than defined time period

v. Calls Handled

w. Abandoned Call Rate

x. Delay Before Abandon (Average/Longest)

y. Staffing related Report

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

5.8.6.7 Monitoring

(i) MSI should extend all the required support to SL-UDI team for monitoring and access all subsystems and records pertaining to helpdesk operations for ICTA.

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

5.9 Security and Network Operations

5.9.1 Security Operations

5.9.1.1 SOC Setup

Note: ICTA/DRP will provide the location, utils, LAN network, furniture, and desks

MSI may refer Section 5.8.1.3 which provides a list of security components required for implementing security solution and security operations centers. The MSI is required to setup the SOC for which physical space will be provided by ICTA/DRP. 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 (including desktop/laptop, IP phones, monitors, etc.), Security Tools and Network (DC, DR, Helpdesk, NOC, Contact Centre, etc.)
(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, BIA, 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 – 12
(ii) Manager – 1
(iii) Supervis–r - 5
(iv) Tot–l - 18

In addition to above manpower, MSP will provide following manpower,

(vii) Analysts – 5
(viii) Supervisor – 5

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:

S. No.	Component
1.	Video wall with controllers, speakers, and other accessories
2.	LED TV
3.	Laptop

S. No.	Component
4.	Desktops / Monitors
5.	Keyboards and Mouse
6.	IP Phone
7.	IP PABX
8.	Printer (Network)
9.	UPS – 20KVA

Table 29 :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. • 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
Level 3 support	• Manage the security incident response processes and

Level	Services
activities will comprise of SOC supervision and management	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 30 :part of SOC operations

5.9.2 Network Operations

5.9.2.1 NOC Setup

Note: ICTA/DRP will provide the location, utils, LAN network, furniture, and desks

The MSI is required to setup the SOC for which physical space will be provided by ICTA/DRP. 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 (including desktop/laptop, IP phones, monitors, etc.), Network Tools and Network (DC, DR, Helpdesk, SOC, Contact Centre, etc.)

(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	• Manage the network incident response processes and procedures • Conduct advance analysis of network incident and prepares the

Level	Services (Indicative)
supervision and management	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 31 :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

Post completion of pilot enrolments of SL-UDI Information System, MSI is expected to undertake an impact assessment exercise to identify process, technology, and operation issues. 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.

5.10.1.1.1 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) **Survey of System Users:** MSI shall undertake a survey of ICTA & DRP 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. MSI shall support the MSP/ICTA & DRP and its employees to log-in the 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 quantum of daily enrolments. The report should include number of enrolments requested, number of requests processed, number of requests which failed, along with the reason for failure, time taken to process such request.

b. Present a report on quantum of authentications. The report should include 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 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.

(v) Study the enrolment process at fixed and mobile enrolment centers and identify possible improvement areas.

(vi) Study the issues raised by residents and other stakeholders using the contact center and/or IT helpdesk.

(vii) Analyze and operations of SL-UDI Data store to identify areas of improvements.

(viii) Incorporate changes in SL-UDI, with approval of the ICTA, prior to full-scale roll-out

5.10.1.1.2 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

(iv) MSI will be responsible to ensure clock synchronization on all IT assets

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 centre 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**

a. **Quality Assurance**: The services of assuring quality of enrolments including sampling and blacklisting/suspending the enrolment operator is covered under this aspect. The DRP will provide its manpower and MSI will be required to train this manpower.

b. **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 DRP will provide its manpower and MSI will be required to train this manpower.

c. **Biometric exception process:** MSI shall assist DRP 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 DRP will provide its manpower and MSI will be required to train this manpower.

d. **Enrolment packet quality check process:** MSI shall assist DRP 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 DRP will provide its manpower and MSI will be required to train this manpower.

e. **Process for blacklisting of Enrolment Officers:** MSI shall assist DRP to develop and implement processes for blacklisting of Enrolment Officers involved in misconduct or non-compliance of SL-UDI policies. The DRP 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 process. 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 services and these biometric devices will have to be pre-registered with the SL-UDI solution. The devices so 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

1. **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) Understand the legal framework for enrolment.

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

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

(iv) Setup of Enrolment Centres and its Administrative Users.

(v) Creation of training content for Enrolment/Authentication Officer training and question papers for certification examination. (refer to Section 5.10.2)

(vi) Resolution of queries of the applicants of certification examination through helpdesk.

(vii) 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.

2. Enablement of Partners for Authentication Services

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

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

(ii) 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

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

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

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

(vi) Facilitating the certification of biometric devices on make, model and specifications and making the details available on the relevant portal for the partners.

(vii) 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.

3. Process for Enrolment Partner Management

This section details the process and services to be provided by the MSI with respect to ICTA as Enrolment Partner. 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: First mile logistics (trainings, manuals, 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 – Partner and enrolment centre setup and preparation

a. Provi"e "Train the Trai"er" training for Enrolment administrators. Guide the ICTA's technical staff and enrolment centres staff in understanding SL-UDI System technical specifications.
b. Integrate the Public Key of the ICTA in Enrolment Software.
c. Assist in enrolment and PIN generation of the administrative users of ICTA.
d. Create the administrative users of the ICTA.
e. Contact Centre and Technical Support – Provide technical support the Enrolment Administrator and associated Enrolment Officer.

(ii) Step 2 – Enrolment Software Support

a. Monitor first-time client software installation at enrolment centre 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 centre on completion of setup through the Admin Portal.
c. Provide patches/updates to Enrolment software.
d. Provide technical support to ICTA to enable them to establish connectivity with the SL-UDI technology solution.

(iii) Step–3 - First mile logistics/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 centre.
b. MSI shall be responsible for upgrading/enhancing the data receipt mechanism.
c. MSI will provide suitable report for tracking and tracing enrolment packets (highlighting missing packets) to ICTA and DRP. Based on the directions of ICTA/DRP as well as proactively MSI shall be responsible for track and trace of all such packets and implementing checks as required by ICTA's information security policy.

d. MSI will provide provision for end-of-the-day quality control at the enrolment centre
e. MSI will provide provision for central quality control at the enrolment centre. In brief, the Central Quality Checks, at incident level, includes checks for age and gender mismatches/anomalies in the enrolment data. In addition, it shall also include visual checks for quality of face image captured. MSI shall assist the Data Quality Check process and shall also be responsible for ongoing process improvements in this area.
f. 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 ICTA 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.
g. MSI shall deliver data quality reports for each Partner and Enrolment Agency.

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

a. MSI shall assist the SL-UDI officials in manual adjudication.
b. For a variety of reasons unique number generation process may fail. MSI shall be required to intervene and resolve the issues that lead to rejection of an enrolment request. The various stages in which rejection could occur include the following, but are not limited to:
   - Manual Citizen Demographic Data Validation
   - ID verification and Biometric verification of Enrolment Officer
   - Manual Adjudication
   - Packet decryption failure
   - Duplicate UID

(v) Step–5 - Last mile logistics

a. MSI shall integrate with the postal providers (couriers, etc.) for successfully or rejected delivery

(vi) Grievance redressal

a. MSI shall offer assistance to Enrolment Officer’s in grievance redressal for residents who are denied a unique number.
b. MSI shall provide the required information as inputs to the Enrolment Officer that may be required for addressing any query/grievance of the citizen.

(vii) Management of Master Data and Profiles of ICTA, Operators and Enrolment Officers:

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

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

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

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

5.10.1.5 Authentication Services Management

(i) The 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 ICTA would appoint TSP and User Agencies (UA) in Sri Lanka for unique identity-based authentication services. It is expected that the ICTA 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 Identi–y - Authentication Services Implementation Framework which will be a document comprising set of standards, processes, protocols, privacy and liability policies, trust models, enforcement mechanisms and specification of authentication devices.

The various entities involved in authentication are:

(i) **Citizens and Residents of Sri Lan–a -** 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. Examples could include micro-ATMs, POS devices etc. These devices would have to be registered by the MSI

(iii) **Business Correspondents (BC)** – In future the SL-UDI System may engage with the Business Correspondents. MSI shall be responsible for designing the processes and protocols to integrate the business correspondents into SL-UDI System.

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

(v) **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 ICTA 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 ICTA 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 ICTA.

(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) ICTA 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 deduplication it is used to eliminate errors such as incorrect photograph, incorrect gender etc.

