NATIONAL INSTITUTE FOR SMART GOVERNMENT ON BEHALF OF

THE GOVERNMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

Ministry of Digital Economy

BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS

Volume 02 of 03 - Annexure 9: Service Levels

Two Stage Bidding Procedure

FOR THE

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

INVITATION FOR BIDS No: NISG/SLUDI-2025

June, 2025
Amended: January, 2026

Table of Contents

9.1 Introduction for the SLA....3
9.1.1 Objectives of Service Level Agreements....3
9.1.2 Service Level Consideration....3
9.1.3 Service Level Monitoring....4
9.1.4 Management of Service Levels....4
9.1.5 SLA Change Control....5
9.1.6 Service Levels Categories....6
9.1.7 Performance and Liquidated Damages....7
9.2 Service Levels for Implementation Services....9
9.3 Service Levels for Manpower....11
9.4 Service Levels for Biometric Registration Kits....11
9.5 Service Levels for Biometric Solution....13
9.6 Service Levels for Application and Software Services....16
9.7 Service Levels for Infrastructure....19
9.8 Service Levels for Business and Technical Services....21
9.9 Service Levels for Security Services....25
9.9.1 Documentation SLAs....25
9.9.2 Security Operations SLAs....26
9.9.3 Business Continuity Management....33

9.1 Introduction for the SLA

The aim of this agreement is to provide a basis for close co-operation between the Employer and the Master System Integrator (MSI) for support and maintenance services to be provided by the MSI, thereby ensuring a timely and efficient support service is available.

This agreement is contingent upon each party knowing and fulfilling their responsibilities and generating an environment conducive to the achievement and maintenance of targeted service levels.

This section details the expected service levels for the services to be provided by the MSI. MSI service performance shall be measured against the Service Levels detailed in this section. MSI will be responsible for complying with the listed Service Levels throughout the duration of the contract.

9.1.1 Objectives of Service Level Agreements

1. Provide clear reference to service ownership, accountability, roles and/or responsibilities
2. Present a clear, concise and measurable description of service provisioning at each level
3. Match perceptions of expected service provisioning with actual service support and delivery.
4. To create an environment conducive to a co-operative relationship between Employer, MSI and Employer's representatives (government organizations) to ensure the effective support of all end users.
5. To document the responsibilities of all parties taking part in the Agreement.
6. To define the commencement of the agreement, its initial term, and the provision for reviews.
7. To define in detail the service to be delivered by each party and the level of service expected, thereby reducing the risk of misunderstandings.
8. To institute a formal system of objective service level monitoring, ensuring that reviews of the agreement are based on factual data.
9. To provide a common understanding of service requirements/capabilities and the principle involved in the measurement of service levels.
10. To provide for all parties to the Service Level Agreement a single, easily referenced document which caters for all objectives as listed above.

9.1.2 Service Level Consideration

This section details the considerations that have been adopted in preparing the Service Levels:

i. A uniform approach to interpreting Service Levels has been adopted and it will be based on coherent reading of Service Levels in-line with the Scope of Work stipulated in the RFP document.

ii. The Service Levels, with MSI, defined for implementation activities are applicable from the date of signing of contract, or effective date of the contract, whichever is earlier,

iii. *The Service Levels defined for Operations are applicable after three months from the date of Go-Live.*

iv. Changes in the Service Levels may be discussed as per Service Levels change control mechanism (refer 9.1.5 SLA Change Control)

v. MSI would be responsible for the overall Service Levels for delivery of all components and

services as per the requirement of the project as specified in Volume 2.

vi. Any change in the team of the MSI during implementation activities and operations activities will be governed by the Service Levels associated with Team Deployment category as detailed in the service levels.

vii. Metrics of all the Service Levels are within MSI's control and are easily measurable.

viii. From the date of Go-Live of the project, the MSI shall deploy automated and transparent tools for the measurement and reporting of Service Levels. The MSI will be responsible for customizing, deploying and maintenance of tool, however SL-UDI will have the control of the tool for measuring the Service Levels through different reports

9.1.3 Service Level Monitoring

The success of Service Level Agreements (SLA) depends fundamentally on the ability to measure performance comprehensively and accurately so that credible and reliable information can be provided to customers and support areas on the service provided.

For transparent and accurate monitoring of service levels, it is important that the information capture is automated as far as possible. Thus, the MSI will be responsible to identify (with detailed justifications) service levels for which information cannot be collected in an automated manner and obtain the sign-off on such a list of service levels. For service levels identified for automated data collection, the MSI will be responsible for configuring the SLA tool in such a manner that the accurate information to monitor service levels is captured in an automated fashion. Wherever such automated capture of information is not feasible, the MSI shall provision an approval workflow within the SLA tool. The MSI will be responsible to publishing SLA reports.

Service factors must be meaningful, measurable, and monitored constantly. Actual levels of service are to be compared with agreed target levels on a regular basis by both GoSL and MSI. In the event of a discrepancy between actual and targeted service levels the MSI is expected to identify and resolve the reason(s) for any discrepancies.

Service level monitoring will be performed by GoSL or nominated partner where necessary reports and monitoring dashboards should be provided by the MSI. The reports will be produced as and when required and forwarded to the GoSL.

(i) Support monitoring of all SLAs defined in the RFP.

(ii) Support definition of thresholds of multiple levels for each SLA.

(iii) Show SLA violations by application, services, infrastructure.

(iv) The dashboard should be customizable to show the required SLAs.

9.1.4 Management of Service Levels

i. Responsibility of MSI: MSI is responsible for delivering the services described in the Schedule of Requirement in this RFP, as per the Service Levels and performance measures stipulated in this section. MSI is also responsible for:

a) Periodic Reporting of Service Levels as per Reporting Procedure mentioned below.

b) Reporting of risks and issues with mitigation strategies to the GoSL as per procedure mentioned below.

c) Immediate action to mitigate the identified risks and issues.

ii. Reporting Procedure

a) Service Levels reporting should be done using an automated tool. To the extent possible Service Levels reporting should be based on automated logs with minimal manual intervention. Well-defined processes should be implemented for those Service Levels that require manual intervention for measurement and reporting.

b) The Service Levels and performance measurement reports should be submitted in an agreed upon format.

c) The reports should include "actual versus target" Service Levels, a variance analysis and discussion of appropriate issues or significant events.

iii. Procedure for Mitigation of Issues

a) A pre-defined exception handling process will be used for situations where issues are not resolved at project team level.

b) GoSL or MSI may raise an issue by documenting the business or technical problem, providing an objective summary of the issue under consideration.

c) GoSL shall determine which project committee or executive level should logically be involved in resolution.

d) A meeting shall be conducted to resolve the issue in a timely manner.

e) Thereafter, Management of GoSL and MSI will examine the report of the project committee and agree on a temporary or permanent solution for the issue under consideration. The MSI will then communicate the resolution to all concerned teams.

9.1.5 SLA Change Control

i. It is understood that the Service Levels may be required to undergo amendments with evolution of GoSL's business needs during the course of the contract period. GoSL or the MSI can request a change in Service Levels. This section defines the following procedures required for amending the Service Levels and bring new Service Levels into effect:

a) SLA Change Process

b) Service Levels for a New Service, Optional Service or Additional Services

c) SLA Version Control

ii. SLA Change Process: The parties may amend the Service Levels by mutual agreement in accordance with the process described below:

a) Either party can review the Service Levels and initiate amendment requests. After the joint review of change requirements, the discussion on changes of Service Levels shall be taken up in monthly review meetings or technical committee meetings. Following actions might result out of discussion:

- Add to, delete or change the Services to be measured and the corresponding Service Levels to reflect changes in SL-UDI operations; and
- Improve the existing Service Levels, where warranted, to reflect operational or technical improvements.

b) With respect to a New Service, MSI and GoSL will establish initial Service Levels following full implementation of such Services which will come into effect within the initial 90-day period of MSI providing such New Service. To the extent appropriate, such initial Service Levels will be the same as or similar to existing Service Levels for the same or similar Services. During these 90 days, MSI and GoSL will conduct a process for Measurement and Validation of Service Levels to validate the initial Service Levels and agree upon the final Service Levels. The finalized service levels shall be documented and implemented in accordance with the Service Levels version control process described below.

c) All negotiated and agreed Service Level changes will require changing the version control number of the Service Level Agreement. Service Levels shall be documented for all new services, optional services and additional services following the completion of measurement and validation process for such services.

9.1.6 Service Levels Categories

The Service Levels have been grouped in the following categories:

(i) Service Levels for Implementation Services

(ii) Service Levels for Manpower

(iii) Service Level for Biometric Registration Kits

(iv) Service Level for Biometric Solution

(v) Service Levels for Application and Software

(vi) Service Level for Infrastructure

(vii) Service Levels for Business and Technical Services

(viii) Service Levels for Project Management Services

(ix) Service Levels for Security Services

**Note: For the components that are mentioned in the RFP to be transferred to MSP from the start of the 2nd support year will be excluded from the MSI's SLA commitment.*

Below are definitions specific to the SLA.

(i) **"Enrolment Transactions"** The transaction related to the successful de-duplication check to establish if there exist any duplicate(s) for one subject to be enrolled.

(ii) **"False Positive Identification"** A term applying to de-duplication transactions only. An incorrect decision of a biometric system that an applicant for a UID has previously been enrolled in the system, when in fact they have not.

(iii) **"False Positive Identification Rate (FPIR)"** A term applying to de-duplication transactions only. The ratio of the number of false positive identification decisions to the total number of enrolment transactions by unenrolled individuals. This rate is expected to depend upon the size of the enrolled database and the database binning/partitioning used.

(iv) **"False Negative Identification"** A term applying to de-duplication transactions only. An incorrect decision of a biometric system that an applicant for a UID, making no attempt to avoid recognition, has not previously been enrolled in the system, when in fact they have. This failure to match might be caused by any algorithm in use by the system (segmentation, comparison, binning, quality, etc.).

(v) **"False Negative Identification Rate (FNIR)"** A term applying to de-duplication transactions only. The ratio of number of false negative identification decisions to the total number of enrolment transactions by enrolled individuals. This rate is expected to depend upon the database binning/partitioning used to meet throughput requirements.

(vi) As no failure-to-enroll decisions will be permitted for residents with any of the 12 biometrics available, failure-to-enroll rates are presumed to be zero and will not be considered in computing the false negative identification rate. Data from residents with none of the 12 biometrics will be exempted from the calculation of this rate.

(vii) **"False Acceptance"** A term applying to authentication transactions only. The decision of a biometric system that submitted biometric samples match enrolment data from a different data subject.

(viii) **"**False **Match Rate (FMR)"** A term applying to authentication transactions only. The ratio of number of verification transactions conducted by data subjects resulting in a false match to the total number of transactions. The definition of "transaction" shall be given by the respondent, with the provision that the same definition is used in determining "False Match Rate."

(ix) **"False Rejection"** A term applying to authentication transactions only. The decision of a biometric system that submitted biometric samples do not match enrolment data of the same data subject.

(x) **"False Non-Match Rate (FNMR)"** A term applying to authentication transactions only. The ratio of number of authentication transactions conducted by data subjects resulting in a false non match to the total number of transactions. The definition of "transaction" shall be given by the respondent, with the provision that the same definition is used in determining "False Non-Match Rate."

(xi) **"Successful De-Duplication"** means assurance through biometric comparisons that no enrolled person has been assigned more than one Unique Identity Number.

(xii) **"Enrolment Transactions"** mean the transaction to perform de-duplication check in order to establish if there exists any duplicate(s) for the subject to be enrolled.

(xiii) **"Allotted Enrolment Transactions"** mean the transaction allocated to a Biometric Solution to perform de-duplication in order to check if there exist any duplicate(s) for the subject being enrolled.

(xiv) **"Total Cost"** refers to the "Contract Value" defined in Payment Schedule in Volume- 1(section 4.13).

(xv) "**Quarterly Revenue (QR)**" refers to Quarterly Amount Payable (definition given in Payment Schedule of Volume-3)

9.1.7 Performance and Liquidated Damages

This section details the Performance and Liquidated Damages applicable on MSI, as a result of not complying with the Service Levels as stipulated in this RFP.

i. A quarterly performance evaluation will be undertaken using the monthly reporting periods of that respective quarter.

ii. Where SLA measurement is done on a monthly basis, sum of Liquidated Damages associated shall apply for the month.

iii. Performance Liquidated Damages shall be levied for not meeting each SLA.

iv. Based on the non-performance and its business impact, GoSL shall invoke the severity level as defined below:

Severity Level for non- compliance	Liquidated Damages as a percentage of total contract value (for the measured month)
9	1.50% and GoSL may decide to issue Notice of Termination to MSI
8	1.25%
7	1.00%
6	0.50%
5	0.25%
4	0.125%
3	0.10%
2	0.05%
1	0.025%

Table 9.2: Performance and Liquidated Damages

v. For the implementation phase, the Cumulative Liquidated Damages for the Service Levels applicable in the Implementation Phase shall be capped to 10% of the Total Cost. In case the penalty exceeds 10% of the Total Cost, GoSL reserves the right to issue a notice of termination of contract to the MSI.

vi. For operations and maintenance phase, the Cumulative Liquidated Damages for each quarter, under no circumstances, shall exceed 10% of the fee payable for that quarter.

- If on Performance evaluation it is realized that liquated damages deducted for each of the 1 quarter is equal to 10% of the fee payable for that month, GoSL reserves the right to issue a notice of termination of contract to the MSI.

9.2 Service Levels for Implementation Services

i. The Implementation Services comprise of activities relating to the implementation work by MSI. Service Levels related to Operation Services are detailed in Section 9.6 Service Levels for Application and Software Services of this document. The Phase wise implementation plan/ implementation roadmap is detailed in the document

- Activation of Service Levels responsibility by MSI: The Service Levels specified in this section shall be activated from the date of signing of the contract.
- De-activation of Service Levels responsibility by MSI: These Service Levels shall be de-activated from the date all service level milestones under this category are achieved by the MSI.

#	Category/ Component	Metric Type	Formula / Definition	Period and Time of Measurement	Target	Severity level
1	Launch of Release_1 Components	Delay	Measured as the difference between the planned date for the milestone and the actual date of its completion in terms of delay in number of calendar days For details about preparedness, please refer to the *Note-B* at the end of this table.	Milestone based Measurement	Delay of <=30 days	0
					Delay >=30 days and <=45 days	5
					Delay >=45 days	9
2	Launch of Release_2 Components	Delay	Measured as the difference between the planned date for the milestone and the actual date of its completion in terms of delay in number of calendar days For details about preparedness, please refer to the *Note-B* at the end of this table.	Milestone based Measurement	Delay of <=30 days	0
					Delay >30 days and <=45 days	5
					Delay >45 days	9
3	SL-UDI System Go-Live	Delay	Measured as the difference between the planned date for the milestone and the actual date of its completion in terms of	Milestone based Measurement	Delay of <=30 days	0
					Delay >30 days	5

#	Category/ Component	Metric Type	Formula / Definition	Period and Time of Measurement	Target	Severity level
			delay in number of calendar days For details about preparedness, please refer to the *Note-B* at the end of this table.		and <=45 days	
					Delay >45 days	9

Table 9.3: Implementation Phase Service Levels

Note:

(A) The preparedness for the Launch of Release_1 would comprise of the following:

- **Hosting Infrastructure:** Supply, installation, configuration, integration and testing of all components and equipment as per the agreed bill of material, to the satisfaction of the GoSL
- **Software**: Supply of necessary licenses as per the agreed bill of material
- **Network Setup**: Installation, configuration, setup and testing of network for all locations (except network at the enrolment centers), to the satisfaction of the GoSL. The networks should be well-integrated with the network operation centers, to the satisfaction of the GOSL.
- **Security Components:** Supply, installation, configuration, integration and testing of all security components and equipment as per the agreed bill of material, to the satisfaction of the GoSL.
- **Field Infrastructure:** Supply, installation, configuration, integration and testing of all field infrastructure components and equipment as per agreed bill of material, to the satisfaction of the GoSL. This will include setup of the service center and availability of all the spares in the agreed location. This shall exclude the installation of the enrolment software and user training.
- **Enrolment Centre**: Readiness of the enrolment center in all aspects for which MSI is responsible.
- **Contact Centre and Helpdesk**: Establishment of the contact center and helpdesk, finalization of documentation (FAQs, SOPs, etc.), availability and training of manpower, etc.
- **SOC and NOC**: Establishment of SOC & NOC, integration with network and security components.
- **Project Management**: Finalization of all reporting formats, configuration of SLA reporting in the identified tool, and other information as

expected to be completed prior to launch.

(B) In addition to the Note-A, the Launch of Release_1 and Release_2 would comprise of the following:

- **Requirement Gathering**: Sign-off from GoSL for SRS document.
- **Design**: Sign-off of design as per the gathered requirements, from GoSL for all the design documents for common aspects (such as architectures) and specific components which are part of respective releases.
- **Development and Customization**: Completion of the development and customization of the components, as per sign-off design, which are part of respective releases
- **Installation:** Installation of the software in the data center environments including the production environment
- **Testing**: Completion of the testing such as integration testing, system testing, performance and load testing, security testing and user acceptance testing and sign-off from GoSL for aforementioned type of testing. This shall exclude the partial acceptance testing as well as benchmarking and final acceptance testing.
- **Improvements (applicable for Release_2 only)**: Incorporation of learnings from the Launch of Release_1 in the applicable areas of the project under purview of the MSI

9.3 Service Levels for Manpower

#	Category/ Component	Metric Type	Formula / Definition	Period and Time of Measurement	Target	Severity level
1	Team Deployment	Availability	Resources to be mobilized on-time as per the Staffing Schedule submitted as part of MSI's Technical Bid. This penalty will be calculated for each resource.	First time deployment of each resource, as per the Staffing Schedule	Delay of <=14 days	0
					Delay of > 14 days	INR 25000 per resource per week

Table 9.4: Service Levels for Manpower

9.4 Service Levels for Biometric Registration Kits

The GoSL (or their representatives) may make a complaint about the equipment/ service through letter, fax, e-mail, phone, SMS or any other means and updated on the respective issue management system, as the GoSL thinks fit or convenient to the Technical Helpdesk of MSI.

Note: The Category-1 locations would comprise of country capital and province headquarters, Category-2 would comprise of district locations, and remaining locations would form part of Category-3 locations.

S. No.	Item	Duration
1.	Telephonic Support (Diagnose the issue and resolve through telephonic support within 2 hours on receipt of the complaint)	Two hours
2.	Physical Visit	Next Two business day
3.	On receiving complaint about equipment/service, the MSI will respond and repair/replace or provide required services in Category-1 Locations	Two business days
4.	On receiving complaint about equipment/service, the MSI will respond and repair/replace or provide required services in Category-2 Locations	Four business days
5.	On receiving complaint about equipment/service, the MSI will respond and repair/replace or provide required services in Category-3 Locations	Five business days
6.	On receiving complaint about equipment/service, the MSI will respond and repair/replace or provide required services for mobile kits (anywhere in the country)	Five business days

Table 9.5: Service Levels for Biometric Registration Kits

Note: For replacements, MSI may use the spares required to be arranged by MSI under the project. These replacements should be of the same make and model which are part of the bill of material.