(iv) Post biometric deduplication it 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 ICTA's manpower to undertake manual adjudication
c. Define a mechanism to correct the data

[3] https://docs.mosip.io/platform/modules/registration-processor/deduplication-and-manual-adjudication

(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

c. The MSI will support redress procedures for citizens or foreign residents of Sri Lanka who were wrongly denied a unique on the basis of having a duplicate in the database

(vii) MSI shall be responsible for development of application required for manual adjudication as part of SL-UDI Software System.

(viii) MSI shall be responsible for provision of required IT Hardware for manual adjudication including desktops.

(ix) MSI is expected to prepare the Manual Adjudication Process in consultation with ICTA, BSP and MSP.

5.10.2 ***Enrolment Officer Certification Program***

5.10.2.1 Introduction

The program mandate is to provide a unique number to all the eligible citizens of Sri Lanka. For such a diverse and collaborative effort of successfully building the citizens' database, uniformity of enrolment and update process across the entire network of enrolment is essential. Achievement of such uniformity requires that the enrolment staff involved in the enrolment or update process at the field level is trained thoroughly to accomplish the job of enrolment. To address this need, MSI needs to develop a comprehensive Training Delivery Methodology and Training Content for all the stakeholders.

To ensure the relevant skills and proficiency to work as enrolment staff, a mandatory training and certification program is to be institutionalized for enrolment personnel to ensure adherence to quality aspects. The main objectives of the training are to make Enrolment Staff understand how to setup and manage an Enrolment Centre, use various devices required for enrolment, familiarizing audience with the enrolment software and how to handle exceptional cases through these programs. The training content for self-study should be made available by MSI at SL-UDI website for enrolment staff and other stakeholders.

Under this program, MSI will deliver need-based training through various programs like Master Trainer's Training and Orientation /Refresher program of enrolment staff.

5.10.2.2 Training and Certification of Master Trainers

In the first round, it has been envisaged that the training of Enrolment Officer shall be undertaken using a 'Train the Trainer' methodology. The MSI will be expected to train a team of 25 master trainers in a batch size of 5. The ICTA shall identify approximately 25 Master Trainers, and the same shall be communicated to the MSI. For successful training of the master trainers, the MSI must:

(i) Prepare training plan and schedule, in consultation with ICTA and obtain its sign-off.

(ii) Prepare and finalize the training content to be delivered during the training session in consultation with the ICTA, and obtain sign-off on the training content from the ICTA.

(iii) Prepare 25 training manuals in Sinhalese, Tamil, and English to be distributed to master trainers during the training. Obtain sign-off on the training manual from the ICTA. The actual bifurcation of the manuals to be printed in aforementioned languages shall be obtained from the ICTA. The approved training manuals will be uploaded on the KMS portal by MSI.

(iv) Train the Master Trainers, under supervision of the ICTA, in a location identified by the ICTA. The facilities for training like training classroom, projector, screen etc., would be provided by the ICTA.

(v) All Master Trainers shall undergo a certification test post training. MSI is expected to design the test methodology, tests, questionnaire, etc. in consultation with the ICTA. Master Trainers are expected to receive at least 90% of marks to be certified. MSI shall re-train all Master Trainers who do not receive 90% of marks, at no additional cost unless they obtain the required marks.

(vi) Upon successful certification, each master trainer will be allocated a biometric based unique identity, master trainer identity and enrolment operator identity. In absence of this, the master trainers should neither be able to train other operators nor carry out the enrolments.

5.10.2.3 Training and Certification of Enrolment Operators

Master trainer in turn would be responsible for training of other Enrolment Officers under supervision of the MSI. For successful training of the master trainers, the MSI must:

(i) Prepare training plan and schedule, in consultation with ICTA, for training of all Enrolment Officers and obtain sign-off of the ICTA.

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

(iii) Prepare printable training manuals in Sinhalese, Tamil, and English to be distributed to Enrolment officers during the training. The MSI will be required to obtain sign-off on the training manual from the ICTA and approved training manuals will be uploaded on the KMS portal by MSI.

(iv) Prepare online tutorials, videos, presentations that shall be uploaded on the KMS portal. Obtain sign-off on the online tutorials, videos, presentations from the ICTA. Upload the content on KMS post approval. At the minimum, the MSI shall prepare the following:

a. Trainer’s guide on Enrolment & Update
b. Lear’er's guide on Enrolment & Update
c. Lear’er's guide on the roles and responsibility of ecosystem partners
d. Test structure and other details
e. Question bank for Certification Exam
f. Any other relevant material for the purpose of this certification program

(vii) The master trainers will train the enrolment officers under supervision of the MSI, in a location identified by the ICTA. The facilities for training like training classroom, projector, screen etc., would be provided by the ICTA.

(viii) The MSI will be responsible for configuration, user creation, data entry, training data, etc. of all enrolment officers in the LMS portal to enable their training, learning and certification. The LMS will be integrated with the KMS portal for accessing all the content uploaded there.

(ix) All enrolment officer(s) shall undergo a certification test post training in which they are expected to receive at least 75% of marks to be certified. Master Trainers shall re-train all enrolment officers who do not receive 75% of marks. In case more than 25% of the batch receives less than 75% marks, the MSI will be responsible to retrain the corresponding Master Trainer.

(x) MSI is expected to design the test methodology, plan, questionnaire, etc. in consultation with the ICTA and obtain its sign-off.

(xi) Prior to commencement of the enrolment, all Enrolment Officers must be allocated a biometric based unique ID and enrolment office identity by the MSI. In absence of this, the officers should not be able to carry out the enrolments and/or updates.

5.10.3 Technical Services

5.10.3.1 Asset Management

1. 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 inflow and outflow of all assets from ICTA/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 ICTA 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.

2. 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 Centre and Disaster Recovery and at the Citizen Services Centres for Enrolment and Authentication.

(ii) MSI will take necessary approvals from the ICTA 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 Warranty or AMC services. ICTA 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 ICTA.

(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) MSI will be responsible for complying with all the regulatory requirements associated with transfer, addition and change of assets.

(vii) 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 ICTA.

(viii) MSI will be responsible for testing the newly added or changed asset in the SL-UDI Information System, for seamless integration and smooth operations.

(ix) MSI will be responsible for forecasting the requirement of any asset transfer, movement and change and also reporting after the activity successfully gets completed.

(x) MSI will be responsible to link the assets with their Warranty and Annual Maintenance services by recording details of incidents and problems observed and rectified vis-à-vis each asset.

3. Software Asset Management

(i) MSI will be required to set up procedures and documentation for managing 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 ICTA.

5.10.3.2 Cell Management

MSI will be required to manage and maintain the supplied hardware and associated components as part of cells. MSI shall be responsible for maintenance and management of cells including, but not limited to, the following activities:

(i) Estimate and forecast the demand of units of cells required in next 12 months in line with the growth in enrolment and authentication services system implementation. Further, MSI will also coordinate with the Biometric Solution Provider to assess the system requirements including performance, throughput etc.

(ii) Comply with the Services Levels pertaining to peak utilization in order to forecast cell requirements.

(iii) MSI will be required to submit a schedule of cell augmentation requirements to the ICTA for timely decision making and adherence to SLAs.

(iv) MSI will provide the Warranty for all the cells and associated components supplied as part of this engagement in accordance with the Warranty.

(v) MSI will be required to integrate the augmented cells with the existing infrastructure in SL-UDI-DS at Primary Data Centre and Disaster Recovery site to meet the requirements of the project whilst adhering to SLAs.

(vi) MSI will be required to continuously assess and optimize the configuration of cells and associated components, to increase the performance.

(vii) MSI will be required to update the architecture documents as and when the cells are augmented or removed from the system respectively.

5.10.3.3 Field Network Management

(i) MSI will be required to provide management services for the upkeep and maintenance of network. The MSI shall undertake the tasks to manage all network related operations at Primary Data Centre, Disaster Recovery Site, Network Operations Centre, and DRP will be responsible for Enrolment Centres. MSI will be responsible to maintain the desired Service Levels of network uptime and resolving issues pertaining to network as given in the SLA Annexure (Annexure 9).

(ii) Monitoring of network will be the responsibility of MSI team. Stakeholders will log incident calls through the Contact Centre to report the network related problems. MSI will undertake troubleshooting of issues and incidents logged by stakeholders.

(iii) MSI will establish mechanism to receive information pertaining to incident and problem logged at the Contact Centre 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.

5.10.3.4 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) Monitoring of traffic flow per IP address

(iv) Integrated DHCP, DNS, and IP address management

(v) IP alerting, troubleshooting, and reporting

(vi) Provide API Support for IP Address Management.

5.10.3.5 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.

5.10.3.6 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 request from citizens to get service request update information.

(ii) Outbound SMS shall be automated based on an event or time during service life cycle. For example, upon successful generation of an PIN number, enrolled beneficiary shall receive an SMS notification providing the PIN number.

(iii) MSI must integrate with a SMS Gateway to enable inbound and outbound SMS services. Cost of SMS Gateway and SMS charges shall be borne by the ICTA.

(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 ICTA on the SMS content before rolling out the SMS services.

5.10.3.7 Payment Gateway

The MSI will be responsible for integration of SL-UDI software system with multiple payment gateways. The ICTA will take responsibility of engaging these payment gateways (incl. security deposit), recurring charges, usage charges, etc.

5.10.3.8 Biometric Solution Management

The Biometric Service Provider (BSP) will be contracted by the ICTA through MSI, and shall install supply, install, commission, operate and maintain the ABIS solution, Biometric SDK, Manual Adjudication, etc. in the Data Centre 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 centre space for hosting of 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 ICTA.

(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 end-points on the servers of BSP.

(v) After the backup, the BSP will hand over the tapes to MSI. The MSI 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 project, the BSP shall impart training, to staff of ICTA 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 enrolment process. The workflow and integration of ABIS shall be 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 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.

5.10.3.9 Biometric device audit and certification agency setup

The enrolment and authentication devices in the SL-UDI ecosystem 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 put in place security controls for biometric capture devices, etc.

In a long-term basis (towards end of contract), the ICTA wishes to utilize a government lab to perform this testing, audit, and certification. For this purpose, either a new lab will be established or an existing lab will the authorized to perform the necessary testing and certification of biometric devices.

The cost of the biometric should be provided by the MSI. In case a local certification lab is available, ICTA will nominate an agency at equal or lower cost.

5.11 Warranty, Operations and Maintenance

At the successful UAT acceptance of iteration I and II, the related components will be operationalized (Go Live). From there onwards the 3 (three) months OAT phase will begin. Warranty, support and maintenance of the SL-UDI will commence with the go Live of iteration I.

5.11.1 Warranty Services

(i) The warranty should include the comprehensive Annual Maintenance Services and Annual Technical Support. The developer support should be provided when required.

(ii) MSI will be required to supply a comprehensive onsite OEM warranty of IT infrastructure supplied under this engagement for a period of 3 years (also referred to as "warranty period") from the go-live.

(iii) ICTA may opt to procure Annual Maintenance Services for all the infrastructure supplied under this engagement for a period of 2 year(s) beyond the warranty period.

(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 for a period of 3 years. For all components (including underlying tools and technologies of MOSIP), the MSI is expected to provide enterprise support for 3 years, wherever available.

(v) ICTA may opt to procure Annual Technical Support (ATS) for System Software, COTS, OTS, Middleware, etc. as supplied and commissioned under this engagement for the duration of 2 year(s) beyond warranty period.

(vi) For field infrastructure, the OEM shall provide comprehensive onsite warranty (including labour and parts) for the warrant period (3 years from the go-live). Any defect observed within 6 months of the supply shall be treated as manufacturing defect and the MSI shall ensure that the equipment is replaced without making any charge to the ICTA and DRP. The defects identified after 6 months would be treated as elaborated above sections. The equipment, if necessary, will be opened only by the OEM Engineer for repair/otherwise during the warranty period. The warranty shall cover the equipment/products should be repaired and made operational within 24 hours, failing which a replacement should be given till the equipment is repaired. In case of software, it shall be replaced.

(vii) MSI needs to have OEM support for ALL the IT Hardware components with documentation which shall be submitted to ICTA on annual basis.

(viii) MSI will be responsible for coordinating with the OEM for the rectification of any problem covered under the comprehensive warranty.

(ix) MSI will be responsible for resolution of any problem in IT hardware as per defined service levels.

(x) MSI will be required to maintain a log of Warranty and AMC status of each of the existing assets.

(xi) For assets whose AMC/Warranty is due for expiry, intimation to ICTA shall be provided at least 3 months prior to the expiry of the contract and MSI shall take action for renewal/extension of AMC/Warranty as per agreement with the ICTA.

(xii) In case any hard disk drive of any server, SAN, or client machine is replaced during warranty/AMC, the unserviceable HDD will be property of ICTA and will not be returned to MSI.

5.11.2 Support Mechanism– Description of Service Levels

5.11.2.1 Help desk Responsibilities

- First point of contact for all User queries / incidents
- Raise incident record for User reported incidents and maintain ownership of incidents until resolution found.
- Responsible for assignment of incident level based on service Incident Classification, applicable tiering and criteria detailed in the individual service SLA.

5.11.2.2 L1 - Support Team Responsibilities

- Undertake initial troubleshooting and attempt resolution of incidents.
- Responsible for reviewing and validation of assigned incident level based on service Incident Classification, applicable tiering and criteria detailed in the individual service SLA.
- Escalate and assign incident tasks t^{o} 2nd line support.
- Responsible for providing updates to Users, including communication of incident resolution and ticket closure.

5.11.2.3 L2 - Support Responsibilities

- Review incident level allocation that has been assigned b^{y} 1st line support.
- Send escalation emails for “1-Major” and “2-High” incidents.
- Escalate t^{o} 3rd line support and liaise with them for the resolution of technical incidents.
- Respond to tasks and requests from other teams in a timely manner.
- Lead preparation of RCA reports.
- Coordinate the change management process

5.11.2.4 L–3 - Support Responsibilities

- Assess impact and prioritise resolution during “Major” incidents.
- Investigate incidents including impact, provide root cause, recommend recovery actions, and provide fix.
- Provid^{e} 3rd party vendor technical support, development activities. i.e. OEM Support
- Lead preparation of RCA reports.

Note:

(1) As the overall solution (infrastructure, software, network, security, etc.) is being procured with 3 years of warranty (Section 5.11.1), the cost of support from OEM (incl. BSP) is expected to be included in the commercial proposal by the MSI.

(2) MSI is expected to procure the solution (infrastructure, software, network, security, devices etc.) in the name of the ICTA.

(3) In the contract between MSI and OEM, the MSI is expected to ensure that the MSP will be able to continue to obtain the warranty services (at no additional cost) for the selected components of the SL-UDI solution on behalf of ICTA at the end of 12 months after go-live till 36 months. Moreover, the contract should also permit the ICTA to procure the Annual Maintenance Services and Annual Technical Support from the OEM beyond the warranty period for at least 2 year beyond the 36 months.

(4) In the contract between MSI and OEM, there should be a provision for MSP to procure the developer support from OEM, wherever available.

5.11.3 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:

(i) 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 ICTA within the given timelines.

(ii) Any equipment, having 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.

(iii) In case of any disk failure on any server or SAN/HCI, this shall be replaced during warranty/AMC. Due to security reasons, the same will not be returned to the MSI.

(iv) Preventive Maintenance (PM) should be carried out of all hardware and testing for virus, 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.

(v) 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.

(vi) There should be warranty for all hardware, equipment, accessories, spare parts, software, etc. procured and implemented against any manufacturing defects during the warranty period specified in the tender document.

(vii) 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.

(viii) Adequate stock for spare parts may be maintained as per the SLAs

(ix) Perform regular hardening, patch management, testing and installation of software updates issued by OEM from time to time after following agreed process

(x) MSI shall provide maintenance support for support software's and Operating system over the contract period

(xi) Ensure overall security and ensure installation and management of every security component at every layer including physical security

(xii) Design and maintain Policies and Standard Operating Procedures

(xiii) 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.

(xiv) The MSI shall report any exceptions to license terms and conditions at right time to SL-UDI. However, the responsibility of license compliance solely lies with the MSI which shall be audited/verified by ICTA 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.