In case MSI fails to meet the above standards of maintenance, there will be per device per day penalty of 5% of the cost of the item. In case the equipment is not repaired/replaced even after one week after the stipulated timeline has passed, the penalty will be charged at 2 (twice) times of the aforementioned penalty.

9.5 Service Levels for Biometric Solution

The Following are the SLA principles adopted for Solution related performance levels

- The Performance targets for the Service Level Measurements during any period of assessment may not fixed for the entire contract period and may be revised for each period prior to the commencement of the period

#	Service Level	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Consequence / Severity in case of Penalty
1	False Positive Identification Rate (FPIR)	Quality	FPIR = (Number of false positive identification decisions in the day) / (total number of enrolment transactions b y unenrolled individuals in the day).	Monthly	<= 1% measured per month	0
					> 1% and <= 2% measured per month	7
					> 2% measured per month	8 Or 9 (if breach occurred for two consecutive cycles Penalty of severity)
2	False Negative Identification Rate (FNIR)	Quality	FNIR = (Number of false negative identification decisions in the day) / (total number of enrolments transactions by unenrolled individuals in the day).	Monthly	<= 1% measured per month	0
					> 1% and <= 2% measured per month	7
					> 2% measuredper month	8 Or 9 (if breach occurred for two consecutive cycles Penalty of severity)
3	False Match Rate (FMR)	Quality	FMR = (Number of biometric verification transactions in the day	Monthly	<= 0.01% for all levels of verification measured per month	0

#	Service Level	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Consequence / Severity in case of Penalty
			resulting in a false match) / (total number of biometric transactions).		> 0.01% and <= 0.1% for all levels of verification measured per month	6
					> 0.1% and <= 1% for all levels of verification measured per month	8
					> 1% for all levels of verification measured per month	9
4	False Non-Match Rate (FNMR)	Quality	FNMR = (Number of biometric verification transactions resulting in a false non match) / (total number of biometric transactions).	Monthly	<= 2% for all levels of verification measured per month	0
					> 2% and <= 3% for all levels of verification measured per month	6
					> 3% and <= 4% for all levels of verification measured per month	8
					> 4% for all levels of verification measured per month	9

#	Service Level	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Consequence / Severity in case of Penalty
5	Response Time per De-duplication check	Throughput	Response Time = Average elapsed time between submission of an enrolment request to Biometric Solution and generation of response (Success or failure of de-duplication)	Monthly	=< 24 hours	0
					>24 hours to <=28 hours	5
					>28 hours to <=32 hours	6
					>32 hours to <=36 hours	7
					>36 hours	8
6	Fine tuning of Biometric Solution	As per scope of work	For each instance when fine-tuning is not carried out by the bidder within the specified timeline	Monthly	Compliant	0
					Non-Compliance	8, or 9 (if breach occurred for two consecutive fine-tunings)

Table 9.7: Service Levels for Biometric Solution

9.6 Service Levels for Application and Software Services

#	Category / Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
1	Authentication Services	Availability	**Metric:** % of Uptime for Authentication Services **Formula:** Uptime % = {1- [(Total Downtime) / (Total Time)]} *100 For the purpose of this SLA, Authentication Services Components comprises of Data Centre and Associated Networks, Fraud Management System, Biometric SDK, Authentication Solution, Resident Data Store, Partner and Device Management Solution, Device management Server, Service Billing System, API Gateway, IDAM, and other components on which the authentication service is responsive and available to the end-users. **Total Time:** 24 hours x 30 days **Total Downtime:** Total cumulative time the Applications are NOT Available. ***Note:*** There is no planned downtime for this service.	Monthly	>= 99.95%	0
					< 99.95% and >=99.90%	3
					<99.90%	6
2	Enrolment Services	Availability	**Metric:** % of Uptime for Enrolment Services **Formula:** Uptime % = {1- [(Total Downtime) / (Total Time – Planned Downtime)]} *100	Monthly	>= 99.0%	0

#	Category / Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
			For the purpose of this SLA, Enrolment Services Components comprises of Data Centre and Associated Networks, Registration Processor, ID repository, ABIS, Biometric Middleware, Manual Adjudication, and other components on which the enrolment service is responsive and available to the process the enrolment packets. **Total Time:** 24 hours x 30 days **Total Downtime:** Total cumulative time the Applications are NOT Available. **Planned Downtime:** Total maintenance time as defined and agreed upon between MSI and GoSL		< 99.0% and >=98.5%	3
					<98.4%	6
3	External facing components (except those covered under Enrolment and Authentication Services)	Availability	**Metric:** % of Uptime for External Facing Components **Formula:** Uptime % = {1- [(Total Downtime) / (Total Time – Planned Downtime)]} *100 For the purpose of this SLA, External Facing Components comprises of Pre-Enrolment, Portals, Call Centre Services, Helpdesk Services, Partner and Device Management, Queue Management System, ITSM, etc. **Total Time:** 24 hours x 30 days **Total Downtime:** Total cumulative time the Applications are NOT Available. **Planned Downtime:** Total maintenance time as defined and agreed upon between MSI and GoSL.	Monthly	>= 99.5%	0
					< 99.50% and >=99.00%	3
					<99.00%	6

#	Category / Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
4	Internal facing components (critical components) (except those components which are covered under authentication services, enrolment services and external facing components)	Availability	**Metric:** % of Uptime for External Facing Components **Formula:** Uptime % = {1- [(Total Downtime) / (Total Time – Planned Downtime)]} *100 For the purpose of this SLA, Internal Facing (Critical Components) comprise of NOC, SOC, BI & Analytics, EMS, etc. **Total Time:** 24 hours x 30 days **Total Downtime:** Total cumulative time the Applications are NOT Available. **Planned Downtime:** Total maintenance time as defined and agreed upon between MSI and GoSL.	Monthly	>= 99.90%	0
					< 99.90% and >=99.5%	3
					<99.50%	6

Table 9.8: Service Levels for Application and Software Services

9.7 Service Levels for Infrastructure

#	Category / Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
1	Hosting Infrastructure	Availability	**Metric:** % of Uptime for Overall SL-UDI DS **Formula:** Uptime % = {1- [(Total Downtime) / (Total Time – Planned Downtime)]} *100 **Total Downtime** - Total cumulative time the hosting services are NOT Available. **Planned Downtime** -Total maintenance time as defined and agreed upon by MSI and GoSL.	• Available - 24 X 7, measured over a period of month. • Monthly Measurement	>= 99.95%	0
					< 99.95% & >= 99.50%	4
					< 99.50% & >= 99%	7
					<99%	8

Table 9.9: Service Levels for Infrastructure

The service support quality matrix provides the details of parameters on which the service support of the MSI shall be evaluated and measured. The service requests and tickets shall have graded priorities (From P1 to P4) based on the business impact and criticality of issue decided by GoSL nominated party.

Highly Critical	Critical	Less-Critical	Non- Critical
Total failure of hardware/network equipment - Virtual appliances/ Security device and Solutions/ Virtualization and container platforms affecting complete or partial down-time Any of the -Active hardware component, sub-component,	Total failure of hardware/network equipment, Virtual appliances / Security device and Solutions / Virtualization and container platforms but no down-time Any of the - Active hardware component, sub-component, - Passive hardware component	Partial failure of hardware / network equipment, Virtual appliances/ Security device and Solutions / Virtualization and container platforms no down-time Any of the - Active hardware component, sub-component,	Alert/ warning - Any critical alert or warning of any of the Active hardware component, sub-component, - Passive hardware component (ex. Patch cable), - Firmware, - Any related equipment

Highly Critical	Critical	Less-Critical	Non- Critical
- Passive hardware component (ex. Patch cable), - Firmware, - Any related equipment - Virtual appliances - Security device and Solutions - Virtualization and container platforms Deployed malfunctioning or failure, which leads to partial or complete outage.	(ex. Patch cable), - Firmware, - Any related equipment - Disk failure - Virtual appliances - Security device and Solutions - Virtualization and container platforms Deployed malfunctioning or partial failure, but no partial or complete outage or degraded performance (>5%). (Ex: total failure of redundant firewall or power supply)	- Passive hardware component (ex. Patch cable), - Firmware, - Any related equipment - Virtual appliances - Security device and Solutions - Virtualization and container platforms Deployed malfunctioning which leads to degraded performance (>5%).	- Virtual appliances - Security device and Solutions - Virtualization and container platforms Without any partial or total failure or degraded performance (>5%).

Table 9.10: Service Support Quality Matrix

#	Category / Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
1	Incident Response Time (P1)	Response Time	Average Time taken to acknowledge and respond once a ticket/incident is logged through calls, email or Ticketing System. This is calculated for all tickets/incidents reported within the reporting month. Target: 15 Minutes	Monthly	100% within the defined target	0
					>=99% and <100% meeting the target	1
					>=97% and <99% meeting the target	3

#	Category / Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
					>=95% and 97% meeting the target	5
2	Incident Response Time (P2)	Response Time	Average Time taken to acknowledge and respond once a ticket/incident is logged through calls, email or Ticketing System. This is calculated for all tickets/incidents reported within the reporting month. Target: 30 Minutes	Monthly	100% within the defined target	0
					>=99% and <100% meeting the target	1
					>=97% and <99% meeting the target	3
					>=95% and 97% meeting the target	5
3	Incident Response Time (P3)	Response Time	Average Time taken to acknowledge and respond once a ticket/incident is logged through calls, email or Ticketing System. This is calculated for all tickets/incidents reported within the reporting month. Target: 45 Minutes	Monthly	100% within the defined target	0
					>=99% and <100% meeting the target	1
					>=97% and <99% meeting the target	3
					>=95% and 97% meeting the target	5
4	Incident Response Time (P4)	Response Time	Average Time taken to acknowledge and respond once a ticket/incident is logged through calls, email or Ticketing System. This is calculated for all tickets/incidents reported within the reporting month. Target: 60 Minutes	Monthly	100% within the defined target	0
					>=99% and <100% meeting the target	1
					>=97% and <99% meeting the target	3
					>=95% and 97% meeting the target	5

Table 9.11: Incident Response Times

9.8 Service Levels for Business and Technical Services

The service support quality matrix provides the details of parameters on which the service support of the MSI shall be evaluated and measured. The service requests and tickets shall have graded priorities (From P1 to P5) based on the business impact and criticality of issue decided by GoSL.

While the service desk shall only be measured on response to incidents, other teams like incident management and problem management shall be measured on restoration of service and resolution of the issues.

				Priority (in hours)				
Service	**Request Type**	**Responsibility**	**Metric**	**P1**	**P2**	**P3**	**P4**	**P5**
Incident Management	Incident Resolution – Resolution of Issue (like security incidents, data theft, etc.) after incident was logged in the system	IT Help Desk	Resolution Time (In Hrs.)	0.50 (30 minutes)	2	24	48	96

Table 9.11: Service Levels for Business and Technical Services

#	Category / Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
1	IT Help Desk	Restoration Time	**Metric**: % of Priority-1 Tickets restored within 2 Hours **Formula**: Number of tickets responded within 2 hours / Total Number of Tickets raised in that Month	Monthly	>= 99%	0
					>= 98% to 99%	1
					>= 97% to 98%	2
					>= 95% to 97%	3
					>= 90% to 95%	4
					<90%	5
2	IT Help Desk	Restoration Time	**Metric**: % of Priority-2 Tickets restored within 24 Hours **Formula**: Number of tickets responded within 24 hours / Total Number of Tickets raised in that Month	Monthly	>= 99%	0
					>= 98% to 99%	1
					>= 97% to 98%	2

#	Category / Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
					>= 95% to 97%	3
					>= 90% to 95%	4
					<90%	5
3	IT Help Desk	Restoration Time	**Metric**: % of Priority-3 Tickets restored within 48 Hours **Formula**: Number of tickets responded within 48 hours / Total Number of Tickets raised in that Month	Monthly	>= 99%	0
					>= 98% to 99%	1
					>= 97% to 98%	2
					>= 95% to 97%	3
					>= 90% to 95%	4
					<90%	5
4	IT Help Desk	Restoration Time	**Metric**: % of Priority-4 Tickets restored within 96 Hours **Formula**: Number of tickets responded within 96 hours / Total Number of Tickets raised in that Month	Monthly	>= 99%	0
					>= 98% to 99%	1
					>= 97% to 98%	2
					>= 95% to 97%	3
					>= 90% to 95%	4
					<90%	5
5	IT Help Desk	Restoration Time	**Metric**: % of Priority-5 incidents resolved within 144 Hours **Formula**: Number of tickets responded within 144 hours / Total Number of Tickets raised in that Month	Monthly	>= 99%	0
					>= 98% to 99%	1
					>= 97% to 98%	2
					>= 95% to 97%	3

#	Category / Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
					>= 90% to 95%	4
					<90%	5

Table 9.12: SLA for IT Helpdesk

Note: (A) "Restoration Time" means time taken (after the trouble call has been logged on the helpdesk), in resolving (diagnosing, troubleshooting, and fixing) or escalating (to the second level to respective OEM, getting the confirmatory details about the same from the OEM and resolving the same). Provisioning of standby, if required, should be done along with associated data being restored, services reinitiated, and SLA conditions being met. Final Resolution shall be deemed to be complete only after the original equipment is replaced / reinitiated along with data being restored to the correct state and services are resumed.

Note: (B) Time taken (after the trouble call has been logged on the helpdesk), in resolving (diagnosing, troubleshooting and fixing) or escalating (to the second level to respective OEMs, getting the confirmatory details about the same from the OEM and resolving the same). Provisioning of standby, if required, should be done along with associated data being restored, services reinitiated, and SLA conditions being met. Final Resolution shall be deemed to be complete only after the original equipment is replaced / reinitiated along with data being restored to the correct state and services are resumed

#	Category / Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
1	Root cause analysis	Problem set management	Should perform an analysis on the alerts and incidents triggered in SL-UDI system to detect the root cause of the incidents and to fine-tune the configured rules. A detailed report including the action plan should be submitted to GoSL management for necessary actions. Root cause analysis shall be done for Priority 1 (P1) and Priority 2 (P2):	During operations and maintenance phase on a monthly basis	>=100%	0
					<100% and >=95%	1
					<95% and >=90%	2
					<90% and >=85%	3

#	Category / Component	Metric Type	Formula/Definition	Period and Time of Measurement	Target	Severity Level
			a. P1 – within 24 hrs. of actual resolution of the incident b. P2 – within 48 hrs. of actual resolution of the incident Priority of the incident will be decided after discussion with GoSL **Formula** RCA Completion percent = (Number of tickets on which RCA was completed within defined timelines / Number of tickets for which RCA was due as per assessment) * 100		<85	4

9.9 Service Levels for Security Services

9.9.1 Documentation SLAs

Note: T= effective date of Go-Live of SL-UDI System

#	Category / Component	Metric type	Formula/Definition	Period and Time of Measurement	Target	Severity Levels
1	SLA Measurement Methodology	Completion and Coverage	MSI shall prepare a measurement methodology for all the SLAs defined in the RFP. Under no circumstances MSI shall change the target or definition and shall only suggest method(s) to measure the SLAs.	One time	T+12 weeks	0
					Delay of <=2 weeks from target	1
					Delay of more than 2 weeks but <=4 weeks from target.	2
					More than 4 weeks delay from target.	3

#	Category / Component	Metric type	Formula/Definition	Period and Time of Measurement	Target	Severity Levels
2	Policy, procedure and hardening standards review / design	Completion and coverage	MSI should review, update, design or create (as applicable) all the security and privacy policies, standard operating procedures, hardening standards and workflows required for effective security of SL-UDI program as mentioned in the RFP. The list of all such documents should be decided in advance by MSI and approved by SL-UDI. All the documents should be submitted within the defined timelines. This activity should be performed for the first time within 3 months of Go-Live and then on an annual basis.	First time: 3 months after Go- live. Thereafter: Annually Finally, upon exiting the contract.	As per target	0
					Delay of <=1 month from target	1
					Delay of more than 1 month but <=2 months from target	2
					More than 2 months delay from target	3

Table 9.13: Documentation SLAs

9.9.2 Security Operations SLAs

#	*Category / Component*	*Metric type*	*Definition*	*Period and Time of Measurement*	*Target*	*Severity level*
1	Device integration with SIEM and custom parsers implementation	Event source coverage	All the new hardware and software that are being implemented in infrastructure should be integrated with Security Information & Event Management (SIEM) before Go-Live.	During operations and maintenance phase on a monthly basis	100% coverage	0
					<100 and >=98%	1
					<98 and >=95%	2

#	*Category / Component*	*Metric type*	*Definition*	*Period and Time of Measurement*	*Target*	*Severity level*
					<95%	3
					<90%	4
2	Alerts monitoring	Monitoring	All the alerts generated in SOC against any of the rules configured in SOC should be tracked and investigated. Alerts which are false positives shall be documented as false positives in the ticket for analysis purpose. Tickets shall be logged for all alerts triggered in SIEM solution.	During operations and maintenance phase on a monthly basis	100% of alerts should be logged as tickets	0
					<100 and >=98%	1
					<98 and >=95%	2
					<95 and >=90%	3
					<90%	4
3	Missed Security incident	Missed incident (per incident)	Missed security incidents are those security incidents for which alerts are not generated by SOC. There shall be no security incidents which are missed by SOC. Security incident for the purpose of this SLA means any malicious activity in SL-UDI infrastructure that could compromise the security even if has not been executed successfully. For e.g., if SQL injection attempts on applications are not detected by SOC even if	During operations and maintenance phase on a monthly basis	No incident	0
					Occurrence of an incident	5

#	*Category / Component*	*Metric type*	*Definition*	*Period and Time of Measurement*	*Target*	*Severity level*
			those did not result in data breach, these shall be considered as missed security incidents or if brute force attacks on password of external applications such as email are not detected, even if there is no compromise, these shall be considered as missed security incidents.			
4	Quality of tickets	Problem set management	Quality of tickets would mean appropriate classification, detailed notes in the ticket describing the incident, appropriate bucketisation, appropriate assignment, appropriate status etc. as per the security incident management policy and procedure. Formula – (Total score for all tickets audited / (100* number of samples selected for audit)) * 100 Random tests with reasonable sampling should be carried out. Checklist with scoring for each parameter shall be formulated for measurement. Score shall be measured from 1 to 100. MSI is expected to prepare a detailed plan for conducting the tests. MSI shall submit the plan to GoSL for approval and begin the exercise post approval.	During operations and maintenance phase on a monthly basis	>=90%	0
					<90% and >=80%	1
					<80% and >=70%	2
					<70% and >=60%	3
					<60%	4

#	*Category / Component*	*Metric type*	*Definition*	*Period and Time of Measurement*	*Target*	*Severity level*
5	Security incident response	Timely response	Definition: Response to security incidents shall be done in a timely manner: P1 incidents shall be responded within 15 minutes a. P2 incidents shall be responded within 30 minutes b. P3 incidents shall be responded within 45 minutes c. P4 incidents shall be responded within 60 minutes Formula: (Number of tickets opened during the period and for which response is provided within defined timelines / Number of total tickets opened during the period) * 100	During operations and maintenance phase on a monthly basis	>=95%	0
					<95% and >=90%	1
					<90% and >=80%	2
					<80% and >=70%	3
					<70%	4
6	Security incident resolution	Timely response	Definition: Resolution to security incidents shall be done in a timely manner: a. P1 incidents shall be resolved/closed within (1 day) b. P2 incidents shall be resolved/closed within 2 days c. P3 incidents shall be resolved/closed within 5 days d. P4 incidents shall be resolved/closed within 15 days	During operations and maintenance phase on a monthly basis	>=95%	0
					<95% and >=90%	1
					<90% and >=80%	2
					<80% and >=70%	3
					<70%	4