(xv) 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

(xvi) Proactive monitoring and Troubleshooting (related to Virtualization, Storage, Network etc)

(xvii) Perform Incident, Problem and Change Management w.r.t. to all Infrastructure and Security components included as part of the RFP

(xviii) Asset Lifecycle Management and providing integration interface for relevant data to be pushed in asset management solution

(xix) MSI shall provide operations and management services for compute, storage, and Database

(xx) MSI shall perform Backup Monitoring, Management, Reporting, including a backup management solution

(xxi) MSI shall provide Data Replication and DR management across Applicable Sites and shall leverage relevant tools to integrate the replication solution with monitoring solution for seamless DR activity

(xxii) The MSI shall leverage log monitoring solution for Reporting and Access Management

(xxiii) 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

(xxiv) Notify, escalate, and communicate to senior management on status of critical service requests, major incidents, and changes as necessary

(xxv) Implementing policies, Access Controls, managing clusters and certificates

(xxvi)User access management to infrastructure resources shall be managed by the MSI.

(xxvii) 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, support centres, operations centres, enrolment centres, etc.

As part of the overall Operations and Maintenance, following are the key activities:

(xxviii) Comprehensive and onsite manufacturer’s warranty 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 warranty for all hardware, equipment, accessories, spare parts, software, etc. procured and implemented against any manufacturing defects during the warranty period.

(xxix)Any equipment, having a hardware failure on four or more occasions in a period of less than three months, should have a replace ability assessment and agreement with the hardware supplier.

(xxx) In case of any hard disk drive of any server, SAN, or client machine is replaced during warranty/AMC, the unserviceable HDD should be maintained by the SL-UDI team.

(xxxi)Preventive Maintenance (PM) should be carried out of all hardware and testing for virus, if any, and proper records should be maintained at both DC and DR site for such PM.

(xxxii) 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.

(xxxiii) 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.

(xxxiv) Adequate stock for spare parts may be maintained as per the SLAs.

(xxxv) 24x7 monitoring and management of availability and security of the infrastructure and assets.

(xxxvi) Perform regular hardening, patch management, testing and installation of software updates issued by OEM from time to time after following agreed process.

(xxxvii)Ensure overall securi–y - ensure installation and management of every security component at every layer including physical security.

(xxxviii) Prepare documentation/policies required for certifications included in the scope of work.

(xxxix) Preventive maintenance plan for every quarter.

(xl) Performance tuning of system as required.

(xli) Design and maintain Policies and Standard Operating Procedures.

(xlii) User access management.

5.11.3.1 Management of Data Centre Sites (DC and DR)

MSI shall be responsible for undertaking the following activities for infrastructure maintenance:

(i) DC and DR operations to be in compliance with industry leading ITSM frameworks like ITIL, ISO 20000 and ISO 27001

(ii) Ensure compliance to relevant SLA’s

(iii) 24x7 monitoring and management of availability and security of the infrastructure and assets

(iv) Perform regular hardening, patch management, testing and installation of software updates issued by OEMs from time to time

(v) Ensure overall security by installation and management of every security component at every layer including physical security

(vi) Prepare documentation/policies required for certifications included in the scope of work

(vii) Prepare preventive maintenance plan for every quarter

(viii) Undertake performance tuning of system as required

(ix) Design and maintain Policies and Standard Operating Procedures

(x) User access management

(xi) Other activities as defined/to meet the project objectives and SLAs

(xii) Periodic update of all documents.

(xiii) During operations phase the MSI needs to submit proof of renewal of support for all IT infrastructure products and other system software's for whom it is mandated to have OEM support. This needs to be submitted on an annual basis and needs to be verified by the ICTA.

5.11.3.2 Infrastructure Management

This includes the design of an appropriate system administration policy with precise definition of duties and adequate segregation of responsibilities and obtaining the approval for the same from ICTA. 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 as 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

5.11.3.3 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
L2 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

Level	Services
	• 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

5.11.3.4 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 Centre, 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 & ICTA 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 the 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 ICTA on need basis.

e. MSI shall implement a password change mechanism in accordance with the security policy formulated, and in discussion with ICTA and based on the industry best practices/frameworks like ISO 27001, ISO 20000 etc.

5.11.3.5 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 Centre, and Disaster Recovery site.

(ii) MSI shall also ensure proper configuration of server parameters and performance tuning on 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, 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) ICTA/MSP 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 latest technologies so as to provision the existing and applicable infrastructure, if required.

5.11.3.6 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 to create/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
Level 1 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 32 : storage operations below activities

5.11.3.7 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 of the database, ensuring the integrity of the data and configuring the data dictionary.

(iv) MSI will follow guidelines issued by ICTA 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.

5.11.3.8 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 ICTA & DRP. The MSI is responsible for getting acquainted with the storage policies of ICTA before installation and configuration. It should be noted that the activities performed by the MSI may be reviewed by ICTA.

(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 ICTA 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 a 24 x 7 support for file and volume restoration requests at the Primary Data Centre, 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
Level 1 support services	• 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 33: backup operations activities

MSI shall develop processes to secure devices/ products/ solutions that provide secure storage, processing, and transmission environment in the data network.

5.11.3.9 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 Centre, 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 Centre, 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 Centre, and Disaster Recovery sites for access of system.

5.11.3.10 Security Management

MSI's scope of work for Security Management includes the following:

(i) Regular hardening and patch management of components of the SL-UDI Information System as agreed with ICTA.

(ii) Performing security services on the components that are part of the ICTA environment as per security policy finalized with ICTA.

(iii) Manage and monitor safety of information/data (IT Security Administration).

(iv) Reporting security incidents and resolution of the same.

(v) Proactively monitor, manage, maintain, and administer all security devices and update engine, signatures, and patterns as applicable.

(vi) Managing and monitoring of anti-virus, anti-malware, phishing, and malware for managed resources.

(vii) Ensuring 100 percent end point detection and response coverage with patterns not old more than period agreed on any given system.

(viii) Reporting security incidents and co-ordinate resolution.

(ix) Monitoring centralized pattern distribution (live update) and scan for deficiencies.

(x) Maintaining secure domain policies.

(xi) Secured IPsec/SSL/TLS based virtual private network (VPN) management.

(xii) 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.

(xiii) Resolution of calls for security notifications, system alerts, vulnerabilities in hardware/software and alerting ICTA as appropriate.

(xiv) Performing patch management using software distribution tool for all security applications including content management system, antivirus, and VPN.

(xv) Providing root cause analysis for all defined problems including hacking attempts.

(xvi) Monthly reporting on security breaches and attempts plus the action taken to thwart the same and providing the same to ICTA.

(xvii) Maintaining documentation of security component details including architecture diagram, policies, and configurations.

(xviii) Performing periodic review of security configurations for inconsistencies and redundancies against security policy.

(xix) Performing periodic review of security policy and suggest improvements.

(xx) 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.

(xxi) Policy management (firewall users, rules, hosts, access controls, daily adaptations).

(xxii) Modifying security policy, routing table and protocols.

(xxiii) Performing zone management (DMZ, MZ).

(xxiv) Sensitizing users to security issues through regular updates or alerts/periodic updates/Help. Support ICTA in issuance of mailers in this regard.

(xxv) Performing capacity management of security resources to meet business needs.

(xxvi) Rapidly resolving every incident/problem within mutually agreed timelines.

(xxvii) Testing and implementation of patches and upgrades.

(xxviii) Network/device hardening procedure as per security guidelines.

(xxix) Implementing and maintaining security rules.

(xxx) Performing any other day-to-day administration and support activities.

(xxxi) 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

(ii) Monitoring the security of the system

a. As per the incident reports shared by the MSI, Third Party Auditor, ICTA, etc.

b. Audit review tools

c. Manual processes

(iii) The MSI shall co-operate with the appointed representatives of ICTA 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 ICTA on a weekly basis. The significant security incidents will be reported on an immediate basis.

(iv) The MSI and MSP shall produce and maintain system audit logs on the system for a period agreed by the MSI and ICTA, at which point they will be archived and stored at off-site or as desired by ICTA. The MSI and MSP will regularly review the audit logs for relevant security exceptions.

5.11.3.11 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 a human intervention and would result in automatic resolution also.

5.11.3.12 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.

(v) Incident Management will be governed by internationally recognized best practice frameworks and tools.

(vi) For IT Service Management, ITIL v3 is the chosen framework and ISO/IEC20000 is the chosen quality standard.

(vii) 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.

(viii) All incidents are stored in a common repository and updated throughout their lifecycle.

(ix) Information on the status and progress of incidents will be available to the client of the affected service.

(x) Predetermined restoration targets shall exist for incidents based upon their Service Level Agreements.

(xi) Incidents will be prioritized and resolved based on the impact and urgency assigned them.

(xii) A full escalation management policy will exist to ensure unresolved incidents become resolved.

(xiii) All aspects of major incidents are controlled and coordinated by the Incident Manager.

(xiv) A continual process of process improvement will take place utilizing the 'plan-do-check-act' cycle.

5.11.3.13 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 tool, servers/devices, and all equipment. Any changes in the configuration manual need to be brought to the notice of the ICTA. Configuration manual should be updated periodically.

5.11.3.14 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 ICTA’s name
- ICTA should be able to renewal of software licenses at the end of the contract.
- License coverage MUST be for the entire duration of the contract
- Cost of all license should be covered with in the proposal and in the total contract price.

5.11.4 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 contract. SL-UDI Software System maintenance and management support includes, but not limited to, troubleshooting, and 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 the MSI while ensuring that the SLA requirements are met at no additional cost to the ICTA.

(ii) MSI shall be responsible for first level maintenance and management of the MOSIP application suite from agency of IIIT Bangalore, India, shall also 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.

5.11.4.1 Annual Technical Support

The MSI shall be responsible for providing annual technology support for the COTS/OTS products supplied by respective OEMs during the entire maintenance and management phase.

It is mandatory for the 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.

5.11.4.2 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 the MSI. Technical upgrades of installation to the new version, as and when required, shall be done by the MSI. Any version upgrades of the software/tool/application will be done by the MSI after seeking prior approval from the ICTA 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 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. A detailed process in this regard will be finalized by the MSI in consultation with the ICTA.

(v) An issue log shall be maintained by the MSI for the errors and bugs identified in the solution as well as any changes implemented in the solution. Issue log shall be submitted to the ICTA monthly.

(vi) The MSI will inform the ICTA, 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 ICTA 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 documentations and Knowledge databases etc. The MSI will carry out all required updates/upgrades by following a defined process at no additional cost.

5.11.4.3 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) IIT-B or its nominated agency will also provide maintenance and management support of MOSIP application suite at OEM Level which can be utilized by MSI on need basis.

(iii) The process for escalation of support tickets will be specified in consultation with ICTA.

5.11.4.4 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 or 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. ICTA will scrutinize the analysis presented by the BSP and may approve the exercise of re-template creation. Upon approval from ICTA, the BSP should undertake this exercise and submit a periodic progress report to the ICTA.

(ii) The BSP shall provide warranty for biometric solution for the duration of contract, commencing from the date when the system goes "live". The warranty 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 warranty 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, version upgrades relevant for the biometric solution at no extra cost to ICTA. ICTA should be informed of all version upgrades (minor & major), patches, releases and enhancements along with impacts to the biometric solution. ICTA will review the impact of the change and will its own discretion decide if the change should be implemented. The BSP will install, test and configure the changed solution in the various environment.

(v) BSP shall be responsible for software version management, software documentation management reflecting current features and functionality of the solution.

(vi) For the support, the BSP may decide 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 ICTA 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, procedure 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) The OEM (BSP) of the biometric solution will be responsible for performance tuning of the biometric solution. The OEM (BSP) will conduct the performance tuning at least as per below mentioned schedule:

a. Within 1 year of go-live: Once in every 4 months,

b. After 1 year from go-live: Once in every 6 months, and

c. During Exit Management: Once

(xii) 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.

After fine tuning the biometric solution, the BSP should re-run the deduplication process on existing records to determine errors occurred during previous deduplications. The BSP should inform the ICTA about the results on this exercise and propose corrective measures.

5.11.4.5Issue 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 ICTA & MSP along with recommended solutions.

5.11.4.6Change and Version 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 version control process through version 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 version control is carried out for the entire contract duration.

5.11.4.7 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.

In the context of SL-UDI Information System, release management is required to be handled at two levels

(ii) .

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 the

MSI. It will be responsibility of the MSI to obtain the modified software and carry out user acceptance test, if required, and then deploy in the product environment.

b. Software incidents related to support application or other enhancements would require change in the respective modules. T It will be responsibility of the MSI to test the modified software (including UAT, if required) and then deploy in the product environment.
c. If any downtime is required, prior approval should be taken from the ICTA 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 to the ICTA for sign-off.

5.11.4.8 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. Any other explanatory notes about system
e. Traceability matrix

f. 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 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.

5.11.4.9 Support during System Audits

(i) The ICTA may get the system audited b^{y} 3rd party auditors. The MSI shall provide necessary support and co-operation for the audit and close the findings of the audit.

(ii) The ICTA 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.

5.11.4.10 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 and BSP will report to ICTA on various aspects of the project. The MSI and BSP will prepare a draft reporting plan containing area of reporting, type of reports and reporting frequency. Upon ICTA'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 and BSP will submit a signed hard copy of reports. The other reports can be sent on email to the recipients decided by the ICTA.

The MSI and BSP will be required to broadly prepare and submit reports under the 4 categories – (i) ABIS, (ii) Data Quality, (iii) Incident and Issues, (iv) SLA and (v) Other reports. The details 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, generate 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 the 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
    (a). **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

    (b). **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

    (c). **Quality of Operators and Devices**: The quality of data is also dependent upon the operator, enrolment centre facility and device. Thus, to ensure the good quality of enrolment, the BSP should submit a statistical and quality analysis for operators, enrolment centres, 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. The Compression will not alter the quality of 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 exception, if despite best efforts image captures do not meet quality standards. The BSP should design and implement 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 ICTA authority on monthly basis. This will help ICTA 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 centre 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 the 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 centre 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 the ICTA and DRP and finalize the reporting requirements in consultation with them. The MSI and BSP will be responsible to prepare and submit the reports in the approved format and frequency.

6. Implementation Schedule

6.1 Implementation Schedule

Note: T – Date of Commencement –

Note: for actual Project Duration Refer Figure 6 : SL-UDI Project Duration in Section 3 Project Scope of this document.

No	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

No	Milestone	Duration (in Months)	Timeline (in Months)
3.	Detailed Design (Iteration_1)	1.0	T + 2.5
4.	Setup of Hosting Infrastructure (LD Effected milestone)	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 Acceptance (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
12.	Operational Acceptance (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 34: Implementation Schedule

6.2 Implementation Milestones

Note: ED – Effective Date as specified in Volume 1

No	Milestone	Output
1.	**Kick-Off and Planning /** **Setup of PMO and Advance Payment Security**	i) Kick-Off Meeting Presentation ii) Setup of Project Management office in Sri Lanka within the one month of signing Contract. iii) Upon submission of Advance Payment Security. iv) Inception Report v) Detailed Project Plan vi) MOSIP Takeover Plan vii) Manpower Deployment Plan (Monthly) viii) Manpower Compliance Report ix) Manpower Escalation Matrix x) Template for Risks and Issue Tracker and Periodic Status Reports xi) Launch of project management tool (on public cloud) with project management plan xii) Launch of task management features on the project management tool xiii) Signed contracts with Service Providers (Data Centre, Network, etc.) and OEMs

No	Milestone	Output
		xiv) Acceptance criteria for deliverables.
2.	**Requirement Gathering and Initial Design**	i) Template for capturing requirements and system documentation ii) Detailed plan for requirement gathering iii) Identification of stakeholders for requirement gathering in accordance with detailed plan iv) Detailed Application, Data, and Infrastructure Architecture Definition Document v) Metadata Standards vi) Demographic Data Standards vii) Biometric Standards viii) Minimum baseline security standards ix) Infrastructure requirements of the project (as per scope of work) x) 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. xi) High-level design and architecture documents for DC/DR infrastructure, platforms, software, security solutions, NOC/SOC, Network, etc xii) Implementation plan of Data Centres, Contact Centre, IT Helpdesk, Network Operations Centre, Security Operations Centre, Service Centre, etc. xiii) Documentation for COTS/OTS Applications xiv) Detailed document on the model registration centre xv) SL-UDI SLA methodology creation xvi) Risk Assessment (Business and Technical) xvii) RACI Matrix xviii) Detail Cutover Plan and pilot rollout plan
3.	**Detailed Design (applicable for Release_1 as well as Release_2 components)**	i) Functional Requirement Specifications (FRS) ii) Use Case Design Document (UDD) iii) End to End Software Requirement Specification (SRS) iv) 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.