#	*Category / Component*	*Metric type*	*Definition*	*Period and Time of Measurement*	*Target*	*Severity level*
			Formula: (Number of tickets opened during the period and for which resolution is provided within defined timelines / Number of total tickets opened during the period) * 100			
7	Security and Privacy breach including Data Theft / Loss / Corruption / Mining	Completion	Any incident where-in a system is compromised, privacy breached, data is corrupted, data is mined or any case wherein data theft occurs (including internal incidents) impacts business operations in a major way. MSI shall provide a report on the breach including remediation measures taken to mitigate the security breach. The report shall be submitted within 5 working days to GoSL management.	Annually	No breach	0
					Any security or privacy breach. These penalties will not be part of overall SLA penalties cap. In case of serious breach of security wherein the data is stolen, mined, privacy breached or corrupted, GoSL reserves the right to terminate the contract or impose appropriate penalties.	8
8	Maintenance of Access control matrix	Accuracy of Access control matrix	Any access provisioning / deprovisioning / update should be reported within the defined timeline in the prescribed format as per the defined policies and procedures and updated in	During operations and maintenance phase on a	100%	0
					<100 and >=98%	1

#	*Category / Component*	*Metric type*	*Definition*	*Period and Time of Measurement*	*Target*	*Severity level*
			the access control matrix/access list. Access list should be updated on a regular basis (near real time). Random access reconciliations exercise with reasonable sampling will be carried out to check for the accuracy of the access list. MSI is expected to prepare a detailed plan for conducting the access reconciliation exercise. MSI shall submit the plan to GoSL for approval and begin the exercise post approval.	monthly basis	<98 and >=95%	2
					<95 and >=90%	3
					<90%	4
9	Inventory management	Accuracy of Inventory	Any asset provisioning / deprovisioning / update should be reported within the defined timeline in the prescribed format as per the defined policies and procedures and updated in asset list Random tests with reasonable sampling will be carried out to check for the accuracy of the inventory. MSI is expected to prepare a detailed plan for conducting these tests and submit the same to GoSL for approval and begin the tests post approval.	During operations and maintenance phase on a monthly basis	100%	0
					<100 and >=98%	1
					<98 and >=95%	2
					<95 and >=90%	3
					<90%	4
10	Web Application security testing	Frequency and	All web applications, APIs, shall undergo security testing before go-live (both during	First time: At Go-live.	100%	0

#	*Category / Component*	*Metric type*	*Definition*	*Period and Time of Measurement*	*Target*	*Severity level*
		coverage	implementation phase and operations and maintenance phase for new applications and APIs introduced in the ecosystem) and on a half yearly basis. MSI shall gather a list of applications, APIs etc. every half year from the GoSL management before initiating the testing. MSI is expected to prepare a detailed plan for conducting the security testing and submit the same to GoSL for approval and begin the testing post approval.	Post this, every half year.	<100%	2
11	Change Management	Completion	Changes should be tracked formally and should be as per the Change Management procedure defined and all changes should be carried out within the timelines defined in the procedure document. 100% of change implementation as per agreed timelines for each change request. Formula – (number of changes that were done within timeline as per the process defined / total number of changes) * 100	During operations and maintenance phase on a quarterly basis	100%	0
					<100 and >=98%	1
					<98 and >=95%	2
					<95 and >=90%	3
					<90%	4

Table 9.16: Security Operations SLAs

9.9.3 Business Continuity Management

#	*Service Level*	*Metric Type*	*Definition*	*Period and Time of Measurement*	*Target*	*Severity Leve*
1	DR Drill for enrolment and authentication	Compliance	Timely conduct of DR drills on quarterly basis. For each instance when DR drill is not carried out for the reasons attributable to the bidder	Quarterly	Per Instance	6
2	DR Drills (Overall)	On Time	Number of drills NOT Conducted as per the defined Business Continuity Plan (BCP) policy.	Quarterly	Per Instance	6
3	Sample restoration of data from backup tapes	Compliance	Timely conduct of successful sample restoration on fortnightly basis For each instance when either restoration is not carried out or restoration is unsuccessful for the reasons attributable to the bidder	Quarterly	Per Instance	6
4	Full Data backup from tapes	Compliance	Timely conduct of successful full backup restoration on half-yearly basis For each instance when either restoration is not carried out or restoration is unsuccessful for the reasons attributable to the bidder	Annual	Per Instance	8 Or 9 (if breach occurred for two consecutive instances)

#	*Service Level*	*Metric Type*	*Definition*	*Period and Time of Measurement*	*Target*	*Severity Leve*
5	RPO	Compliance	Timely and successful demonstration of RPO For each instance when either demonstration is not carried out or demonstration hasn't achieved the intended levels of RPO for enrolment and authentication	Quarterly	Per Instance. Refer Vol-2 Section 5.8.2.~~2~~	8 Or 9 (if breach occurred for two consecutive instances)
6	RTO	Compliance	Timely and successful demonstration of RTO For each instance when either demonstration is not carried out or demonstration hasn't achieved the intended levels of RTO for enrolment and authentication	Quarterly	Per Instance Refer Vol-2 Section 5.8.2.~~2~~	8 Or 9 (if breach occurred for two consecutive instances)
7	Backup	Scheduled Backups	**Metric**: Compliance to the backup schedule as agreed upon by the MSI and GoSL **How**: Monthly reporting of successful backup activities	Monthly	100%	0
					< 100%	5

Table 9.20: Business Continuity Management

NATIONAL INSTITUTE FOR SMART GOVERNMENT ON BEHALF OF

THE GOVERNMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

Ministry of Digital Economy

BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS

Volume 02 of 03 - Annexure 10: Manpower Requirements

Two Stage Bidding Procedure

FOR THE

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

INVITATION FOR BIDS No: NISG/SLUDI-2025

June, 2025
Amended: January, 2026

Table of Contents

10.1 Professional Staff and Engagement Approach 3
10.2 Minimum Qualifications of Key Professional Staff 5
10.3 Resource Requirement 48
10.3.1 Guidelines for Staffing and Provisioning of Manpower 48
10.3.2 Removal of Personnel 48
10.3.3 Replacement of Personnel 49
10.3.4 Logistics Requirements of the Personnel 49
10.3.5 Escalation Matrix 49
10.3.6 Role of GoSL and Responsibilities 49

10.1 Professional Staff and Engagement Approach

The following key professions are required for the core team.

No	Key Professional Staff	Deployment (Implementation Phase)	Deployment (O&M Phase)
(A) Project Management Role			
1	Project Director	Onsite on need basis for one month every quarter	Offsite on need basis for one month every quarter
2	Technical Project Manager	Full-Time Onsite	
3	Support and Operations Manager		Full-Time Onsite after Go-Live
(B) Architects			
1	Chief Architect	Primarily Offsite during design phase and Onsite on need basis during the design phase as per deployment schedule.	On need basis
2	Software Architect (Application Architect)		
3	Security and Network Architect		
4	Infrastructure & Systems Architect		
5	Database Architect		
6	Quality Assurance Architect		
(C) Team Leads and Track Leads			
1	Team Lead – UI/UX	Primarily Offsite during design phase and Onsite on need basis during the design phase as per deployment schedule. ***Note: Business Analyst will be Onsite Fulltime during Design Phase***	Onsite on need basis for after Go-Live.
2	Team Lead – Business Analyst		
3	Team Lead – Quality Assurance		
4	Team Lead – Training and Certification		
5	Track Lead – Data and Analytics		
6	Track Lead – Network & Security		
7	Track Lead – Data Center Manager		
8	Track Lead – Systems Engineering		
9	Track Lead – Application Manager		

No	Key Professional Staff	Deployment (Implementation Phase)	Deployment (O&M Phase)
11	Track Lead – Enrolment and Authentication		
(D) Engineers			
1	Infrastructure Engineer	Full-Time Onsite	Offsite
2	Network Engineer	Full-Time Onsite	Offsite
3	CRM Engineer	Full-Time	Offsite
4	BI Reporting and Data Analytics Engineer	Full-Time	Offsite
5	Application Engineer	Full-Time	Offsite
(E) Biometrics (From BSP)			
1	Manager – Biometric	Onsite on during design phase and on need basis.	Onsite on need basis
2	Biometric - Implementation and Integration Engineer	Onsite full-time after design phase	
(F) Security			
1	Information Security Manager	Full-Time Onsite	Onsite Part-Time
(G) Software			
2	Business Analysts	Onsite full-time during the implementation phase.	Offsite on need basis
(H) Other			
1	IT Helpdesk Agents	Onsite full-time at least one month before helpdesk launch	Onsite full-time
2	NOC Agent	Onsite full-time at least one month before NOC launch	Onsite full-time
3	SOC Agent	Onsite full-time at least one month before SOC launch	Onsite full-time
4	Administrators (Server, Network, Storage, Database)	Onsite full-time at least one month before data center launch	Onsite full-time

Table 1: Key Professionals

i. The MSI is required to submit a detailed organization structure in the technical proposals which should mention all the resources, their roles in project, responsibilities assigned to them, their deployment (man-months). In addition, the deployment plan for these resources should be consistent with the deployment duration specified in the technical proposal.

ii. The MSI should propose an adequate team comprising of key professionals (mentioned above) and other professionals to meet the timelines, quality norms, service levels, etc.

iii. The MSI should ensure the other key professionals who are proposed through this assignment/ contract are available on-demand throughout the duration of the assignment/contract without delay to ongoing SL-UDI project activates.

iv. The MSI should allocate the full-time Project Management professional(s) for this assignment. The other key professionals can be allocated on a need basis.

v. The MSI should ensure adequate support staff to assist the Project Management professionals who are assigned to this project.

vi. The resources (engineers, developers, and testers) should be adequately trained in the respective technologies being proposed for this engagement. Wherever such certification is available from the OEM, the resources should also have the OEM issued certification for their specific roles.

10.2 Minimum Qualifications of Key Professional Staff

i. The MSI should give the team of professionals with the curriculum vitae and team organization, of which the validity and accuracy of the CVs are very important. For the profile included under the technical evaluation (refer Volume-1), the CVs are to be submitted by the bidder with the technical proposal. For other profiles (not included in technical evaluation as well as non-key professionals), the CVs are to be submitted by the selected bidder at the time of team mobilization.

ii. For technical profiles, the resources should have the relevant technology/product certifications from the respective OEM, wherever available.

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
Project Management Roles						
1	Project Director	MBA/ME/M-Tech/BE/B-Tech or Equivalent Certifications: Certification in Project Management (PMP, or Prince2 and related)	20 years	05 years	Experience in handling at least 5 (five) technology-led end-to-end projects of similar scale (scope, timeline, and budget) and out of this at least 1 (one) project should be in government sector. Experience of managing a portfolio of projects, and experience of periodic interaction with C-level of the organization Experience of working in a multi-cultural and diverse environment in at least 3 countries.	• Shall be deployed on-site during implementation Phase and part time during O&M phase in Sri Lanka as per the proposed deployment plan • Responsible for organizing, planning, directing and coordinating overall program effort • Should have extensive experience and proven expertise in managing similar contracts • Establish overall SL-UDI Programme and project management strategy • Link objectives of the SL-UDI Programme and the technical solution being implemented • Implement SL-UDI Implementation Strategy and Plan • Development of procurement strategy and deployment strategy • Monitor overall project progress and provide direction • Responsible for periodically assessing the project resourcing and ensuring it is in line with proposed deployment and adequate for project requirements

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
						• Assess project risks and ensure timely resolution • Ensure compliance to the terms and conditions of contract and SLAs • Manage project scope and ensure its deliverables
2	Technical Project Manager	MBA/ME/M-Tech/BE/B-Tech or equivalent Certifications: Desired – SCRUM Master Other Certification (PMP or Prince2) in Project Management	15 years	10 years	Experience in handling at least 3 (three) technology-led end-to-end projects of similar scale (scope, timeline, and budget) and out of this at least 1 (one) project should be in government sector. Experience as project manager on a national identity project with biometric aspect	• Shall be deployed on-site full time for the duration of the project during implementation phase • Act as single point of contact for Project Committee • Responsible for implementation of Project Governance Systems and Procedures in consultation. • Responsible for successful delivery of SIs deliverables and scope of work • Shall oversee all transition and scaling activities of SL-UDI. • Responsible for supervising allotted resources, procurement, forecasting and demand management of services in SL-UDI. • Own and be responsible for all SL-UDI policies and procedures implemented by SI • Responsible for audit readiness of the SI and shall be the owner in charge of redressal of all audit findings

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
						• Shall participate in all fortnightly / monthly project meetings and project review meetings • Shall ensure Quality Assurance for all goods and services delivered by SI
3	Support and Operations Manager	MTech / ME/B-Tech/BE or equivalent Certifications: ITIL (Desired)	15 years	05 years	Experience of at least 3 (three) technology-led projects as support manager role in a project of similar scale (scope, timeline, and budget) Experience in managing operations, maintenance, and support (L1, L2 and L3) aspects during O&M phase of a large project in the government sector Experience in managing operations, maintenance, and support (L1, L2 and L3) aspects during O&M phase of a large project with multiple	• Oversee daily operations, ensuring efficiency and productivity. • Develop and implement process improvements. • Manage vendor relationships and contracts. • Ensure compliance with regulatory requirements. • Lead customer support team, providing guidance and training. • Develop and implement support processes and procedures. • Ensure timely resolution of customer issues. • Analyze and report on support metrics. • Manage and mentor support and operations staff. • Conduct performance reviews and provide feedback. • Foster collaboration and open communication. • Contribute to organizational strategic planning.

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					OEMs, ecosystem partners, sub-contractors, etc. Experience is mandatory in a similar capacity on (a) biometric based projects, (b) DevSecOps, (c) Cloud Infrastructure, (d) Network and Security, and (e) Change Management	• Develop and manage departmental budgets. • Identify areas for improvement and propose solutions.
Architects						
1	Chief Architect	MS / MTech / ME / MCA/BE/B-Tech or equivalent Certifications (Desired): TOGAF	15 years	10 years	Experience in designing enterprise architecture for at least 3 (three) large scale technology-led projects of similar scale (scope, timeline, and budget) and out of this at least 1 (one) project should be in the government sector. Experience is mandatory in a similar capacity on (a) biometric based	• Should be deployed onsite as per the deployment plan during design phase of the SL-UDI project • Shall be single point of contact for the SL-UDI Technology solution requirements • Develop deep understanding of SL-UDI architecture • Manage architectural requirements • Imbibe key architectural principles proposed and perform detailed design of software, hardware, network and security architecture of SL-UDI Registry

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					projects, (b) DevSecOps, (c) Cloud Infrastructure, (d) Network and Security, (e) microservices, (f) enterprise architecture, server architecture, network architecture, database architecture, security architecture, deployment architecture etc. Experience of National Identity project is mandatory Experience or Knowledge of MOSIP is desirable	• Responsible for creating or selecting the most appropriate architecture and technology components for SL-UDI such that it suits the business needs, satisfies user requirements, and achieves the desired results under given constraints • Review software solution development to ensure alignment with the architecture designed should proactively monitor the adherence of the implementation to the chosen architecture during all iterations • Re-design the solution based on feedback received on functionality and performance, if needed • Implement continuous improvements in architecture, solution, algorithms and infrastructure to contain costs • Manage SL-UDI architectural changes and ensure timely and accurate documentation of all key changes
2	Software Architect (Application Architect)	MS / MTech / ME / MCA / BTech / BE	12 years	5 years	Experience in designing solution/application architecture for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget)	• Should be deployed onsite as per the deployment plan during design phase of the SL-UDI project till Go-Live of key SL-UDI modules • Shall be single point of contact for the SL-UDI Software solution requirements • Manage architectural requirements from a

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					Experience is mandatory in a similar capacity on (a) biometric based projects, (b) Agile methodology, (c) DevSecOps, (d) Microservices architecture, (e) software architecture (Docker based deployment, Hybrid Mobile Application Development, etc.), (f) integration architecture, and (g) quality engineering Experience of National Identity project is mandatory Experience or Knowledge of MOSIP is desirable	software perspective • Imbibe key architectural principles proposed and perform detailed design of software and required data and application security • Responsible for creating or selecting the most appropriate architecture and technology components for SL-UDI such that it suits the business needs, satisfies user requirements, and achieves the desired results under given constraints • Implement continuous improvements in architecture, solution, algorithms and infrastructure to contain costs • Manage SL-UDI architectural changes and ensure timely and accurate documentation of all key changes
3	Security and Network Architect	BE / BTech / MS / MTech / ME / MCA	12 years	5 years	Experience in designing security architecture for at least 5 (give) large scale technology-led	• Responsible for developing the IS policies and procedures for SL-UDI and their periodic review • Head of the Information Security function

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					projects. Experience is mandatory on (a) Biometric based projects, (b) DevSecOps, (c) establishing and managing security operation center, (d) governance, risk, and compliance, (e) authentication and authorization standard, (f) Information security products design and deployment and (g) business continuity planning Experience is mandatory in information technology security design, operations, encryption, information	from the SI's team • Work closely with other vendors appointed to ensure that IS policies and procedures are implemented properly • Review overall Information Security posture of SL-UDI and undertake architecture reviews and enhancements in consultation with the Chief Technology Architect • Responsible for training, communications and obtaining necessary Information Security certifications for SL-UDI • Overall security of SL-UDI Data centers. Should work with the Data Center Managers to ensure that security is adequately safeguarded. • Be responsible for establishing governance and processes to ensure that the company's information Security and Personal Data Privacy policies, standards and practices are updated, implemented and complied • Develop, promulgate, and maintain policies, standards and practices of Information Security by establishing and maintaining efficient processes to monitor compliance of defined policies, standards and practices. • Assist in planning for information security

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					access, biometric security, and authentication processes. Relevant experience in managing and reviewing the configuration of security devices and solutions such as IAM, DLP, WAF, firewall etc. Experience of projects with ISO 27001 and ISO 22301 compliances Experience of National Identity project is mandatory Experience or knowledge of MOSIP is desirable	risk monitoring, risk analysis, incident management • Manage and perform internal IS audits at regular intervals and assist in External Audits and certifications • Ensure that threats, vulnerabilities, cyber-attack and attendant risks are proactively identified and appropriately mitigated, avoided or accepted • Lead regular reviews of emerging technology risks and vulnerabilities that may impact the company and its business • Lead the IS incident response team, and investigate security violations • Administer IS training and awareness program • Monitor the development of IT and IS related legislation and industry developments, and advise senior management of necessary actions and countermeasures in conformance with relevant legislation • Establish and Manage Business Continuity Management and ensure all BCP-DR activities performed on timely manner

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
4	Infrastructure & Systems Architect	MS / MTech / ME / MCA / BTech / BE or equivalent Certifications: Cloud Architect (Desired)	12 years	5 years	Experience in designing systems and infrastructure architecture for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience is mandatory on (a) Highly scalable private cloud platforms, (b) DevSecOps, (c) Object storage platforms, (d) Kubernetes, (e) Microservices, (f) Docker based deployment, (g) multi-site architecture Experience or Knowledge of MOSIP is desirable	• Should be deployed onsite as per the deployment plan during design phase of the SL-UDI project till Go-Live of key SL-UDI modules • Shall be single point of contact for the SL-UDI IT infrastructure requirements • Manage architectural requirements from IT infrastructure perspective • Imbibe key architectural principles proposed and perform detailed design of IT infrastructure and required data and IT infrastructure security • Responsible for creating or selecting the most appropriate architecture and technology components for SL-UDI such that it suits the business needs, satisfies user requirements, and achieves the desired results under given constraints • Implement continuous improvements in architecture to optimize costs • Manage SL-UDI architectural changes and ensure timely and accurate documentation of all key changes
5	Database Architect	MS / MTech / ME / MCA / BTech / BE or equivalent	12 years	5 years	Experience in designing database architecture for at least 2 (two) large scale technology-led	• Will be responsible for coordinating current and future development efforts involving all elements of the databases

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
		Certifications: DBA (Desired)			projects of similar scale (scope, timeline, and budget) Experience is mandatory in a similar capacity on (a) biometric based projects, (b) relational and non-relational database, (c) clustering and replication, (d) backup and restoration, (e) database optimization and tuning, (f) disaster recovery, (g) space management Experience in the architecture and design of population scale databases Experience of National Identity project is mandatory Experience or Knowledge of MOSIP is desirable	• Lead all planning, database design, code review, and performance optimization • Will oversee documentation activities. • Will choose to implement the databases in accordance with the specifications and in collaboration with the various stakeholders (project manager, architects, integrators, consultants, etc.) • Optimally define database settings. • Define data security rules (physical and logical) as well as standards for the use of the bases. • Model the bases and the relationships between them and supervise the design of tables and keys. • Will take into account the specificities of the internal or external customer in collaboration with the infrastructure architect, in particular with regard to the size of the database (capacity planning). • Review and approve server sizing. • Guarantee of data availability and quality by maintaining and improving performance and functionalities (by improving their automation, optimizing processing and queries, parameterization, etc.).