No	Milestone	Output
		v) Low Level design document, with detailed algorithms and logic of the important API's stored procedures etc. vi) 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) vii) UI/UX Style Guide viii) Traceability matrices with updated design features against the requirements
4.	**Setup of Hosting Infrastructure**	**Site Setup** i) Establishment of co-location space within the hired data centres ii) Plan for commissioning of Primary Data Centre and Disaster Recovery iii) Site Survey Report for Primary Data Centre and Disaster Recovery iv) Detailed plan for site set-up v) Rack Plan vi) Data Back-up strategy vii) Disaster Recovery Strategy and Procedures **IT Infrastructure –** (i) Strategy, Approach, Design, Architecture, and Plan for commissioning of Primary Data Centre and Disaster Recovery (ii) Supply, (iii) Installation and Commissioning of IT Infrastructure(among others hardware. software, appliances, platforms, security, network connectivity ..etc) (iv) Deployment Plan(among others overall DC/DR deployment , server deployment, storage, network, virtualization, enterprise container platform, security ..etc). (v) Creation of environments relevant for this stage in DC and DR sites. (vi) Test Plan and Commissioning Report

No	Milestone	Output
		(vii) 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 centres to DC, DR (viii) BCP and DR test plan and report.
5.	**Software Development and Testing**	(i) Setup of DevSecOps environment in the DC and DR (ii) Solution Implementation Plan (including integrations) (iii) Updated design documents (if any) (iv) GUI wireframes (v) Prototypes (vi) Data Model Descriptions (vii) Software Development and Customization (viii) Technical and product related manuals (ix) Source code of the applications with version control mechanism in the source code repository (x) Change management histories (xi) Testing Strategy and Test Plan for various types of testing (automation testing, integration testing, system testing, performance testing, security testing and user acceptance testing) (xii) 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) (xiii) For BCP and DR testing the test report, recovery logs and learnings report (xiv) Draft documentation for relevant components on installation guides, user manuals, system administrator manuals, Toolkit guides and troubleshooting guides (xv) Draft Training Plan (xvi) Release management plan
6.	**First Software Release (Iteration_1 components) , Benchmarking**	**Software** (i) Iteration 1 release and deployment on relevant environments (including production environment) (ii) Source code of the applications with version control mechanism in the source code repository **(iii)** Secure source code review **System Documentation** (iv) Updated design documents (FRS, SRS, UDD, etc.) if any

No	Milestone	Output
		(v) 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. (vi) Documents revised after previous milestones (vii) SOPs, procedures, policies, processes, etc. (viii) Frequently asked questions guide **Benchmarking Testing (BT)** (ix) Confirmation of readiness of system for BT (x) Formal submission of final versions of system (incl. ABIS/SDK) to be tested for BT and confirmation about the same. (xi) Creation of BT environment, as per required specifications, (xii) Installation of BT tools (includes development of logging tools for passive tests within the production environment) (xiii) Integration of BT suite with system (xiv) Generate artificial test data, if necessary, and acceptance of sample data (xv) Participate and monitor the conduct of tests and review of test logs provided after the tests (xvi) Investigate system results to determine deficiencies in performance of system, and performing analysis of test logs xvii) Benchmarking test report in the format specified by ICTA / DRP xviii) Identify the gaps between current infrastructure and requirement infrastructure to meet the performance requirements (xix) Prepare the differential bill of material as per the gap (xx) Supply, install, and commission the material as per differential bill of material (xxi) Repeat the relevant activities for re-test xxii) 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**

No	Milestone	Output
		xxiii) Carryout a Complete software audit for the Iteration 1 release and ensure the Iteration 1 is complaint. xxiv) Carryout an Information Security audit for the complete end-to-end Iteration 1 release, including infrastructure, platform, etc. ensure the Iteration 1 is complaint. xxv) Facilitate the third-party independent Information Security audit carried out by ICTA ensure the Iteration 1 is complaint. **Training** xxvi) Final Training Plan xvii) Training Material, Training Manual, Training Content, Conduct of Trainings, and Satisfactory assessment reports for Trainings viii) Approved online tutorials, videos, presentations loaded on KMS xxix) Process for Manual Adjudication xxx) Training plan and material on manual adjudication xxxi) Training Reports and Certifications for Enrolment Offices **Field Infrastructure and Enrolment Centre** xxii) Plan for deployment, testing and commissioning of enrolment kits xxiii) Commissioning Report and deployment of enrolment software on registration kits xxiv) Onboarding of enrolment operators xxv) Operational internet for mobile registration centres **Network Connectivity** xxvi) Supply and Provisioning of connectivity from Data Centres (DC & DR) to NOC, SOC, Contact Centre, Technical Helpdesk xvii) Supply and Provisioning of internet connectivity links in Data Centres (DC & DR) **Contact Centre and Technical Helpdesk** viii) Setup of Technical Helpdesk xxix) Deployment of approved software (CRM, Helpdesk, etc.) (xl) Preparation of documents i.e., SOPs, FAQs, etc. (xli) Deployment of manpower and certificate of their training

No	Milestone	Output
		Network Operations Centre (NOC) and Security Operations Centre (SOC) (xlii) Setup of NOC and SOC xliii) Design of operations model including detailed technical design xliv) Undertake integration of tools and architecture and prepare a process for reporting requirement (xlv) Deployment of manpower and certificate of their training xlvi) Switch-over Strategy xlvii) Emergency response procedures
7.	**User Acceptance and Go-Live (Iteration_1)**	**Acceptance Testing** (i) Confirmation of readiness of system (ii) Formal submission of final versions of system (incl. ABIS/SDK) to be tested for Acceptance Testing and confirmation about the same. (iii) Creation of Acceptance Testing environment, as per required specifications (iv) Integration of test suite with ABIS/SDK (v) Development of logging tools for passive tests within the production environment (vi) Generate artificial test data, if necessary (vii) Acceptance of sample data (viii) Participate and monitor the conduct of tests and review of test logs provided after the tests (ix) Investigate all errors discovered in system results to determine accuracy of test data (x) Performing analysis of test logs and suggestions of re-test (xi) Making necessary changes in the system as per the ICTA observations (xii) Repeat the relevant activities for re-test 124. **Final Acceptance** (i) Deployment of the differential bill of material as per the gap (ii) Acceptance plan (iii) Acceptance test cases and scenarios (iv) Acceptance Test Plan (v) Acceptance Test Schedule (vi) Acceptance Test Environment Inventory (vii) Acceptance Test Summary Report (viii) Acceptance Test Final Report

No	Milestone	Output
8.	**Operational Acceptance (Iteration_1)**	(i) OAT Acceptance Plan (ii) OAT Acceptance Report
9.	**Detailed Design (Iteration_2)**	(i) Updated Functional Requirement Specifications (FRS) (ii) Updated Use Case Design Document (UDD) (iii) Updated Software Requirement Specification (SRS) (iv) 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. (v) Updated Low Level design document, with detailed algorithms and logic of the important API's stored procedures etc. (vi) 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) (vii) Updated UI/UX Style Guide (viii) Updated Traceability matrices with updated design features against the requirements
10.	**Second Software Release (Iteration_2 components)**	**Software** (i) Enhancements in components in Iteration_1 as per the enhancement identified during pilot (ii) Release and deployment on relevant environments (including production environment) (iii) Source code of the applications with version control mechanism in the source code repository (iv) Secure source code review (v) Integration of remaining COTs Solutions (vi) Optimize the authentication by among others adjusting biometric authentication parameters / quality scores using existing data. (vii) Biometric tests, Benchmarking and Acceptance **System Documentation** (i) Updated design documents (FRS, SRS, UDD, etc.) if any

No	Milestone	Output
		(ii) 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. (iii) Documents revised after previous milestones (iv) Design of fraud management process **Audits** (i) Carryout a Complete software audit for the Iteration 2 release and ensure the Iteration 2 is complaint. (ii) Carryout an Information Security audit for the complete end-to-end Iteration 2 release, including infrastructure, platform, etc. ensure the Iteration 2 is complaint. (iii) Facilitate the third-party independent Information Security audit carried out by ICTA ensure the Iteration 2 is complaint. **Training** (i) Updated Training Plan (ii) Updated Training Material, Training Manual, Training Content, Conduct of Trainings, and Satisfactory assessment reports for Trainings (iii) Approved updated online tutorials, videos, presentations loaded on KMS **Technical Helpdesk, NOC, SOC** **(i)** Deployment of additional manpower and certificate of their training as required
11.	**User Acceptance and Go-Live (Iteration_2)**	**Acceptance Testing** (i) Confirmation of readiness of system (ii) Acceptance of remaining COTS Solutions. (iii) Creation of Acceptance Testing environment, as per required specifications (iv) Development of logging tools for passive tests within the production environment (v) Generate artificial test data, if necessary (vi) Acceptance of sample data (vii) Participate and monitor the conduct of tests and review of test logs provided after the tests