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
6	Quality Assurance Architect	MS / MTech / ME / MCA / BTech / BE Certifications (Desired): ISTQB (International Software Testing Qualifications Board) or CMSQ (Certified Manager of Software Quality)	12 years	5 years	Note – This profile should directly report to Project Director as well as Chief Architect Experience in designing quality architecture for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience is mandatory in a similar capacity on (a) biometric based projects, (b) Agile methodology, (c) DevSecOps, (d) manual and automation testing, and (e) non-functional testing Experience of National Identity project is mandatory Experience or Knowledge of MOSIP is desirable	• Develop and maintain QA vision, mission, and strategic plans. • Define QA processes, standards, and best practices. • Collaborate with cross-functional teams to ensure QA alignment. • Design and implement QA architectures for software applications. • Ensure scalability, reliability, and maintainability of QA solutions. • Evaluate emerging technologies and trends in QA. • Develop and execute comprehensive testing strategies. • Conduct manual and automated testing. • Identify and report defects. • Lead and mentor QA teams. • Conduct performance reviews and provide feedback. • Foster collaboration and open communication. • Analyze and improve QA processes. • Implement continuous integration and delivery. • Ensure compliance with industry standards.

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
Team Leads						
1	Team Lead – UI/UX	MS / MTech / ME / MCA / BE / BTech or equivalent Certifications preferred: UI/UX or design thinking	10 years	5 years	Experience in designing user experience and user interfaces for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience is mandatory on (a) Design thinking, (b) Enterprise Applications, (c) Wireframing and Prototyping, and (d) Hybrid Mobile Applications	• Lead and mentor a team of UI/UX designers. • Foster a collaborative environment and encourage open communication. • Develop and implement design processes and standards. • Conduct performance reviews and provide constructive feedback. • Design and deliver high-quality, user-centered UI/UX solutions. • Conduct user research, create wireframes, prototypes, and high-fidelity designs. • Collaborate with cross-functional teams (Product, Development, QA). • Ensure design consistency across products. • Develop and maintain design guidelines, standards, and best practices. • Stay current with industry trends, technologies, and design tools. • Contribute to product strategy and roadmap development. • Manage design projects from concept to launch. • Ensure timely delivery of design assets and specifications.

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
						• Conduct design reviews and provide constructive feedback.
2	Team Lead – Business Analyst	MBA / MS / MTech / ME / MCA / BE /BTech / BCA or equivalent Certification: IIBA, PBA, CSPO	10 years	5 years	Experience in leading the business analysis for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience is mandatory in (a) requirement gathering and elicitation, (b) agile practices, (c) product ownership experience, (d) Lead the team of business analysts in a cross-territory environment, (e) business process re-engineering, and (f) national identity. A knowledge of MOSIP and all COTS/OTS	• Provide tools for in-depth analysis of data resulting from the various processes (enrollment, authentication, etc.) • Simplify and automate reporting, and other data-driven activities. • Define and implement business intelligence tools adapted to the requirements of the RNP • Build solutions to have maximum capacity for self-service by stakeholders. • Improve data sources for greater accuracy and simplicity. • Recognize and adopt best practices in reporting and analysis: data integrity, test design, analysis, validation, and documentation. • Propose tactical and critical data analysis schemes and models.

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					components is preferable. Note: This profile should be supported with adequate number of Business Analysts and Product Owners (at least one per component working in parallel as per the project plan).	
3	Team Lead – Quality Assurance	MBA / MS / MTech / ME / MCA / BE /BTech or equivalent Certifications (preferred): ISTQB (International Software Testing Qualifications Board) or CMSQ (Certified Manager of Software Quality)	12 years	8 years	Note – This profile should directly report to quality assurance architect Experience in leading the quality assurance for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience is mandatory on (a) Test plan development, (b) agile practices, (c) Test automation and DevSecOps, (d) leading security, performance, integration, and API testing etc. as applicable	• Leads the identification and disposal of duplicate enrollments, enrollments with poor demographic or biometric data quality, and quality checks of cases with biometric exceptions and cases with anomalous biometrics • Work closely with Manager – Software Development and Manager – BI, Analytics and AI / ML to implement automation procedures for Quality Checks, Demographic Validations and Manual Adjudication • Assist in case management of high risk cases • Publish operational metrics to improve Enrolment operations and also assess quality of BSP's services

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					for this project.	
4	Team Lead – Training and Certification	Any degree.	10 years	5 years	Experience in leading the training as a master trainer under the train the trainer approach for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) out of which at least 1 (one) project should be in the government sector Experience of the establishing a certification program for a large-scale project Should be able to fluently read and speak local languages (Sinhalese and Tamil) as well as English	• Work closely with the Software Development team for timely rollout of the Learning Management System and Knowledge Management System • Prepare detailed Training Plan in consultation with the Program Manager in line with the rollout requirements • Implement Training Effectiveness Evaluation procedures • Prepare strategy for training large number of resources in a short interval including Training the Trainer, Online training, etc. • Organize training content and coordinate content development efforts • Systematically identify key knowledge objects and work closely with the architecture, information security and software development teams to ensure that documentation is up-to-date and maintained in a central Knowledge Repository • Implement procedures for managing access to key knowledge objects • Work closely with the Manager – CRM, Manager – Enrollment and Manager –

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
						Ecosystem Partnerships to identify frequently encountered questions from various stakeholders and implement easy to access and understand procedures to the relevant answers / knowledge objects • Publish calendar of Training and Knowledge sharing events and organize virtual / physical events to ensure that learning and knowledge management are effectively embedded into SL-UDI implementation
5	Track Lead – Data and Analytics	MS / MTe ch / ME / MCA / BE / BTech / BCAor equivalent	10 years	5 years	Experience in leading the data and analytics track for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience is mandatory on (a) structured and unstructured data handling, (b) data visualization, (c) trend analysis, fraud analysis, etc.	• Shall be responsible for architecting key data stores and carrying out data engineering routines to enable timely metrics analysis and reporting • Help key stakeholders analyse operational data and enable data-driven decision making • Help create AI / ML based systems to support fraud management, improve resident services and robustness of the overall SL-UDI system

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
6	Track Lead – Network & Security	MS / MTech / ME / MCA / BE / BTech / BCA or equivalent Certifications preferred: PMP / CISSP / CCNA / CISM / CompTIA Network+ / CGRC- IT / ITIL / TOGAF	10 years	5 years	Experience in leading the network and security tracks for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience in following is mandatory in similar capacity (a) At least 6 years of experience in IT / networks and telecommunications including at least 4 years as network administration for large missions. (b) Experience as main administrator of 3 large network	• Responsible for developing the IS policies and procedures for SL-UDI and their periodic review • Head of the Information Security function from the SI's team • Work closely with other vendors appointed to ensure that IS policies and procedures are implemented properly • Review overall Information Security posture of SL-UDI and undertake architecture reviews and enhancements in consultation with the Chief Technology Architect • Responsible for training, communications and obtaining necessary Information Security certifications for SL-UDI • Overall security of SL-UDI Data centers. Should work with the Data Center Managers to ensure that security is adequately safeguarded. • Be responsible for establishing governance and processes to ensure that the company's information Security and Personal Data Privacy policies, standards and practices are updated, implemented and complied • Develop, promulgate, and maintain policies, standards and practices of Information

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					installations (c) Experience in managing at least 5 completed projects for large, enterprise scale clients for information security related work. (d) Should have in-depth knowledge of international information security related standards such as ISO 27001, NIST cybersecurity framework, etc. (e) Experience in advising senior management on IS strategies and implementation plans at the organization ecosystem level. (f) Experience in using open sources	Security by establishing and maintaining efficient processes to monitor compliance of defined policies, standards and practices. • Assist in planning for information security risk monitoring, risk analysis, incident management • Manage and perform internal IS audits at regular intervals and assist in External Audits and certifications • Ensure that threats, vulnerabilities, cyber-attack and attendant risks are proactively identified and appropriately mitigated, avoided or accepted • Lead regular reviews of emerging technology risks and vulnerabilities that may impact the company and its business • Lead the IS incident response team, and investigate security violations • Administer IS training and awareness program • Monitor the development of IT and IS related legislation and industry developments, and advise senior management of necessary actions and countermeasures in conformance with relevant legislation • Establish and Manage Business Continuity

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					tools and technologies and managing risks and vulnerabilities across the same (g) Technical expertise in the management of the deployment and maintenance of large networks, network security, access administration, system integrity / reliability (h) Experience of establishing, supervising, and operating the Security Operations Centre	Management and ensure all BCP-DR activities performed on timely manner
7	Track Lead – Data Centre Manager	MS / MTech / ME / MCA / BE / BTech / BCA / BSc / MSc or	10 years	5 years	Note – This profile should be from the data center co-location provider in Sri Lanka.	• Assist the IT infrastructure architect in preparing detailed implementation architecture • Prepare detailed installation, commissioning

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
		equivalent			Experience in leading the data center and/or cloud infrastructure tracks for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience of Data Center for large scale technology-led projects in the government sector Experience in following is mandatory in a similar capacity (a) At least 5 years of experience as a Data Center Manager, managing all aspects of large infrastructure projects (b) At least 3 years of experience in the operations of data center in a highly scalable manner	plan for the Data Center assigned • Coordinate delivery of equipment to the Data Center • Carry out detailed rack level planning and work with the Data Center physical infrastructure managers to ensure that adequate Power and HVAC facilities are available • Check on basic Data Center amenities such as fire protection, rodent control, moisture control, power backup, air quality and noise / vibrations and resolve any issues prior to Go-Live • Organize the equipment with clear signages and markings within the Data Center • Organize structured cabling for network and power with appropriate labelling • Track and improve Power utilization on an ongoing basis • Track presence of harmonics and other electrical fluctuations which can potentially damage the equipment and work with the Data Center providers for early resolution • Organize business continuity and disaster recovery drills in consultation with the CISO • When required, plan for data center

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					(c) Experience in the supervision and administration of DC infrastructure operations Experience in the design and management of structured cabling infrastructures and in-depth knowledge of cable distribution systems and industry standards	migrations and execute the same in consultation with the Program Manager and other Data Center managers • Manage tape backups and ensure their traceability • Implement well-designed Asset IMAC procedures
8	Track Lead – Systems Engineering	MS / MTech / ME / MCA / BE / BTech / BCA or equivalent	10 years	5 years	Experience in leading the data center and/or cloud infrastructure tracks for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience in following is mandatory in a similar capacity	• As part of Build Phase, coordinate the efforts of the OEM engineers to ensure that all devices are deployed and configured as per the overall SL-UDI architecture • Work closely with the CISO to ensure that Information Security policies and procedures are implemented in a timely manner • Assist in conduct of VAPT exercises and perform remedial measures as per recommendations received from the testing

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					(a) At least 5 years of experience as a System Engineer, managing all aspects of large infrastructure projects (b) At least 3 years of experience in the establishment and operations of on-premises cloud environment and highly scalable private cloud platforms (c) Experience in the supervision and administration of DC infrastructure operations	team • Carry out periodic vulnerability assessment of key assets and contribute to the risk identification exercise • Ensure that the team of administrators are adequately trained and aware of key policies and procedures • Organize the work of Network Operations Center and manage deployment of personnel to ensure 24x7 operations • Assist in conducting BCP / DR drills

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					(d) Experience in Micro services, Object storage platforms, Kubernetes, Micro services, Docker based deployment Experience in backup and restoration, disaster recovery and business continuity	
9	Track Lead - Application Manager	MS / MTech / ME / MCA / BE / BTech / BCA or equvalent	10 years	5 years	Experience in leading the software tracks for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience in following is mandatory in a similar capacity (a) At least 5 years of experience in application development and implementation management (b) Experience in implementing,	• Work closely with the Software Architect to finalize requirements, architecture and align the software development plan with overall SL-UDI implementation timelines • Develop detailed project plan for software development in consultation with key stakeholders and publish Release Plans to all stakeholders • Work closely with CISO to ensure that secure coding standards are implemented and software incorporates Information Security requirements • Implement Software Quality Assurance processes • Participate in project reviews and coordinate the efforts of the software development team • Implement systematic issue tracking and

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					operating, and maintaining a wide range of applications (bespoke applications, open-source products, commercial products, etc.) (c) Experience in national identification systems, enrolments, and authentication Experience in identification and authentication systems (d) Mastery of biometric algorithms (e) In-depth knowledge of proposed ABIS system (c) Extensive experience on the ISO biometric standards used in this project	ensure that production issues are tracked to closure in line with SLAs

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					(d) Experience in following projects is desirable in similar capacity (a) National ID projects and (b) MOSIP based solutions in projects (e) Proficiency in risk assessment procedures, policy training, role-based authorization methodologies, and authentication technologies (f) Experience of National Identity project is mandatory (g) Experience or Knowledge of MOSIP is desirable Knowledge of business models, pricing, etc. is desirable	
Experts and Administrators						

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
1	Infrastructure Engineer	BE / BTech / MSc / MCA / MTech or equivalent Certifications: ITIL or equivalent (preferred)	10 years	5 years	Experience in leading infrastructure aspects for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience in following is mandatory in a similar capacity (a) Experience in managing all aspects of large infrastructure projects (b) Experience in managing at least 3 completed projects for large, enterprise scale clients for IT Infrastructure related work (c) Object storage platforms, Kubernetes, Docker based	• Should be deployed onsite as per the deployment plan during design phase of the SL-UDI project till Go-Live of key SL-UDI modules • Shall be single point of contact for the SL-UDI IT infrastructure requirements • Manage architectural requirements from IT infrastructure perspective • Imbibe key architectural principles and perform detailed design of IT infrastructure and required data and IT infrastructure security • Responsible for creating or selecting the most appropriate architecture and technology components for SL-UDI such that it suits the business needs, satisfies user requirements, and achieves the desired results under given constraints • Implement continuous improvements in architecture to optimize costs • Manage SL-UDI architectural changes and ensure timely and accurate documentation of all key changes

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					deployment. (d) Highly scalable private cloud platforms	
2	Network Engineer	BE / BTech / MSc / MCA / MTech or equivalent Certifications: CCNP	8 years	5 years	Experience in leading networking aspects for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience in following is mandatory in a similar capacity (a) Deploying Network Components within the Data Centre and Disaster Recovery Site (b) Experience in implementation and operations of at least 3 completed projects for large, enterprise scale clients for Data Centre Network	• Configure and install the various network devices and services (routers, switches, firewalls, load balancers, VPNs, QoS) • Write network maintenance procedures and define system upgrade procedures, including packs, patches, and security configurations • Track performance and ensure system availability and reliability • Monitor system resource usage and trends and plan capacity • Provide level 2/3 support and troubleshooting to resolve any issues • Work within established configuration and change management policies to ensure successful changes to network infrastructure • Ensure the implementation of the defined network architecture (physical and logical components) • Select and implement security tools, policies, and procedures in collaboration

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					(c) Experience of leased line, MPLS, SDWAN, etc.	with the security team • Provide technical support in the operation of RNP network infrastructure • Ensure proper configuration for external customers (RNP user agencies) • Control facilities and ensure compliance with network requirements • Support internal application groups and troubleshoot any issues • Formalize network administration and high availability procedures • Backup of all critical data center devices for the base layer and network aggregation layer. • Monitor system stability and performance, ensuring 24/7 operations
3	CRM Engineer	BE / BTech / MSc / MCA / MTech or equivalent	8 years	5 years	Experience as CRM engineer for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience in following is mandatory in similar capacity (a) Experience in managing CRM	• Work closely with the architecture team to detail the business requirements for CRM and CCM and hold responsibility for comprehensive requirements documentation from CRM / CCM perspective • Work closely with Manager – Software Development in Release Planning, performance of User Acceptance Test and Handhold the rollout of various versions of CRM, CCM and Helpdesk solutions for SL-UDI

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					Software (b) Experience in managing at least 3 call center projects	• Organize the Resident Support unit, arrange for required training of staff and ensure operational readiness of the Resident Support unit in line with SL-UDI • roll out timelines • Provide support via the Technical Helpdesk to users and align operations with the Ticket Resolution SLAs • Analyze Contact Center metrics and provide recommendations for improving operational areas and Quality of Services to residents
4	BI Reporting and Data Analytics Engineer	BE / BTech / MSc / MCA / MTech or equivalent	8 years	5 years	Experience as BI Reporting and Data Analytics Engineer for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience in following is mandatory in similar capacity (a) Experience in managing BI Reporting and Data Analytics Software	• Provide tools for in-depth analysis of data resulting from the various processes (enrollment, authentication, etc.) • Simplify and automate reporting, and other data-driven activities. • Define and implement business intelligence tools adapted to the requirements • Build solutions to have maximum capacity for self-service by stakeholders. • Improve data sources for greater accuracy and simplicity. • Recognize and adopt best practices in reporting and analysis: data integrity, test design, analysis, validation, and documentation. • Propose tactical and critical data analysis

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					(b) Experience in designing, developing, and maintaining the reports, dashboards and analytics	schemes and models.
5	Application Engineer	B.E. / B. Tech / M.Sc. / MCA / M. Tech or equvalent	8 years	5 years	Experience as Application Engineer for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience in following is mandatory in similar capacity (a) Experience in managing Software Applications (b) Experience in designing, developing, and maintaining the software applications (bespoke, COTS etc.)	• Carry out the technical evaluation of the target application park and prepare its introduction • Predict and resolve product quality issues • Initiate and conduct assigned technical activities leading to effective products, processes and applications • Prepare reports and provide presentations on application progress • Lead training and demonstration to internal customers • Work on the maintenance of coding projects • Analyze and understand complex application code and perform code corrections to resolve any issues • Support for deploying software in production environments • Develop tools to facilitate operations and maintenance. • Report system and media status.

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
						• Work with engineering teams to escalate or support active support issues • Create an app knowledge base and monitor the performance of teams working on different apps
Biometrics (From BSP)						
1	Biometric – Implementation and Integration Engineer	BE / BTech / BSc / MSc / MCA / MTech or equivalent	8 years	3 years	Experience as integration engineer for biometric applications in large scale technology-led projects Experience in following projects is mandatory in a similar capacity (a) Software integration of biometric applications using similar architecture (b) Should have been a lead integration engineer for a biometric project of comparable size	• Will be deployed on a full-time basis in Sri Lanka and will be required to travel within Sri Lanka to effectively manage the Enrollment and Update operations • Implement the Resident Enrollment and Update procedures as per the Enrollment and Update Manual • Identify challenges faced during Enrollment and Update operations and recommend process improvements • Work with Ecosystem Partners to ensure that processes are well understood and documented and quality of services is consistent • Actively implement Mass Communication programs as well as targeted communication programs to inform Residents of the processes and procedures for Enrollment and Update as well as the various Service Access channels

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					and complexity (Multi- modal ABIS of at least 20 million gallery size) (c) Windows, Linux, middleware, high performance messaging, Java/J2EE, C, ISO standards for biometrics and other technologies needed for server integration or experience in knowledge of Windows, .NET, C#, C, biometric device protocols and formats (d) Knowledge of integrating the proposed biometric SDK (e) Exposure to Rest APIs and API security	• Work in close coordination with the CRM and CCM department to ensure timely issue resolution for residents • Implement metrics gathering mechanisms working in close association with the Software Development team to assist in decision making • Will be responsible for publishing accurate Enrollment and Update metrics • Ensure adequate training of Enrollment and Update operators • Work with the software development team to implement workflow enhancements and improve usability of the SL-UDI system, especially the Pre-registration module and Mobile app(s)
4	Manager - Biometric	BE / BTech / BSc / MSc / MCA / MTech or	10 years	5 years	Experience as biometric specialist for biometric applications in large	• Will be deployed on a full-time basis and will be required to travel within Sri Lanka to

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
		equvalent Certifications (desired): IEEE Certified Biometrics Professional (CBP) Program,			scale technology-led projects Experience in following is mandatory in a similar capacity (a) Should have been a Lead biometric specialist for a project of comparable size and complexity (Multi-modal ABIS of at least 20 million gallery size) (b). Should have thorough knowledge biometric algorithms, biometric devices, and identity management systems. (d). Should have over 2 years of experience in conducting performance and accuracy improvements Should have over 2 years of experience with (i) fingerprint	effectively engage with key stakeholders • Identify challenges faced by various user agencies and recommend process and technology improvements • Responsible for ensuring that key Service Levels of Authentication, e-KYC and APIs is maintained for availability and performance • Work closely with BSP to ensure that quality of services is maintained and improved • Work with Ecosystem Partners to ensure that processes are well understood and documented and quality of services is consistent • Actively implement Mass Communication programs as well as targeted communication programs to inform Residents of the processes and procedures for authentication and e-KYC • Work in close coordination with the CRM and CCM department to ensure timely issue resolution for residents • Implement metrics gathering mechanisms working in close association with the Software Development team to assist in decision making

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					devices and algorithm, (ii) iris devices and algorithm, (iii) facial capture devices and algorithm and (iv) voice capture devices and algorithm	• Will be responsible for publishing accurate authentication and e-KYC metrics
Security Team						
1	Information Security Manager	BE / BTech / BSc / MSc / MCA / MTech / MBA or equivalent Certifications (desired): PMP / CISSP / CISM / CGRC-IT / ITIL / TOGAF	10 years	6 years	Experience as information security manager for at least five large scale technology-led projects. Experience in following is mandatory in a similar capacity: (a) Experience in managing all aspects of large cybersecurity projects. (b) Managing and performing internal audits at regular intervals and manage external audits.	• Definition of the security organization and policy. • Participation in the creation of the safety charter. • Definition and implementation of security procedures. • Assessment of risks, threats and consequences. • Implementation of security measures • Establishment of the prevention plan. • Awareness of security issues in the general management • Training of operational departments and business lines in the field of security. • Facilitation of security awareness meetings. • Technical validation of security tools. • Definition of security norms and standards. • Participation in the development of safety

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					(c) Periodic reviews of emerging technology risks and vulnerabilities that may impact the SL UDI project. (d) Ensuring that threats, vulnerabilities, cyber risks are proactively identified and appropriately mitigated, avoided or accepted. (e) Experience in managing at least 3 completed projects for large, enterprise scale clients for security related work. (f) Experience of developing, implementing, and	rules at the global level • Assurance that security plans have been completed according to defined plans. • Steering periodic security audits and ensuring that teams comply with security measures. • Monitoring of regulatory and technical developments in its field. • Monitors the evolutions necessary to guarantee the logical and physical security as a whole • Will need to be aware of cybersecurity trends and best practices in the field

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					monitoring security policies, protocols, and procedures. (g) Experience of managing and operating the next generation security operations center.	
Note: For the profiles listed below, The MSI is expected to submit the resumes for the given profiles along with the bid proposal and the Resume will be evaluated to ensure the qualification criteria is met by GOSL prior to staff deployment for this assignment. If any profile is unsatisfactory the MSI shall replace the same which meets the minimum qualification criteria spiced here.						
Software Development						
1	Business Analysts	BSc / BE / BTech / MCA/ MTech or equivalent Relevant certifications	5 years	3 years (BA) and 5 years (senior BA)	Experience in following projects is mandatory in a similar capacity (a) Knowledge of relevant COTS components (b) Experience in agile methodologies (c) Hands on experience of user acceptance testing (d) Knowledge of industry standards and best practices related to software development (e) Hands on experience	• Assess business processes and anticipate organizational and support resource needs • Discover areas for improvement and develop and implement solutions for optimizing organizational processes. • Propose an effective organizational structure • Assess IT alignment with business processes • Hold meetings and presentations to share ideas and findings on the ongoing operations • Perform analysis of the organizational requirements of the ecosystem and their impact on the system • Gather critical information in meetings with various stakeholders and propose ways to

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
					as product owner is preferable Note: For business analysts responsible for enrolment and authentication, the relevant knowledge is desirable.	improve • Train various employees on the organizational requirements • Perform user acceptance testing • Ensure the implementation of business procedures • Prioritize organizational initiatives to be put in place to ensure effective service • Ensuring liaison between stakeholders, user agencies and users • Propose a change management plan to be extended to the ecosystem
2	IT Helpdesk Agents	BE / BTech / MCA / MTech or equivalent Certification in relevant tools and technologies, wherever available is desired	5 years	2 years (junior engineer) and 4 years (senior engineer)	At least 4 years of experience in the IT helpdesk	• Answer user calls • Understand the situation of users by asking specific questions as needed and rephrasing the explanations provided • Remotely diagnose a failure (hardware or software) • Identify the resources needed to resolve the issue, and recommend that a technician be dispatched to the site if necessary • Guide the user through the resolution process or take control of the system remotely • Changing or repairing defective items • Perform function tests

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
						• Fill in the intervention monitoring materials and send them to the department concerned
3	NOC Agent	BE / BTech / MCA / MTech or equivalent Certification in relevant tools and technologies, wherever available is desired	5 years	2 years (junior engineer) and 4 years (senior engineer)	At least 3 years of experience in a network operations center of a public entity or large enterprise	• Provide 24-hour network status monitoring and generate the follow-up reports • Report alerts using network monitoring tools • Review and run the network trouble ticket queue • Ensure 1st/2nd level problem resolution and escalate them to safety managers in case of difficulty
4	SOC Agent	BE / BTech / MCA / MTech or equivalent Certification in relevant tools and technologies, wherever available is desired	5 years	2 years (junior engineer) and 4 years (senior engineer)	At least 3 years of experience in a security operations center of a public entity or large company	• Review identified alerts and determined the level of urgency to postpone • Create new trouble tickets for alerts that require higher-level action • Run vulnerability scans and communicate assessment reports • Manage and configure security monitoring tools (NetFlow, IDS, correlation rules, etc.) • Review incident records and follow resolution/climb procedures
5	Administrators (Server, Network, Storage,	BE / BTech / MCA / MTech or equivalent	5 years	2 years (junior engineer) and 4 years (senior	At least 5 years of experience as a Server / Network / Database administrator in a large	**Server** • Administer and maintain server hardware. • Respond to requests to change user

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
	Database)			engineer)	organization At least 5 years of experience as a Storage administrator in DCs larger than 5000 m² Experience in administering large Storage solutions (> 100 TB)	accounts, install software, allocate storage capacity, etc. • Define system configurations to meet availability requirements. • Develop automation scripts and processes to streamline administrative tasks • Create and manage alert thresholds tailored to system requirements. • Interact with vendors for the diagnosis of hardware and software failures. • Perform capacity planning analyses. • Monitor and report on system security, performance, and notable events using server monitoring tools. • Apply patches and updates to infrastructure components • Apply virtualization and redundancy techniques • Prepare, deliver, and maintain documentation related to server systems • Respond to and resolve Level 3 support requests through the ticketing system **Network** • Participate in the design and optimization of the network • Assess the need for additional hardware for

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
						potential network upgrades • Maintain the necessary bandwidth and connectivity. • Ensure that the operating system, servers, switches, routers, and cabling are properly configured to support RNP system requirements. • Perform software installations, upgrades, and patches. • Ensure the integrity of the server's workstations/data. • Administer system resources, user groups, and identities. • Create and maintain all internal technical documentation. **Storage** • Establish user needs and monitor user access and security • Monitor performance and manage settings to provide quick responses to front-end users • Consider both back-end data organization and front-end accessibility for end users • Refine the logical design so that it can be translated into a specific data model • Further refine the physical design to meet

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
						the storage requirements of the system • Install and test the different versions of the database management system (DBMS) • Write database documentation, including standards, procedures, and data definitions for the data dictionary (metadata) • Control access permissions and privileges • Develop, manage, and test backup and recovery plans • Ensure that storage and archiving procedures are working properly • Perform capacity planning • Manage the security and disaster recovery aspects of a database. **Database** • Coordinate daily storage tasks • Monitor volume allocation and zone management • Manage fabric security, analyze storage resource utilization, and optimize performance • Plan capacities, coordinate system upgrades or patches with the various system administrators • Maintain appropriate backup schedules • Ensure data retrieval operations in the event

#	Key Professional Staff	Academic & Professional	Minimum Overall Experience	Minimum Experience in the proposed role	Specific Qualifications / Requirements	Job Descriptions
						of a request • Facilitate out-of-tape storage and employ storage optimization techniques • Monitor storage performance, and plan for requirements based on the expected rate of RNP transactions • Identify and resolve storage issues and bottlenecks • Monitor and comply with design parameters • Ensure compliance with device storage and update procedures • Assist in the management of production and test environments and assist users in troubleshooting storage issues

Table 2: Minimum Qualifications of Key Professional Staff

10.3 Resource Requirement

10.3.1 Guidelines for Staffing and Provisioning of Manpower

i) Implementation of SL-UDI is envisaged offsite at SI's premises wherein, a dedicated core team shall be stationed at the Purchaser's premises while the development will take place in an offshore location.

ii) The bidder shall provide a detailed staffing schedule in their Technical Proposal as per the format provided as part of this RFB.

iii) The staffing schedule should also include an Organization Chart showing the proposed organization to be established by the SI for execution of the scope of work. The organization chart should clearly bring out variations to the Organization structure if any envisaged by the SI for various phases/stages of the project.

iv) A separate organization structure should be provided for clearly identifiable activities such as Development of SL-UDI Software System, call center management, etc.

v) Detailed CVs should be provided for key profiles that will be subject to evaluation. CVs should be as per the format given in this RFP Volume 1 Section 4.4. Area of expertise, role and tasks assigned should be clearly identified for each of the key profiles. Purchaser might interact with the said resources and this interaction shall be considered in technical evaluation.

vi) Key roles in the MSI's team should be held only by Permanent employees of the MSI

vii) The Staffing Schedule should contain the schedule of deployment of the Key personnel. It should also clearly highlight the onsite and offsite effort of each profile.

viii) The SI should ensure that well-qualified and experienced resources with in-depth knowledge hold the respective positions.

ix) The Purchaser shall approve this schedule after its careful study and may ask the SI to make the changes to the schedule, if required.

x) The infrastructure or other facilities required for the efficient execution of work under the Contract, should be provided by MSI or its Sub-Contractors to its employees who are working under this contract.

10.3.2 Removal of Personnel

i) GOSL reserves the right to request MSI to remove any of MSI's authorized representatives due to negligence, professional incompetence and/or being assigned work for which he/she is not qualified and/or suited for. This includes the SI's

employees, or any person(s) deployed by the SI in any of the sites.

ii) GOSL shall state, in writing, the reasons for the request for removal and the SI should ensure that the personnel are removed and replaced with a competent substitute. GOSL will not bear any additional cost with regard to the personnel change.

10.3.3 Replacement of Personnel

i) The MSI should ensure, to the best of its efforts, to avoid any changes to the proposed manpower and organizational structure during the implementation period.

ii) If this is required due to unavoidable circumstances, the ISI should inform GOSL in writing and should seek approval from GOSL. The replacement resource should conform to the guidelines stated under Section 4 - Minimum Qualifications of Key Professional Staff. The MSI should also ensure that the knowledge is transferred effectively and should ensure that sufficient overlap between outgoing and incoming resources to ensure the same level of service.

10.3.4 Logistics Requirements of the Personnel

i) GoSL may require MSI's representatives to be present at its premises. The MSI shall ensure that required representation is available as per demand.

ii) The MSI shall be responsible for the deployment, transportation, accommodation, and other requirements of all its employees required for the execution of the work and provision of services for all costs/charges in connection thereof.

10.3.5 Escalation Matrix

i) The MSI should propose a detailed escalation matrix mapped with the proposed organizational structure of the MSI, including a steering committee for expedited decision making with GOSL as head of the committee.

ii) The escalation matrix should cover key requirements stated in the Service Level Agreements covering the entire project lifecycle. The triggers for escalation should be clearly identified and stated for each category of service in the Technical Proposal.

iii) MSI will also prepare the Escalation Matrix for support relating to MOSIP components in consultation with the Purchaser.

10.3.6 Role of GoSL and Responsibilities

During project duration, GoSL shall have following roles and responsibilities:

i) If onsite presence is required, GoSL will provide basic office amenities to the MSI's personnel at its office locations for performing their part of the obligations. MSI will

not be entitled to any facilities beyond the contractual time frame.

ii) Conducting UAT for the Foundational ID platform deployed and Issuing the Acceptance Certificate on successful deployment of the software application.

iii) Provide necessary support such as coordination between necessary departments to provide necessary information, provision of list of participants coordination with stakeholders' participants, etc. to the workshops for the Stakeholder departments, if any.

iv) The purchaser will provide the following infrastructure and no other facilities beyond this scope mentioned.

   a. Office space for onsite manpower including Seating Facility that includes desks and chairs for this number of staff.

   b. Communication Room for Connectivity

   c. LAN connectivity, Network printing facility, Electrical Connectivity.

v) GoSL through its Nodal department/agency will assist in coordination between all the divisions/departments for providing necessary information for the study and development/customization of the necessary solution.

vi) GoSL will provide necessary support to MSI for conducting workshops for the stakeholder departments, if any.

vii) GoSL will jointly monitor overall timelines, SLAs, and calculation of penalties accordingly.

viii) Ensuring the staff members and other stakeholders attend the training programs as per the approved training calendar.

ix) Any other requirements that could arise during operations for effective governance and to meet any administrative requirement.

NATIONAL INSTITUTE FOR SMART GOVERNMENT ON BEHALF OF

THE GOVERNMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

Ministry of Digital Economy

BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS

Volume 02 of 03 - Annexure 11: Overview of Technology

Two Stage Bidding Procedure

FOR THE

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

INVITATION FOR BIDS No: NISG/SLUDI-2025

June, 2025
Amended- January, 2026

Table of Contents

1. Introduction 4
2. Solution Overview 5
2.1. Reference Functional Architecture 5
2.2. Design Principles 5
2.3. Solution Framework and Description of Building Blocks 7
2.4. Framework for MOSIP Solution 13
2.5. Framework for Biometric Solution 16
2.6. Data Retention and Encryption 32
2.7. Authentication 32
3. Software Solution Requirements 33
3.1. MOSIP 33
3.2. Business Intelligence and Analytics 34
3.3. Customer Relationship Management 36
3.4. Document Management System (DMS) 39
3.5. Identity and Access Management 39
3.6. Automated Biometric Identification System 40
3.7. Web Portal 42
4. Infrastructure Functional Requirements 55
4.1. Indicative Architecture for Virtualized platform 55
4.2. Indicative Container platform and Security Solution Architecture 56
4.3. Indicative Security framework/Architecture 58
4.4. Latest and Proven Technologies by MSI 58
4.5. Indicative Overall DC/DR Architecture - Bird's Eye View 60
4.6. Indicative Zoning 64

Table of Tables

Table 1:Components of SL-UDI Software System 8
Table 2: Components of SL-UDI-Data Store 9
Table 3: SL-UDI DS 11
Table 4: SL-UDI Software System 11
Table 5: Guiding Factors for Biometric Solution 22
Note: Table 6:licenses 26
Table 7: Usage of Biometric Solution in SL-UDI Information System 29
Table 8: Mobile Application 47

Table of Figures

Figure 1: Overall SL-UDI 4
Figure 2: Reference Functional Architecture 5
Figure 3: functional architecture of MOSIP 15
Figure 4: Indicative Architecture for Virtualized platform 55
Figure 5: DC Site 56
Figure 6: Indicative Container platform and Security Solution Architecture Diagram 57
Figure 7: Indicative Security framework/Architecture 58
Figure 8:Indicative Overall DC Architecture - Bird's Eye View 60
Figure 9: Indicative Overall DC/DR Architecture - Bird's Eye View 61