No	Milestone	Output
		(viii) Investigate all errors discovered in system results to determine accuracy of test data (ix) Performing analysis of test logs and suggestions of re-test (x) Making necessary changes in the system as per the ICTA observations **Final Acceptance** (i) Deployment of the differential bill of material as per the gap (ii) Acceptance plan (iii) Acceptance test cases and scenarios (iv) Acceptance Test Plan (v) Acceptance Test Schedule (vi) Acceptance Test Environment Inventory (vii) Acceptance Test Summary Report (viii) Acceptance Test Final Report
12.	**Operational Acceptance (Iteration_2)**	(i) OAT Acceptance Plan (ii) OAT Acceptance Report
14.	**Operations and Maintenance** **(After Iteration 1 GO Live)**	**General** (i) Reports as per scope of work (ii) Methodology and Plan for undertaking a preventive maintenance (PM) (iii) Monthly Support and Maintenance Report (iv) Relevant documentation updates as required (v) Report on proof of renewal of OEM support for all IT infrastructure i.e., hardware, software, etc. (vi) Comprehensive reports on enrolment and authentication services on a daily, weekly, and progressive basis (vii) Daily and weekly tracker of issues logged and rectification measures **Project Management** (i) Project Management Weekly status review reports (ii) ABIS and Data Quality Report (iii) Incident Management Report (iv) SLA monitoring report **Enhancement and Maintenance of SL-UDI Software System including MOSIP Components**

No	Milestone	Output
		(i) Continuous update and modification of the technical manual to align it with the ICTA's and DRP's decision on releases on software system. (ii) Monthly Issue Log for the errors and bugs identified and changes implemented in the solution (iii) Recommendations for improvement of enrolment software, ABIS, quality checks, manual de-duplication, and fraud management functions (iv) Patch Release Management Process **Data Centres** (i) Data Centres Hosting Infrastructure (ii) Policies for management of Primary Data Centre and Disaster Recovery, backup and archival policy, and updated security policy (iii) Continuous performance tuning, storage , network ,virtualization , container platform performance benchmarking (iv) Path management (v) Monthly Issue Log for the errors and bugs identified and changes implemented in the solution (vi) Configuration manual for OS, appliances, middleware etc. **IT Helpdesk** (i) Periodic Root Cause Analysis report **Business and Technical Services** (i) Forecast of demand of required assets (ii) Asset management report containing assessment of required inventory, gaps and forecast of required asset (iii) Report on renewal of support for all IT infrastructure products and other system software's taken from OEMs (iv) Process for change and configuration management (v) Storage management policy (vi) Database administration guidelines (vii) Backup and archival policy (viii) Configuration manual for all software (ix) Schedule of infrastructure augmentation requirements (x) Detailed security architecture for the authentication services (xi) IP Address Management Plan

No	Milestone	Output
		Partner Management (i) One-time creation, validation, update, and modification of technical manual for on boarding of enrolment officer. (ii) Report on enrolments (centre-wise, enrolment officer-wise reports, etc.) and on data quality (iii) Report on authentications **Operations and Continuous Improvements** (i) Undertake necessary operations and coordination **(ii)** Identification and rectification of issues on continuous basis (iii) Assessment reports (iv) Logging of enhancements in hardware, software, security, network, etc **Information Security and Business Continuity** **(i)** 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 o) Exception management review p) Internal security audit including vulnerability assessment and penetration testing. q) Risk assessment methodology design / review **(ii)** 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

No	Milestone	Output
		d) Privacy gap assessment and privacy impact assessment e) Privacy inventory **(iii)** Annual f) Periodic secure source code review report **(iv)** Half-Yearly Basis g) Periodic application security testing report h) Phishing simulation exercise report **(v)** Quarterly Basis i) Incident management review j) Data Leakage Prevention (DLP) and End Point Detection Response (EDR) review k) Periodic vulnerability assessment and penetration testing report l) Review and enhancement of existing fraud rules **(vi)** Monthly m) Comprehensive compliance dashboard (Monthly workshop / presentation to ICTA stakeholders every month with the updated tracker and dashboard) **(vii)** Other frequencies n) Report on training and awareness (First time within 3 months of Go-live. Report on yearly basis subsequently) o) Security solution review and improvement report (First time 12 months after Go-live, and post this annually)
15.	**Transition and Exit Management**	(i) Transition and Exit Management plan (ii) AMC support related documents, credentials for all OEM Products (iii) Inventory Details (iv) Knowledge Management (v) Up-to-date source code (vi) Up-to-date documentations (vii) Final S&M report should consist of comprehensive knowledge transfer documentation.

Table 35 : Implementation Milestones

Note: This is a indicative list of deliverable the vender is expected to provide and deliver the entire SL-UDI solution.

7. Bill of Material

An indicative Bill of Material is given below. The MSI is expected to submit the complete Bill of material as per the requirements in Vol 1 during proposal submission.

(i) The devices mentioned in the tender is just indicative, the bidder is expect to provide the require no of devices , hardware based during the requirement analysis Phase.

(ii) The final decision for the device quantities and the required ancillary systems will be taken only after the SRS stage".

(iii) 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 components with no additional cost to the ICTA.

Serial Number	**Product and /or Service Item Description**	**Units**	**QTY**
Software			
1.	Modular Open Source Identity Platform (MOSIP)	Items	
2.	Integration Middleware	Items	
3.	Biometric SDK	Items	
4.	Automated Biometric Identification System	Items	
5.	Portal Solution	Items	
6.	Customer Relationship Management	Items	
7.	BI & Reporting Solution	Items	
8.	Document Management System	Items	
9.	Fraud Management System	Items	
10.	Service Billing System	Items	
11.	Knowledge Management System	Items	

12.	Learning Management System	Items	
13.	TSP and UA Software	Items	
14.	Enterprise Service Bus	Items	
15.	API Gateway	Items	
16.	Business Rules Engine	Items	
17.	Business Process Management Suite	Items	
18.	Web Server	Items	
19.	Distributed Caching	Items	
20.	Program / Project Management Tool	Items	
21.	Version management	Items	
22.	Operating System	Items	
23.	Database Solution	Items	
24.	Performance Testing Tool	Items	
25.	Messaging Platform - Publish/Subscribe Queues	Items	
26.	IT Service Management Tools	Items	
27.	Enterprise Management System	Items	
Data Center(Co-Locations)			
28.	Data Centre Hosting Space (Primary Site)	Items	
29.	Data Centre Hosting Space (Secondary Site)	Items	
30.	Data Centre Power (Primary Site)	Items	
31.	Data Centre Power (Secondary Site-DR))	Items	

IT Infrastructure			
32.	Blade Servers (Biometric Solution)	Items	
33.	Blade Chassis (Biometric Solution)	Items	
34.	Rack Server (Biometric Solution)	Items	
35.	Server Rack (Biometric Solution)	Items	
36.	SAN (Biometric Solution)	Items	
37.	SAN Switch (Biometric Solution)	Items	
38.	Tape Library and Tapes (Biometric Solution)	Items	
39.	Blade Servers (Other than Biometric Solution)	Items	
40.	Blade Chassis (Other than Biometric Solution)	Items	
41.	Rack Server (Other than Biometric Solution)	Items	
42.	Server Rack (Other than Biometric Solution)	Items	
43.	SAN (Other than Biometric Solution)	Items	
44.	SAN Switch (Other than Biometric Solution)	Items	
45.	Tape Library (Other than Biometric Solution)	Items	
46.	Virtual Tape Library (Other than Biometric Solution)	Items	
47.	Internet Router (For entire infrastructure)	Items	
48.	MPLS Router (For entire infrastructure)	Items	
49.	Global Load Balancer (For entire infrastructure)	Items	
50.	Application Load Controller - Server / Application Load Balancer (For entire infrastructure)	Items	