1. Introduction

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

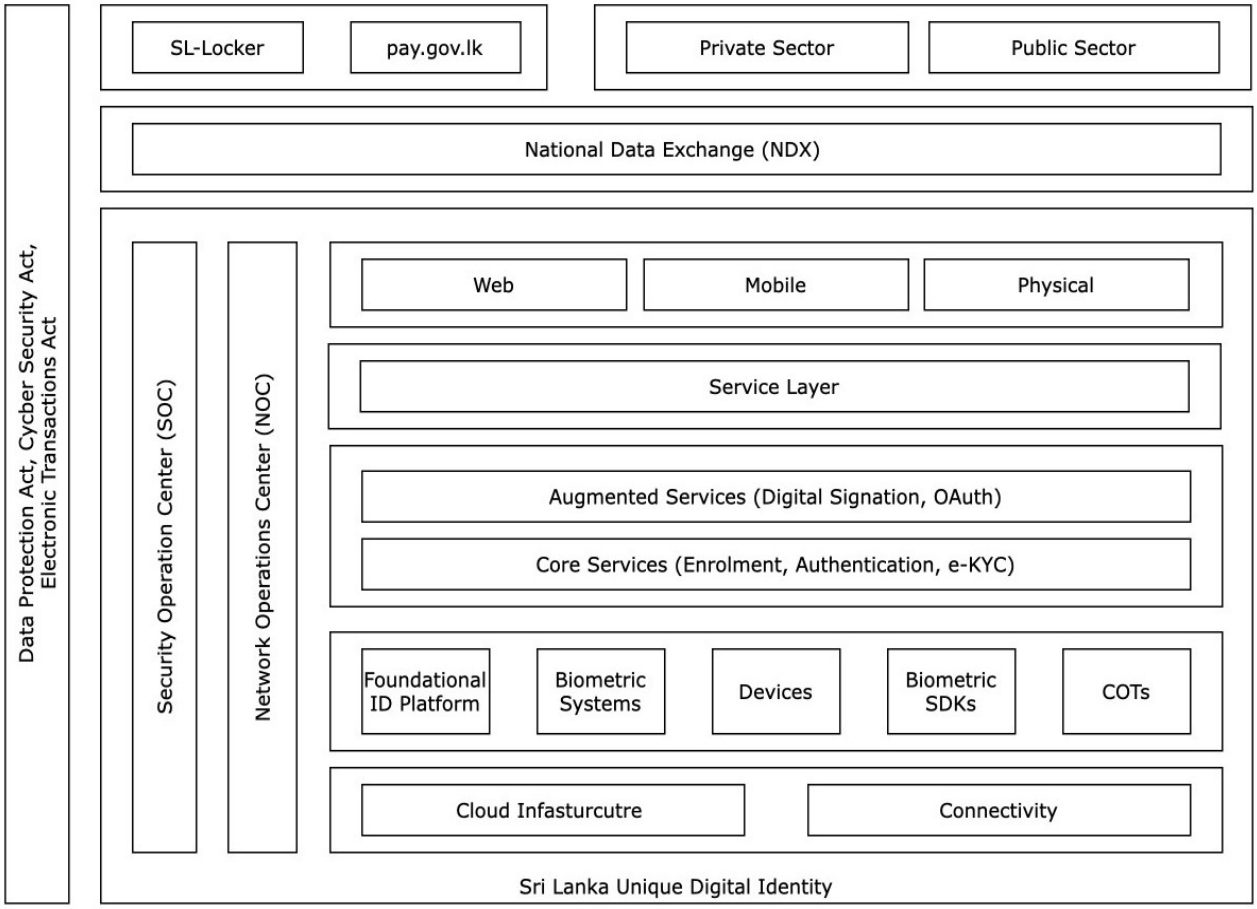


Figure 1: Overall SL-UDI

2. Solution Overview

2.1. Reference Functional Architecture

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

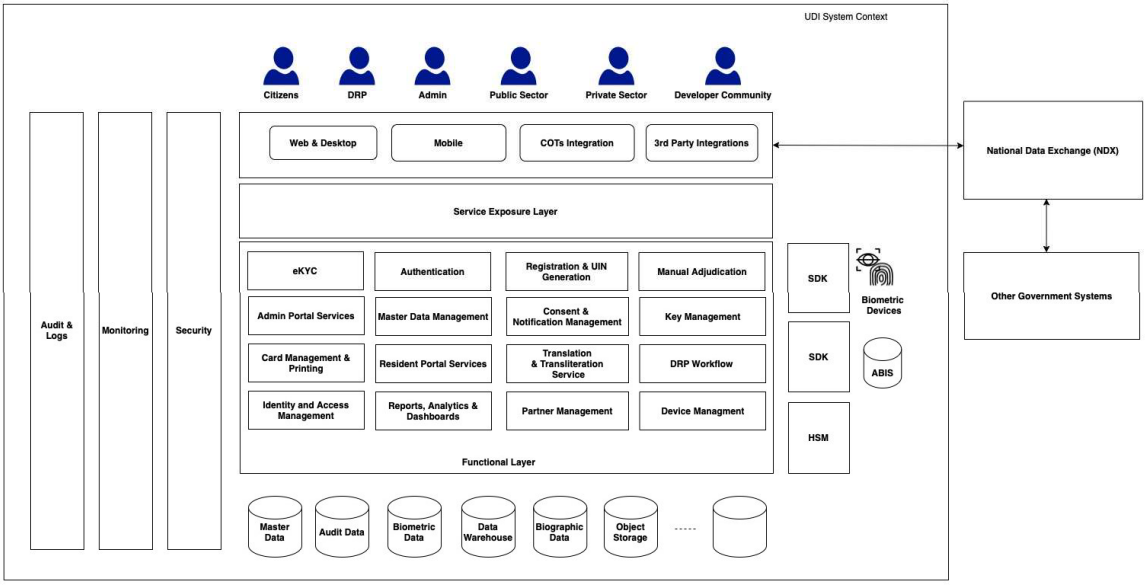


Figure 2: Reference Functional Architecture

2.2. Design Principles

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

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

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

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

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

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

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

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

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

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

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

2.3. Solution Framework and Description of Building Blocks

2.3.1 SL-UDI Software System

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

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

Key Components	MOSIP	Biometric Solution Provider	MSI - Bespoke Application	MSI - COTS Application
19. TSP and UA Software (Three sample applications – One in J2EE, one in JAVA script and one in .Net)			Y	
20. Enterprise Management System				Y

Table 1:Components of SL-UDI Software System

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

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

The SL-UDI-DS would form the backend of the SL-UDI System and would consist of among others the following (the key components are mentioned here in) :

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

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

Table 2: Components of SL-UDI-Data Store

Above table is an “indicative” list. MSI needs to provide additional hardware and software components as per the proposed solution requirements. For more details, please refer to the scope of work.

2.3.3 SL-UDI-DS Operations

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

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

Table 3: SL-UDI DS

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

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

2.3.4 Software Lifecycle Management and Release Management

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

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

Table 4: SL-UDI Software System

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

2.3.5 Solution Integration

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

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

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

portal.

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

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

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

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

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

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

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

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

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

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

2.4. Framework for MOSIP Solution

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

2.4.1 Guiding Principles

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.4.2 Components of MOSIP

i. MOSIP application suite shall comprise of the following applications which will have to be customized and integrated with other components by the MSI:
   a. **Pre-Enrolment Application**: This application shall allow the residents to submit pre-enrolment information through a web-based portal or mobile app interface and obtain appointment at enrolment centers.

b. **Enrolment Software:** This application shall be hosted on a Desktop/Laptop of the Enrolment Officer and will be used for enrolment of the citizen. The Enrolment Officers would login using the SL-UDI number and their own biometrics. With regard to citizen enrolment, through this software, the Enrolment Office will fetch the pre- enrolment information (wherever applicable), enter remaining demographic information, scan supporting documents, capture photograph and biometrics (all fingerprints and both iris), fetch the photograph taken from the Studios. Citizen information once captured would be stored in the desktop/laptop in an encrypted format for onward transmission to SL-UDI-DS in a secure format.

c. **Identity Management System**: This application shall receive the enrolment packet and process it in a sequential staged manner from the validation of the packet, Verification activities by the Department of Registration of Persons, to the generation of SL-UDI number and intimation of the SL-UDI to the citizen. This application shall contain a management and a core layer. The management layer will orchestrate requests, and the core layer will host the business logic.

d. **SL-UDI Generator:** The unique identity numbers to be allocated in the SL-UDI system would be sourced from the SL-UDI generator. Thus, every successful transaction confirmed from all stages will be assigned a unique number from this generator.

e. **Authentication Solution:** This software application shall provide online authentication and e-KYC services. **The** core functions of authentication solution shall include the following:
   i) An extractor which extracts the biometric templates for newly enrolled residents and stores in a citizen database. The citizen database would be used for biometric based authentications.
   ii) The biometric matcher shall compare on 1:1 matching the biometric templates received as part of a biometric authentication request with the biometric template of citizen stored in citizen database after enrolment.
   iii) A set of open APIs for different types of authentications (Demographic, Biometric and OTP).
   iv) A cached OTP retained and deemed valid for designated time period. Authentication requests would come to this application through an array of Trusted Service Providers (TSP) and User Agencies (UA).

f. **Partner and Device Management:** The Partner and Device management application would **cater** to the needs of the partner community, which includes the Trusted Service Providers, User Agencies and Enrolment Centers.
   i) Administration and User Management of Enrolment Community: The application would allow Administrators to setup new users as Enrolment officers by allotting them a unique Number. This application would also allow the setup of Enrolment centers and manage the lifecycle of these centers.
   ii) View Statistics and KPI's for Enrolment Community: This application would provide the **capability** to view statistics related to enrolment at various enrolment centers such as time taken for enrolment, number of enrolment packets that failed from an enrolment center/ enrolment officer, etc.
   iii) Administration and User Management of TSPs and UAs: The application would allow **administrators** to setup new users as TSP/UAs along with their credentials etc. This would **allow** for registration of devices, services permitted (w.r.t. limited e-

KYC).

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

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

g. **Integration Methodology :** Data exchange between the SL-UDI Information System and other **Internal**/External Systems will be carried out through APIs. The MSI, in consultation with GoSL, will also be required to set up a process for issuance of standards for the SL-UDI Information System APIs. The MSI needs to set up, operationalize and maintain system for APIs. **The MSI shall be entirely responsible for customization of the solution which satisfies all features, functions and performance requirements as captured during requirements gathering stage and as described in RFP and relevant documents**.

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

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

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

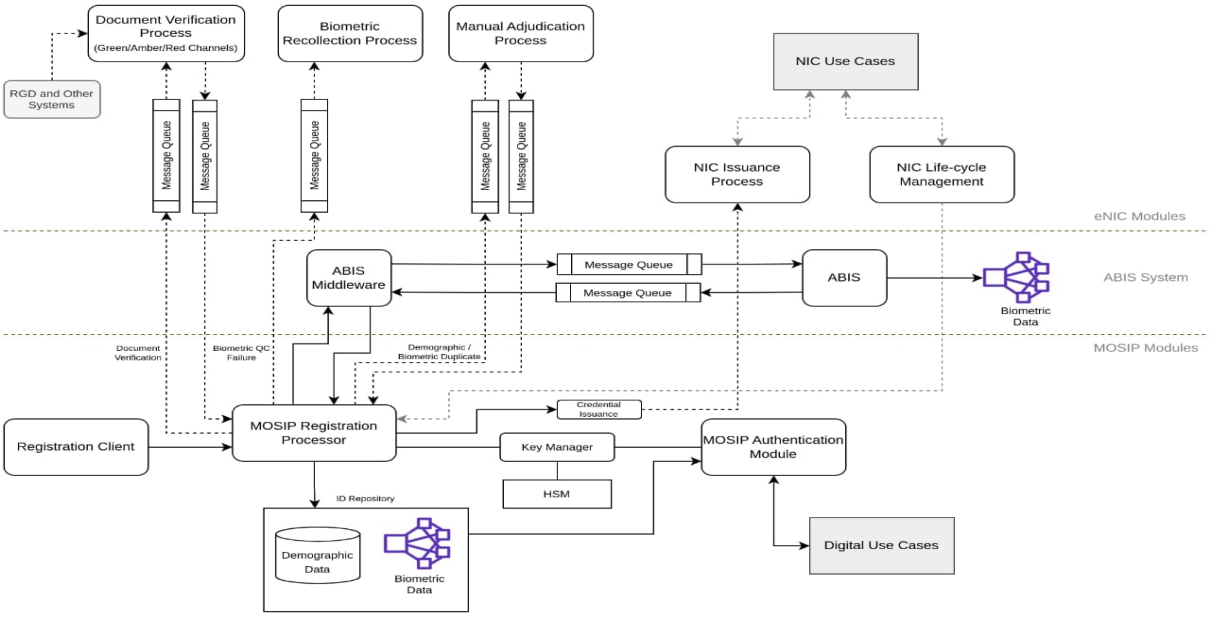


Figure 3: functional architecture of MOSIP

iv. The MOSIP, as far as possible, is built on free and open-source components. The Technology

Stack of MOSIP is provided on its website (https://docs.mosip.io/platform/architecture/mosip-architecture/technology-stack).

v. MSI shall work with International Institute of Information Technology, Bangalore (IIIT Bangalore), India to provide architecture, design specifications, drawings, performance benchmark, etc. as per SL-UDI requirements.

vi. The MOSIP software (long term version) can be downloaded from MOSIP website. This software needs to be customized as per the requirements of the Sri Lanka Unique Digital Identity program.

2.5. Framework for Biometric Solution

2.5.1 Guiding Principles

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

1. With regard to slap fingerprints, search outcome should not be impacted by inversion of thumb placement.
2. Iris images will be automatically labelled by the capture device as left or right and therefore this label may be used to restrict iris searches for de-duplication.
3. ABIS system should not restrict the search on the basis of demographics (gender, age, location) initially, but this capability should be preserved for potential insertion at a later stage in the program.
4. Face photo image enhancement at the enrolment software may include cropping and rotation but must not include non-reversible grey-level alterations (i.e., pose and illumination normalization).
5. The ABIS system must create a record in the reference database whenever SL-UDI Application invokes INSERT method regardless of biometric image quality.
6. With the growth of the database, MSI ~~<Nominated agency>~~ may require the BSP to enhance or replace algorithm. The ABIS should be structured to allow for replacement, enhancement, or insertion of new algorithm.
7. De-duplication flow over multiple modalities can be chosen by the BSP. However, GoSL ~~<Nominated agency>~~ may upon review of results, may require that MSI must perform de-duplication on all (fingerprint, iris, and face) modalities fully.
8. Authorizations for all requests will be verified at the SL-UDI application level. Therefore, all requests sent by the SL-UDI application to the ABIS can be assumed to be from an authorized source.
9. During enrolment as well as authentication, the biometric capture devices of various OEM's will be utilized. These biometric devices will be compliant to the defined biometric standards (Section 2.5.3). The biometric solution should be device agnostic i.e., should operate properly with biometric capture devices, of different OEMs, meeting the aforementioned biometric standards.

2.5.2 Biometric Solution Design Principles

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

1. **Modularity**: The design must allow for replacement and updating of various components, from various partners, without any impact on the other components. The components in this context should be as fine grained as possible. For example, the enrolment server and authentication server are fully decoupled and will use separate database and could use different matcher.

2. **Standards**: Use of standards prescribed by GoSL is mandatory. All interfaces to the outside systems must be based on current industry standards adopted by GoSL for maximum interoperability. Use of open source also aids in standardization.

3. **Avoidance of MSI lock-in**: In the area of biometrics, proprietary algorithms and data representation are perhaps required to achieve performance and accuracy requirements of the GoSL. The system is designed such that these algorithms and data representation form a part of the black box, **and the entire box or a sub-system can be r**eplaced without any impact on the other biometrics black boxes. All proprietary data formats needed within each solution are not exposed outside of the black box.

4. **Resident Convenience**: The entire process of enrolment and authentication must be conducted with strict conformance to quality and precision. At the same time, the process will provide transparency, flexibility, and convenience to the residents. For example, the collection of biometric features will have user interface that is consistent with these requirements.

5. **Risk Mitigation**: Sri Lanka is proposing to undertake biometric collection of the entire population and biometric authentication for service delivery. As the quality and availability of biometric measures across the population is currently not known, alternate methods for de-duplication and fallback strategy must be incorporated in the design to ensure quality.

6. **Universality:** To support scalability and inclusiveness of the solution, three biometric profiles will be collected fingerprint, face, and iris. Fingerprint will be all 10-fingerprints, Iris images will be collected in pairs and facial image will be full frontal.

7. **Security:** Biometric Solution must be secure and conform to Government of Sri Lanka's data security and GoSL's security guidelines, including encryption and decryption. For example, all personal information stored on a permanent storage media must be encrypted.

8. **Enrolment data quality:** The quality of data depends on enrolment process and technology. GoSL will use best practices for enrolment process and utilize optimum technology to capture best quality of data while ensuring that no one is denied enrolment due to poor biometric data. A number of techniques such as operator enrolment and verification of enrollee's biometric against all registered operators and supervisors will be performed at the enrolment station.

9. **Service Oriented Architecture:** The biometric components follow SOA principles. They provide specific services using well defined interfaces.

10. **Isolation -** ABIS will not have access and should not try to access any network resources except the resources referenced by the URLs provided through the API.

11. **DBMS –** The DBMS should be compatible with RDBMS of SL-UDI application and should be able to import/export data with ease

12. **Distributed Database** – Solution should provide distributed database for the purpose of authentication.

2.5.3 Biometric Standards

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

2.5.4 Biometric Solution Architecture Requirements

Given below is the biometric architecture requirement.

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

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

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

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

Table 5: Guiding Factors for Biometric Solution

The key functionalities of biometric solution are as follows:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.5.5 Biometric Solution Components

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

2.5.5.1. Automated Biometric Identification System (ABIS)

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

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

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

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

2.5.5.2. Multimodal SDKs for Server and Client

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

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

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

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

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

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

SDK Client Side	SDK Server Side
enrolment kit, the representative of the BSP will be informed about the identity of enrolment kits (original as well as new one). The BSP should provide updated license, if necessary, for SDK free of charge.	• In case MSI wishes to add more servers to meet the volumes, the representative of the BSP will be informed about the details of additional servers. The BSP should provide updated license, if necessary, for SDK free of charge.

Note : Refer to MOSIP website and documentation for latest versions of Java and other components to meet the compatibility requirements.

2.5.5.3. Biometric Middleware

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

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

2.5.5.4. Resident Data Store (Authentication Repository)

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

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

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

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

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

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

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

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

2.5.5.5. Manual Adjudication Solution

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

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

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

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

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

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

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

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

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

Table 6: Usage of Biometric Solution in SL-UDI Information System

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

2.5.5.7. Enrolment Data Capture

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

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

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

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

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

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

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

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

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

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

2.5.5.8. Biometric Deduplication and update of Resident Data Store

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

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

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

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

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

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

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

For deduplication the following guidelines will be applicable:

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

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

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

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

2.5.5.9. Authentication Solution

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

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

authentication solution will integrate with reference database.

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

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

For authentication the following guidelines will be applicable:

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

2.5.5.10. Biometric System Monitoring & Analysis

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

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

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

2.5.5.11. Manual Adjudication

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

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

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

2.6. Data Retention and Encryption

2.6.1 Data Retention

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

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

2.6.2 Data Encryption

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

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

2.7. Authentication

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

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

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

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

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

3. Software Solution Requirements

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

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

The description of these solutions is provided below:

3.1. MOSIP

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

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

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

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

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

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

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

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

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

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

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

b) Enrolment Data (Iris Image)

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

c) Enrolment Data (Face Image)

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

3.2. Business Intelligence and Analytics

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

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

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

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

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

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

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

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

The key functionalities of the application are provided below:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.3. Customer Relationship Management

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

The MSI's scope of work includes:

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

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

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

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

5) MSI shall be responsible for operations, maintenance, and support of CRM solution as part of

the Application Maintenance and Annual Technical Support from OEM including associated updates and upgrades.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

21) The solution should support call routing functionalities.

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

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

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

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

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

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

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

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

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

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

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

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

The key functionalities of the application are provided below:

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

period.