51.	Core Switches (For entire infrastructure)	Items	
52.	Data Centre Access Switches (For entire infrastructure)	Items	
53.	Enterprise Management System	Items	
54.	Replication and Backup Solution *(Note: MSI and BSP may bring same solution or their separate solutions)*	Items	
		Items	
55.	Network Access Controller	Items	
56.	Virtualization Solution	Items	
57.	Enterprise Container Application Platform	Items	
58.	Enterprise Monitoring System	Items	
59.	Virtual Desktop Infrastructure Solution	Items	
NOC / SOC			
60.	Video wall with controllers, speakers, and other accessories	Items	
61.	LED TV- (4 X 4 configuration)	Items	
62.	Laptop (for manager and L1 analysts)	Items	
63.	Desktops / Monitors (13 resources X 2 monitors each)	Items	
64.	Keyboards and Mouse	Items	
65.	IP Phone	Items	
66.	IP PABX	Items	
67.	Printer (Network)	Items	
68.	UPS – 20KVA	Items	

Field Infrastructure			
69.	Enrolment Fingerprint Scanner (4-4-2)	1625	
70.	Enrolment Iris Scanner (Dual)	1625	
71.	Signature Pad	1625	
72.	Auth- Fingerprint scanners	250	
73.	Auth - Facial Scanner	250	
74.	Auth - Iris Capture Device	250	
Mobile Registration KITS			
75.	Enrolment Kit Container for mobile registration kits	40	
76.	Laptop for mobile registration kits	40	
77.	QR Reader (Scan PRN included QR)	40	
78.	Document Scanner	40	
79.	Printer	40	
80.	Enrolment - Fingerprint Scanner (4-4-2)	40	
81.	Enrolment - Iris Scanner (Dual)	40	
82.	Web Camera	40	
83.	Signature Pad	40	
84.	UPS	40	
85.	USB Hub	Items	
86.	Internet Dongle	Items	
87.	USB Storage Device for mobile registration kits	Items	

88.	Flash Light	Items	
89.	Background Screen	Items	
Network Connectivity			
90.	Data Centre – Interconnection Network	Items	
91.	Data Centres (DC & DR) – Internet Links	Items	
92.	Internet Connectivity for mobile registration centres	Items	
93.	Data Centres (DC & DR) – NOC / SOC/ Technical Helpdesk	Items	
Security			
94.	DLP Solution	Items	
95.	Network Vulnerability Scanner	Items	
96.	Anti-Advanced Persistent Threat (APT)	Items	
97.	Privilege Access Management	Items	
98.	Two Factor Authentication	Items	
99.	Web Gateway with content Filtering & Proxy Solution	Items	
100.	Web Vulnerability Scanner	Items	
101.	Code Review Tool	Items	
102.	Anti-Virus Solution	Items	
103.	Identity and Access Management	Items	
104.	Hardware Security Module	Items	
105.	Security Information and Event Monitoring (SIEM) Solution	Items	
106.	Anti-DDoS solution	Items	

Security Component (Hardware)			
107.	Patch Management Solution	Items	
108.	Email Gateway (Security Solution)	Items	
109.	Database Activity Monitoring	Items	
110.	SSL VPN	Items	
111.	External Firewall	Items	
112.	Internal Firewall	Items	
113.	Web Application Firewall	Items	
114.	Host Intrusion Prevention System	Items	
115.	Network Intrusion Prevention System (NIPS) and NIDS	Items	
116.	Intrusion Detection System / Intrusion Prevention System	Items	
117.	Security Racks (same as other racks)	Items	
118.	Security Testing Solution	Items	
119.	Network Detection and Response	Items	
120.	Container Runtime Security and East west Traffic Inspection and Attack Mitigation Solution	Items	
121.	Extended Detection and Response Solution	Items	
Other Tools			
122.	Specify if any	Items	

Table 36 : Bill of Martial

8. Change Request

Given below are details on Change Request Process at a very high-level based on the Change Management policy.

No	Deliverables	Phase	Duration
1.	1.1 CR proposal including effort.	Estimation	-
2.	2.1 Proper maintenance of source code in GIT 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 2.1 User manuals (if applicable) 2.2 Administrator manuals (if applicable)	Implementation	Agreed duration for the CR

Table 37 : Change Request

8.1 Review Committees and Review Procedures

The MSI is required to work closely with the ICTA Technology Team and the Software Process Audit (SPAMSI should have updated/completed all the deliverables and testing tasks prior to submission for SPA audit. MSI should submit all the deliverables requested on above Section 4 to the SPA team and SPA will review all the deliverables and verify the application based on Functional and Non-functional aspects prior to acceptance. Any bugs, not adhering to best practices or failed to meet quality standards will directly cause to rejection of the versions.. All versions of deliverables will be reviewed and accepted by the team appointed by ICTA.

9. Compliance to Schedule of Requirements

The supplier shall provide the consent for the Schedule of requirements as described in Volume 2.

S.No	Schedule of Requirement	Description	Compliance (Y/N]	Remarks

1	Volume 2 - Schedule of Requirements	Scope of Work		
2	Annex 1- High Level Process Flow	DRP Process Flow		
3	Annex 2 - Non-Functional Requirements	System Non-Functional Requirements		
4	Annex 3 - Min Tech Specification	Technical Specifications		
5	Annex 4 - Software Engineering	Software Engineering Practices		
6	Annex 5 - Demand Capacity	Demand Capacity for Enrollment		
7	Annex 6 - Transition and Exit Management	Transition and Exit Management		
8	Annex 7 - Project Management and Governance	Project Management Procedures		
9	Annex 8 - Biometric Device Certification	Device Certification Process		
10	Annex 9- Service Level	Description of Service levels		
11	Annex 10 - Manpower Requirement	Manpower for the Project		
12	Annex 11: Overview of Technology	Technology Functional Specifications		
13	Annex 12: Project sites / sites	Project Enrollment Sites and Other Sites		

Table 38 : 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.

10. Services Offered by the Supplier

Given Below are the services offered by the supplier.

#	Solution Component	Provider
Enrolment Centers		
01	Locations, Civil and Electrical works (UPS, DG etc..)	DRP
02	WAN connectivity at field offices (Registration Centers)	DRP
03	Web Camera	DRP
04	Desktop PC and other components	DRP
05	Dual Displays	DRP
06	Document Scanner	DRP
07	Printer	DRP
08	Multi-Functional Printers (Fax)	DRP
09	IP Phones	DRP
10	Power Extension	DRP
11	QR Reader (Scan PRN included QR)	DRP
12	USB Hubs	DRP
13	Flashlights	DRP
14	Background Screens	DRP
General		
15	Card Storing Location	DRP
16	Indexing System	DRP
17	IC Inquiry System	DRP
18	Transliteration System	DRP
19	Manpower for cover overall Registration Process	DRP
20	Polycarbonate pre-printed blank card	DRP
21	Card personalization System	DRP
22	Card Management System	DRP
23	ICAO Photo Capturing System (e-Studio)	DRP

24	Citizen Call Center , Equipment and connections(Including toll free numbers)	DRP
25	Training Locations and equipment	DRP/ ICTA
26	Fireproof cabinet for backup store	DRP
27	SMS Gateway	ICTA
28	IPG	DRP
NOC/SOC IT Help desk		
29	Location, Civil and Electrical works	ICTA
30	LAN and Physical Access Control	ICTA
Policies and Procedures		
31	RACI Matrix	ICTA
32	Access Control Policy and Procedure	ICTA
33	Business Continuity Management Plan	ICTA
34	Capacity Management Policy and Procedure	ICTA
35	Change Management Policy and Procedure	ICTA
36	Development and Maintenance Policy and Procedure	ICTA
37	Dispute Resolution Policy and Procedure	ICTA
38	Governance Policy	ICTA
39	Incident Management Policy and Procedure	ICTA
40	Information Backup Management Policy and Procedure	ICTA
41	Information Security Policy and Procedure	ICTA
42	Release Management Policy and Procedure	ICTA
43	Log Management Policy and Procedure	ICTA
44	Patch Management Policy and Procedure	ICTA
45	Service Level Management Procedure	ICTA
46	Stakeholder onboarding Policy and Procedure	ICTA
47	Vulnerability Management Policy and Procedure	ICTA
48	Risk Management Policy & Plan	ICTA

Table 39 : Services offered by the employer.