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

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

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

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

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

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

3.4. Document Management System (DMS)

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

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

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

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

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

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

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

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

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

3.5. Identity and Access Management

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

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

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

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

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

3.6. Automated Biometric Identification System

The key functionalities of the application are provided below:

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

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

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

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

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

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

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

8. **Biometric Matching Engine –** ABIS would provide a biometric matching engine to compare

the generated biometric templates with the ones existing in the ABIS gallery.

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

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

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

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

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

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

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

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

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

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

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

3.7. Web Portal

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

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

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

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

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

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

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

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

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

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

d) Mobile Application

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

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

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

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

S. No.	Functions	Requirements
		be scanned by the client. To get the consent of the user in sharing data, a popup will be appearing.
		• This predefined QR code can be utilized as login credentials to acquire other necessary government services.
12.	**My Profile - Track My Request**	• The option will allow the users to track their requests which were made through the application.
		• An option to create a new request which directs the user to the e-services section.
13.	**My Profile - Settings**	• The users will be able to update their preferred languages. (Sinhala, English)
		• Settings will provide the option to enable and disable authentication modes.
14.	**My Profile - My History**	• Users will have the ability to access all the historical transactions made through the application.
15.	**E-Services Section**	• Two separate sections will be available for Government Services and Private Sector Services
		• Integrated Private or Government Services will be listed under each tile
		• The users are able to search necessary government departments and add them as a tile
		• Based on the security sensitivity of the services, user Authentication with UDI is required. (example: if the user request service for police report, re authentication is popup)
16.	**My Requests**	• This option will display all the services which require the user to act upon.
		• User authentication with the UDI is required based on the security sensitivity of the services. o Simple authentication request o Request digitally stored documents (Digi locker)
		• In a scenario where the user wants to submit information along with documents in the Digi locker, the users will have to enter their UDI in the necessary website. After the UDI is entered a popup will be displayed to take the consent to share this information.
		• Open requests tab: The tab will display all the open requests. Which user wants to take actions on

S. No.	Functions	Requirements
		• Rejected requests tab: Tab to display rejected requests.
		• Approved requests: This will display all the approved requests.
17.	**Support Center**	• Chatbot tab: The chatbot option is available for the user to communicate with the system virtually.
		• FAQ tab: In order to find solutions for the frequently raised questions, the user can refer to this.
		• Email Option: The user is able to send mails through this option when needed.

Table 7: Mobile Application

e) Knowledge Management System (KMS)

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

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

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

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

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

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

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

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

f) Learning Management System (LMS)

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

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

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

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

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

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

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

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

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

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

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

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

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

g) Mobile Application

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(xii) Should provide Role Based Access control.

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

(xiv) Should support in-device authentication

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

1. Access to SL-UDI Mobile Portal

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

2. Loading Page

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

3. Binding Device with the Mobile Application

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

3.2. **Application reinstall (new device):** In case of changing the device, the user is obligated to reinstall

the app which requires the re- binding process. This, however, exempts the app-update process. In case of re-installing the app in the existing device, the rebinding process can be exempted.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. Simple and User-Friendly Landing Page

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

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

6. Basic application Component

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

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

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

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

7. My Profile View

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

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

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

8. My Profile - Edit My Profile

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

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

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

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

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

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

9.4. Define validity period for the Virtual ID.

10. My Profile - Display e-UDI

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

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

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

11. My Profile - QR code generation

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

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

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

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

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

12. My Profile - Track My Request

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

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

13. My Profile - Settings

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

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

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

14. E-Services Section

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

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

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

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

15. My Requests

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

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

- Simple authentication request
- Request digitally stored documents

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

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

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

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

16. Support Center

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

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

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

h) Citizen Portal

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

i) Service Billing System

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

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

features:

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

b. Support billing for G2C and G2B scenarios

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

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

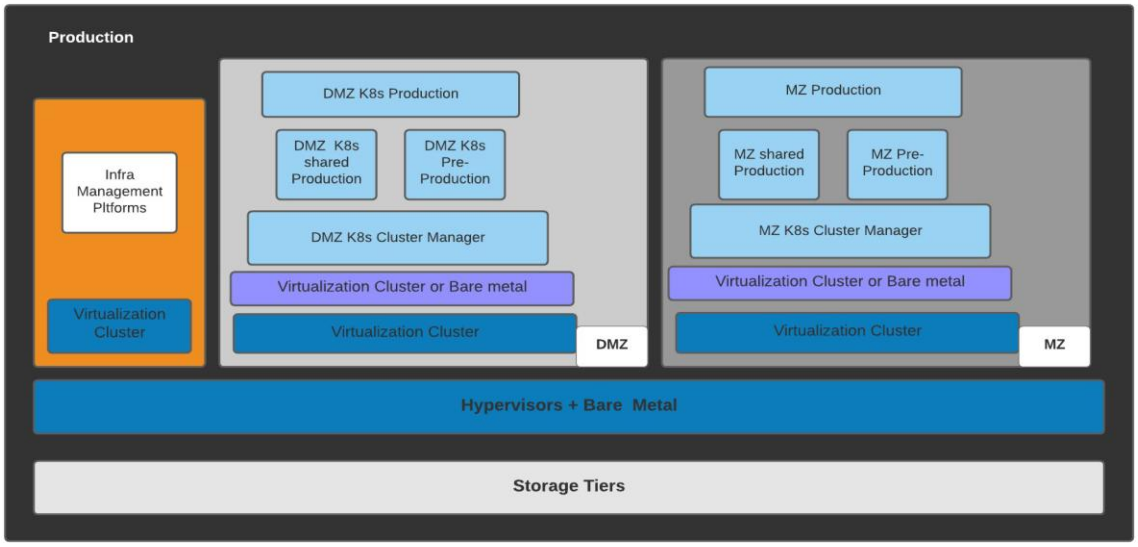
e. Should support create payment transaction records, record an audit trail of all actions, payment refund, payment status tracking, etc.

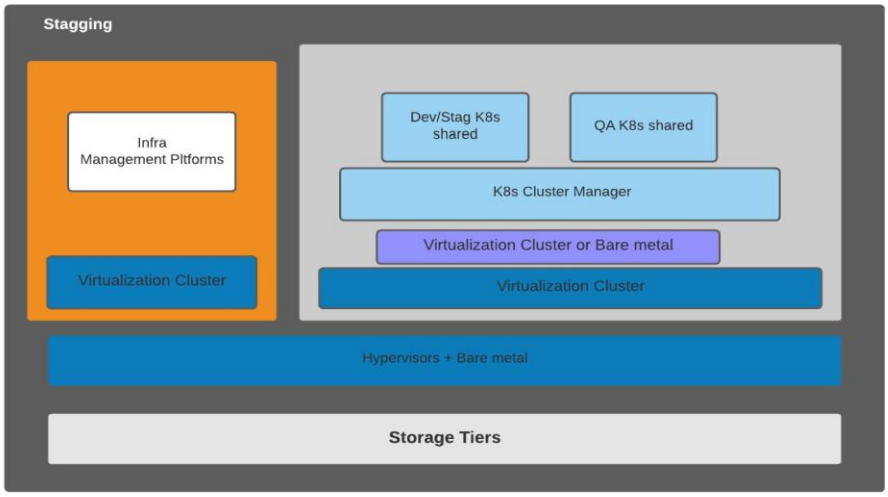
4. Infrastructure Functional Requirements

4.1. Indicative Architecture for Virtualized platform

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

Figure 4: Indicative Architecture for Virtualized platform





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

Multi storage tiers to be used in underline storage infrastructure in order to cater to general IOPS and higher IOPS workload requirements. Separate management cluster to be deployed and production MZ and DMZ zones to be segregated. Inter-zone workload communications shall strictly through firewall cluster. This should also include a highly- available administrative console for management of the

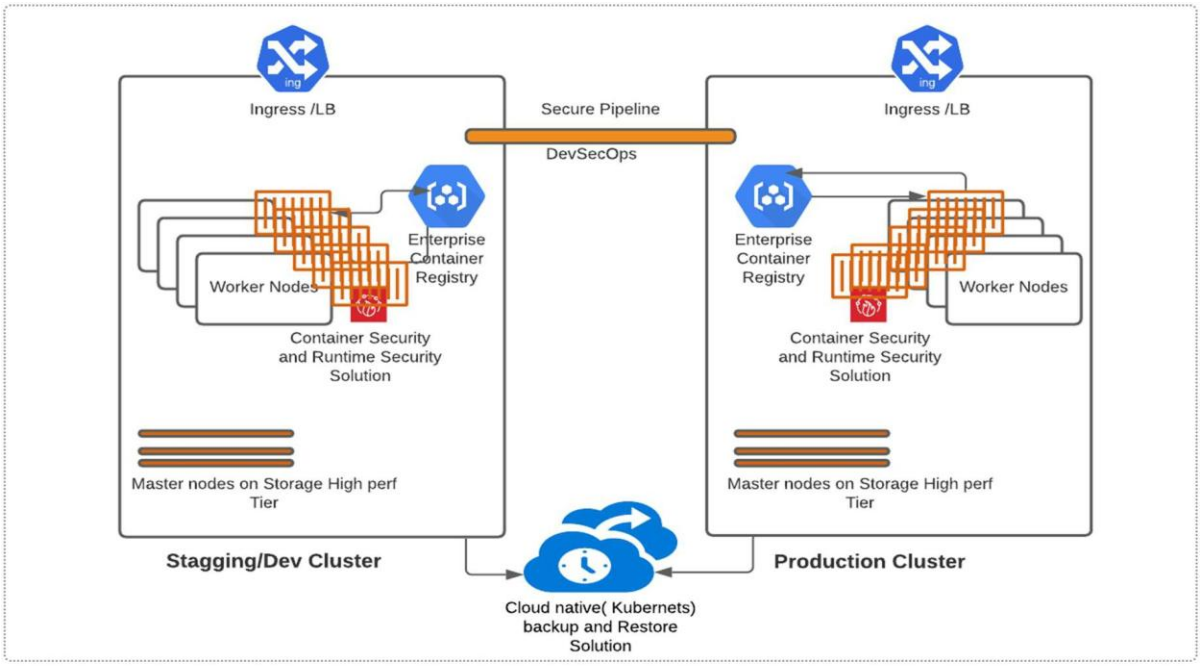
virtual data center platform to conduct activities such as onboarding/managing/updating hosts, virtual machines, storage, and networks. Provide the ability to hot-add CPU and memory and hot-plug disks and NICs (provided the same is supported by the guest operating system).

Refer to Annex 3: Virtualization Platform and subsections of specification

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

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

4.2. Indicative Container platform and Security Solution Architecture



DC Site

Figure 5: DC Site

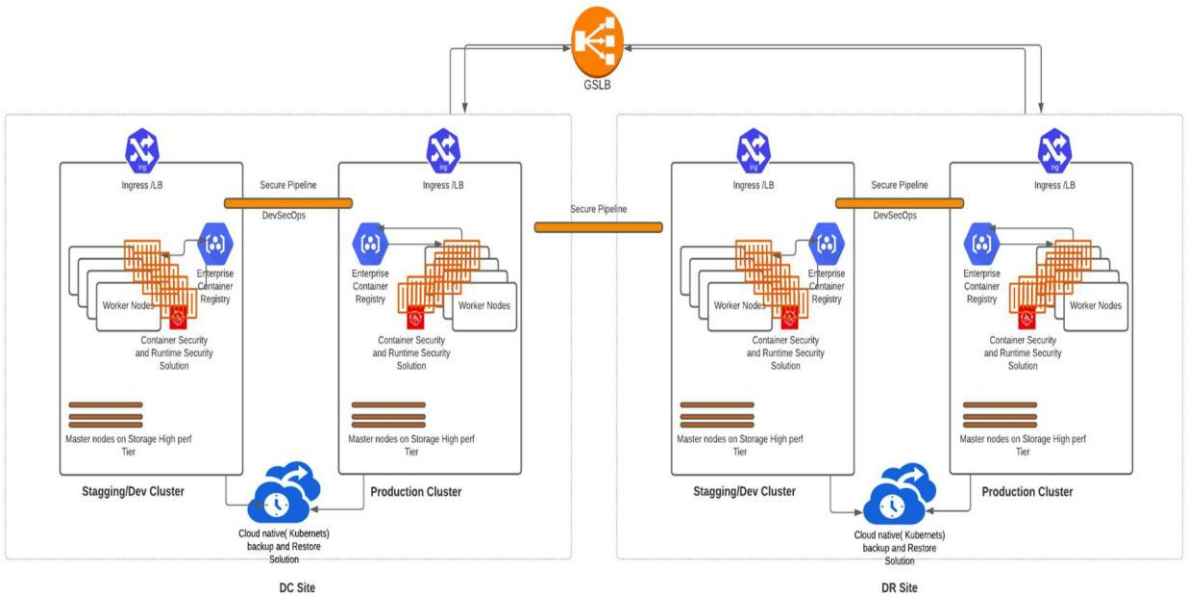


Figure 6: Indicative Container platform and Security Solution Architecture Diagram

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

4.3. Indicative Security framework/Architecture

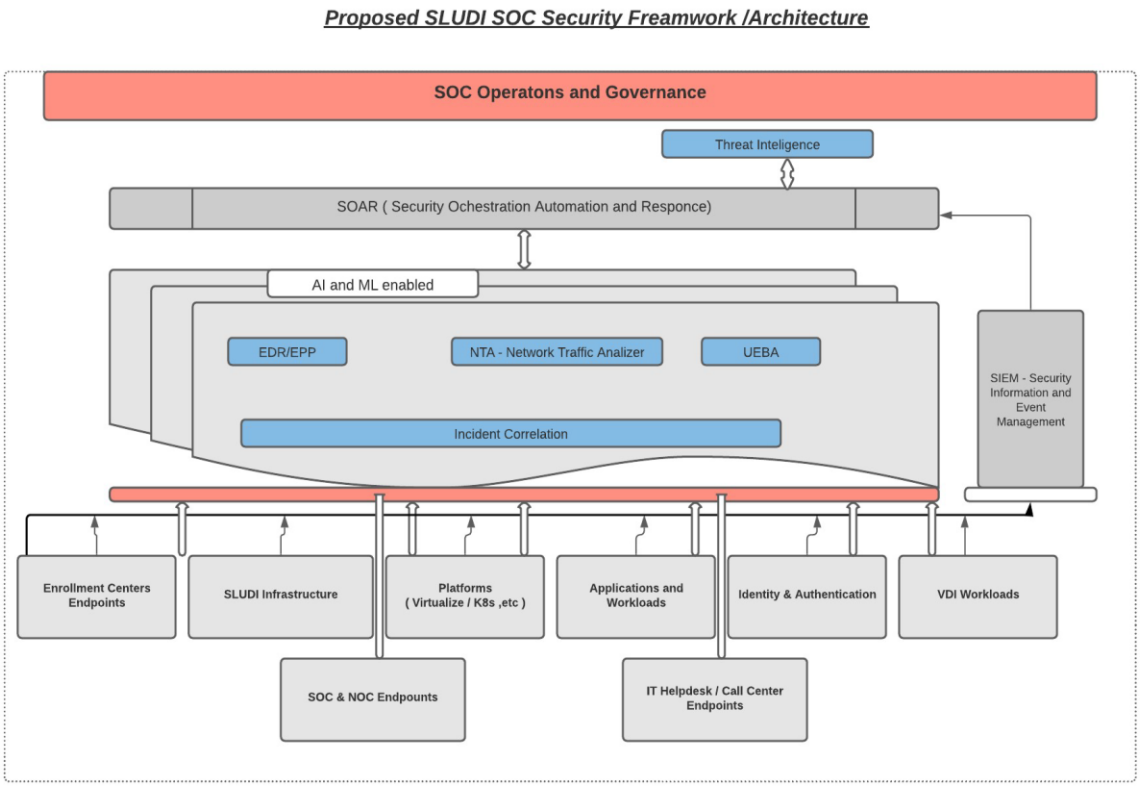


Figure 7: Indicative Security framework/Architecture

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

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

4.4. Latest and Proven Technologies by MSI

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

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

b) **Security Information and Event Monitoring (SIEM)**: To get full visibility of the infrastructure via logs. Provides enterprises with network security intelligence and real- time monitoring for network devices, systems, and applications. SIEM shall be deployed and integrated with all systems in the SL-UDI program such as servers, databases, network devices, applications etc. Monitoring rules and correlation rules shall be developed to ensure that real time alerts are generated and shall be monitored. Solution deployment shall be capable of developing correlation rules across sites such as between DC and DR. Configuration, integration and rule review shall be performed as per the defined SLA.

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

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

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

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

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

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

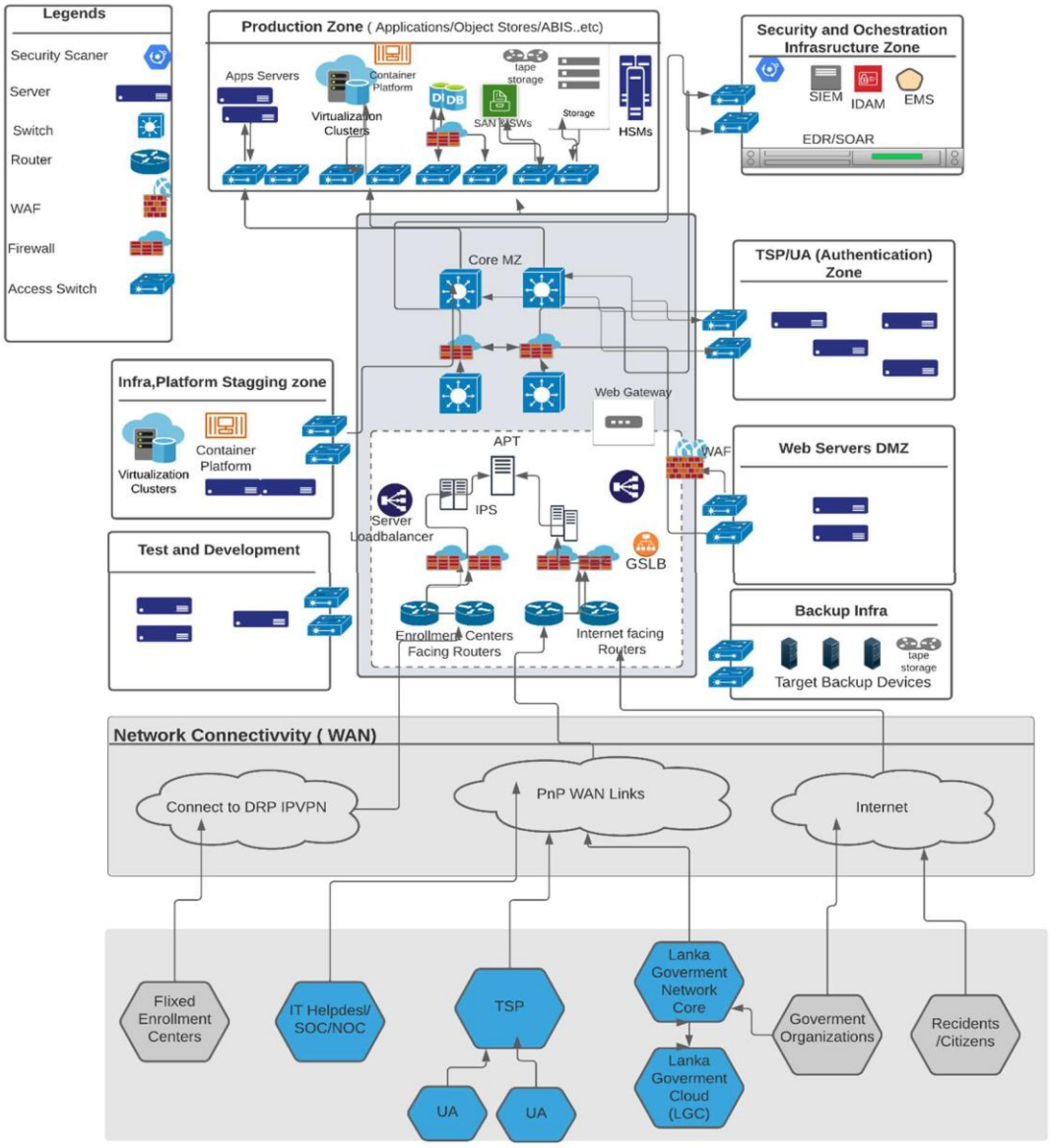


Figure 8:Indicative Overall DC Architecture - Bird's Eye View

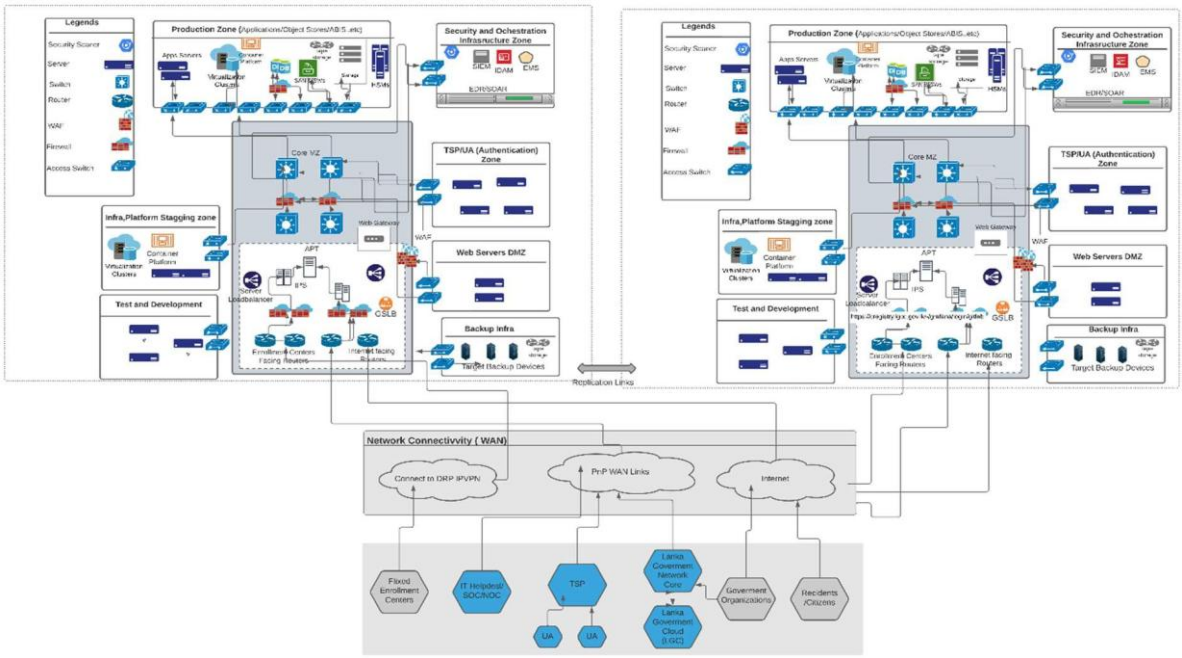


Figure 9: Indicative Overall DC/DR Architecture - Bird's Eye View

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

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

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

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

(Refer Annex 3 : Minimum Technical Specification)

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

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

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

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

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

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

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

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

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

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

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

~~files etc.~~

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

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

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

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

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

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

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

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

s) **Anti-Advanced Persistent Threats (Anti-APT)**: Advanced Persistent Threat Protection solution. Anti-APT solution shall be deployed for the network, endpoints etc. as per specifications. All network traffic shall go through the Anti-APT solution and shall be analyzed for

malwares/malicious software etc. The deployment, configuration etc. shall be reviewed on a periodic basis as per the SLAs.

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

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

4.6. Indicative Zoning

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

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

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

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

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

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

   Management zone only) after Firewall and other security measures.

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

   Access to infrastructure hosted in this zone:

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

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

   Access to infrastructure hosted in this zone

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

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

   Access to infrastructure hosted in this zone

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

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

   Access to infrastructure hosted in this zone

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

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

   Access to infrastructure hosted in this zone

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

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

   Access to infrastructure hosted in this zone

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

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

   Access to infrastructure hosted in this zone

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

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

NATIONAL INSTITUTE FOR SMART GOVERNMENT ON BEHALF OF

THE GOVERNMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

Ministry of Digital Economy

BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS

Volume 02 of 03 - Annexure 12: Project Sites

Two Stage Bidding Procedure

FOR THE

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

INVITATION FOR BIDS No: NISG/SLUDI-2025

June, 2025
Amended: January, 2026

Table of Contents

12.1. Project Sites..... 3

12.2. List of Registration Centers 4

12.1. Project Sites

S. No.	District	DS Name
1	ICTA Premises	Colombo
2	DRP Head Office	Colombo
3	DRP Regional Offices	Kurunegala
		Galle
		Vavunia
		Batticaloa
		Nuwara Eliya
4	Data Center Location – Primary	GoSL's responsibility
5	Offsite Back up	Would be Informed to the selected bidder
6	DR site	GoSL's responsibility
7	NOC/SOC	To be Informed to the selected bidder
8	IT Help Desk	To be Informed to the selected bidder
9	Project Governance	To be Informed to the selected bidder
10	Device Storage Location	To be Informed to the selected bidder

12.2. List of Registration Centers

S. No.	District	DS Name
1	Ampara	Pothuvil
2	Ampara	Kalmunai
3	Ampara	Kalmunai Tamil Division
4	Ampara	Addalachchenai
5	Ampara	Damana
6	Ampara	Dehiattakandiya
7	Ampara	Uhana
8	Ampara	Akkaraipattu
9	Ampara	Ninthavur
10	Ampara	Thirukkovil
11	Ampara	Sainthamaruthu
12	Ampara	Sammanthurai
13	Ampara	Alayadiwembu
14	Ampara	Ampara
15	Ampara	Mahaoya
16	Ampara	Lahugala
17	Ampara	Padiyathalawa
18	Ampara	Navithanveli
19	Ampara	Karaitheevu
20	Ampara	Irakkamam
21	Anuradhapura	Thambuttegama
22	Anuradhapura	Nuwaragam Palatha Central
23	Anuradhapura	Nochchiyagama
24	Anuradhapura	Nuwaragam Palatha East
25	Anuradhapura	Thirappane
26	Anuradhapura	Ipalogama
27	Anuradhapura	Kahatagasdigiliya
28	Anuradhapura	Thalawa
29	Anuradhapura	Kekirawa
30	Anuradhapura	Nachchadoowa
31	Anuradhapura	Rambewa
32	Anuradhapura	Galenbindunuwewa
33	Anuradhapura	Mihinthale
34	Anuradhapura	Galnewa
35	Anuradhapura	Medawachchiya
36	Anuradhapura	Horowpothana
37	Anuradhapura	Rajanganaya
38	Anuradhapura	Padaviya
39	Anuradhapura	Palagala
40	Anuradhapura	Mahavilachchiya

S. No.	District	DS Name
41	Anuradhapura	Kebithigollewa
42	Anuradhapura	Palugaswewa
43	Badulla	Badulla
44	Badulla	Bandarawela
45	Badulla	Mahiyanganaya
46	Badulla	Lunugala
47	Badulla	Rideemaliyadda
48	Badulla	Haputale
49	Badulla	Passara
50	Badulla	Haldummulla
51	Badulla	Uva Paranagama
52	Badulla	Hali-Ela
53	Badulla	Welimada
54	Badulla	Kandaketiya
55	Badulla	Ella
56	Badulla	Soranathota
57	Badulla	Meegahakivula
58	Batticaloa	Manmunai Pattu (Araipattai)
59	Batticaloa	Manmunai South & Eruvil Pattu
60	Batticaloa	Manmunai West
61	Batticaloa	Eravur Pattu
62	Batticaloa	Kattankudy
63	Batticaloa	Manmunai South-West
64	Batticaloa	Koralai Pattu South (Kiran)
65	Batticaloa	Porativu Pattu
66	Batticaloa	Eravur Town
67	Batticaloa	Koralai Pattu Central
68	Batticaloa	Manmunai North
69	Batticaloa	Koralai Pattu (Valachchenai)
70	Batticaloa	Koralai Pattu West (Oddamavadi)
71	Batticaloa	Koralai Pattu North (Vaharai)
72	Colombo	Sri Jayawardanapura Kotte
73	Colombo	Seethawaka
74	Colombo	Kolonnawa
75	Colombo	kaduwela
76	Colombo	Dehiwala
77	Colombo	Maharagama
78	Colombo	Thimbirigasyaya
79	Colombo	Colombo
80	Colombo	Moratuwa
81	Colombo	Ratmalana
82	Colombo	Padukka

S. No.	District	DS Name
83	Colombo	Kesbewa
84	Colombo	Homagama
85	Galle	Habaraduwa
86	Galle	Bope-Poddala
87	Galle	Welivitiya-Divithura
88	Galle	Karandeniya
89	Galle	Benthota
90	Galle	Neluwa
91	Galle	Hikkaduwa
92	Galle	Ambalangoda
93	Galle	Galle Four Gravets
94	Galle	Niyagama
95	Galle	Akmeemana
96	Galle	Yakkalamulla
97	Galle	Balapitiya
98	Galle	Imaduwa
99	Galle	Baddegama
100	Galle	Elpitiya
101	Galle	Nagoda
102	Galle	Thawalama
103	Galle	Gonapeenuwala
104	Galle	Rathgama
105	Galle	Wanduramba
106	Galle	Madampagama
107	Gampaha	Mahara
108	Gampaha	Divulapitiya
109	Gampaha	Mirigama
110	Gampaha	Dompe
111	Gampaha	Wattala
112	Gampaha	Ja-Ela
113	Gampaha	Negombo
114	Gampaha	Attanagalla
115	Gampaha	Minuwangoda
116	Gampaha	Kelaniya
117	Gampaha	Gampaha
118	Gampaha	Biyagama
119	Gampaha	Katana
120	Hambantota	Sooriyawewa
121	Hambantota	Walasmulla
122	Hambantota	Lunugamvehera
123	Hambantota	Weeraketiya
124	Hambantota	Ambalantota

S. No.	District	DS Name
125	Hambantota	Tangalle
126	Hambantota	Angunakolapelessa
127	Hambantota	Thissamaharama
128	Hambantota	Beliatta
129	Hambantota	Katuwana
130	Hambantota	Hambantota
131	Hambantota	Okewela
132	Jaffna	Valikamam East (Kopay)
133	Jaffna	Valikamam South -West (Sandilipay)
134	Jaffna	Jaffna
135	Jaffna	Valikamam North
136	Jaffna	Nallur
137	Jaffna	Vadamaradchi North (Point Pedro)
138	Jaffna	Vadamaradchi South-west (Karaveddy)
139	Jaffna	Thenmaradchi (Chavakachcheri)
140	Jaffna	Valikamam West (Chankanai)
141	Jaffna	Valikamam South (Uduvil)
142	Jaffna	Island North (Kayts)
143	Jaffna	Karainagar
144	Jaffna	Island South (Velanai)
145	Jaffna	Delft
146	Jaffna	Vadamaradchi East
147	Kalutara	Millaniya
148	Kalutara	Dodangoda
149	Kalutara	Horana
150	Kalutara	Beruwala
151	Kalutara	Palindanuwara
152	Kalutara	Mathugama
153	Kalutara	Agalawatta
154	Kalutara	Panadura
155	Kalutara	Bandaragama
156	Kalutara	Madurawala
157	Kalutara	Kalutara
158	Kalutara	Bulathsinhala
159	Kalutara	Ingiriya
160	Kalutara	Walallavita
161	Kandy	Hatharaliyadda
162	Kandy	Minipe
163	Kandy	Delthota
164	Kandy	Medadumbara
165	Kandy	Thumpane
166	Kandy	Doluwa

S. No.	District	DS Name
167	Kandy	Pathahewaheta
168	Kandy	Akurana
169	Kandy	Pasbage Korale
170	Kandy	Udapalatha
171	Kandy	Poojapitiya
172	Kandy	Panvila
173	Kandy	Harispattuwa
174	Kandy	Kandy Four Gravets & Gangawata Korale
175	Kandy	Udunuwara
176	Kandy	Pathadumbara
177	Kandy	Kundasale
178	Kandy	Yatinuwara
179	Kandy	Ganga Ihala Korale
180	Kandy	Udadumbara
181	Kegalle	Rambukkana
182	Kegalle	Kegalle
183	Kegalle	Yatiyanthota
184	Kegalle	Dehiovita
185	Kegalle	Aranayaka
186	Kegalle	Warakapola
187	Kegalle	Bulathkohupitiya
188	Kegalle	Deraniyagala
189	Kegalle	Mawanella
190	Kegalle	Galigamuwa
191	Kegalle	Ruwanwella
192	Kilinochchi	Karachchi
193	Kilinochchi	Kandavalai
194	Kilinochchi	Pachchilaipalli
195	Kilinochchi	Poonakary
196	Kurunegala	Galgamuwa
197	Kurunegala	Pannala
198	Kurunegala	Polpithigama
199	Kurunegala	Kuliyapitiya East
200	Kurunegala	Ududbaddawa
201	Kurunegala	Mallawapitiya
202	Kurunegala	Ibbagamuwa
203	Kurunegala	Giribawa
204	Kurunegala	Wariyapola
205	Kurunegala	Bingiriya
206	Kurunegala	Nikaweratiya
207	Kurunegala	Ganewatta

S. No.	District	DS Name
208	Kurunegala	Kurunegala
209	Kurunegala	Bamunakotuwa
210	Kurunegala	Kuliyapitiya West
211	Kurunegala	Narammala
212	Kurunegala	Kobeigane
213	Kurunegala	Ehetuwewa
214	Kurunegala	Weerambugedara
215	Kurunegala	Maspotha
216	Kurunegala	Maho
217	Kurunegala	Polgahawela
218	Kurunegala	Alawwa
219	Kurunegala	Mawathagama
220	Kurunegala	Panduwasnuwara East
221	Kurunegala	Rideegama
222	Kurunegala	Ambanpola
223	Kurunegala	Panduwasnuwara West
224	Kurunegala	Kotavehera
225	Kurunegala	Rasnayakapura
226	Mannar	Mannar Town
227	Mannar	Musalai
228	Mannar	Madhu
229	Mannar	Nanaddan
230	Mannar	Manthai West
231	Matale	Naula
232	Matale	Yatawatta
233	Matale	Rattota
234	Matale	Pallepola
235	Matale	Dambulla
236	Matale	Wilgamuwa
237	Matale	Galewela
238	Matale	Ukuwela
239	Matale	Matale
240	Matale	Ambanganga Korale
241	Matale	Laggala-Pallegama
242	Matara	Hakmana
243	Matara	Akuressa
244	Matara	Kamburupitiya
245	Matara	Kotapola
246	Matara	Welipitiya
247	Matara	Pitabeddara
248	Matara	Weligama
249	Matara	Mulatiyana

S. No.	District	DS Name
250	Matara	Pasgoda
251	Matara	Devinuwara
252	Matara	Malimbada
253	Matara	Thihagoda
254	Matara	Dickwella
255	Matara	Matara Four Gravets
256	Matara	Athuraliya
257	Matara	Kirinda Puhulwella
258	Monaragala	Madulla
259	Monaragala	Buttala
260	Monaragala	Sevanagala
261	Monaragala	Siyambalanduwa
262	Monaragala	Badalkumbura
263	Monaragala	Bibile
264	Monaragala	Moneragala
265	Monaragala	Wellawaya
266	Monaragala	Thanamalvila
267	Monaragala	Medagama
268	Monaragala	Katharagama
269	Mullaitivu	Maritimepattu
270	Mullaitivu	Puthukudiyiruppu
271	Mullaitivu	Thunukkai
272	Mullaitivu	Welioya
273	Mullaitivu	Manthai East
274	Mullaitivu	Oddusuddan
275	Nuwaraeliya	Nuwara Eliya
276	Nuwaraeliya	Walapane
277	Nuwaraeliya	Ambagamuwa
278	Nuwaraeliya	Kothmale East
279	Nuwaraeliya	Hanguranketha
280	Nuwaraeliya	Norwood
281	Nuwaraeliya	Kothmale West (Thispane)
282	Nuwaraeliya	Nildandahinna
283	Nuwaraeliya	Thalawakele
284	Nuwaraeliya	Mathurata
285	Polonnaruwa	Welikanda
286	Polonnaruwa	Thamankaduwa
287	Polonnaruwa	Dimbulagala
288	Polonnaruwa	Lankapura
289	Polonnaruwa	Elahera
290	Polonnaruwa	Medirigiriya
291	Polonnaruwa	Hingurakgoda

S. No.	District	DS Name
292	Puttalam	Dankotuwa
293	Puttalam	Puttalam
294	Puttalam	Chilaw
295	Puttalam	Nattandiya
296	Puttalam	Mahawewa
297	Puttalam	Arachchikattuwa
298	Puttalam	Madampe
299	Puttalam	Anamaduwa
300	Puttalam	Wennappuwa
301	Puttalam	Kalpitiya
302	Puttalam	Mundel
303	Puttalam	Pallama
304	Puttalam	Karuwalagaswewa
305	Puttalam	Mahakumbukkadawala
306	Puttalam	Vanathavilluwa
307	Puttalam	Nawagattegama
308	Ratnapura	Weligepola
309	Ratnapura	Ayagama
310	Ratnapura	Kalawana
311	Ratnapura	Eheliyagoda
312	Ratnapura	Nivithigala
313	Ratnapura	Elapatha
314	Ratnapura	Imbulpe
315	Ratnapura	Pelmadulla
316	Ratnapura	Balangoda
317	Ratnapura	Kalthota
318	Ratnapura	Opanayaka
319	Ratnapura	Embilipitiya
320	Ratnapura	Ratnapura
321	Ratnapura	Kolonna
322	Ratnapura	Kuruvita
323	Ratnapura	Kiriella
324	Ratnapura	Godakawela
325	Ratnapura	Kahawatta
326	Trincomalee	Trincomalee Town and Gravets
327	Trincomalee	Kuchchaveli
328	Trincomalee	Muttur
329	Trincomalee	Thambalagamuwa
330	Trincomalee	Kantalai
331	Trincomalee	Kinniya
332	Trincomalee	Verugal (Echchilampattu)
333	Trincomalee	Morawewa

S. No.	District	DS Name
334	Trincomalee	Gomarankadawala
335	Trincomalee	Seruvila
336	Trincomalee	Padavi Sri Pura
337	Vavuniya	Vavuniya
338	Vavuniya	Vengalacheddikulam
339	Vavuniya	Vavuniya North
340	Vavuniya	Vavuniya South

NATIONAL INSTITUTE FOR SMART GOVERNMENT ON BEHALF OF

THE GOVERNMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

Ministry of Digital Economy

BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS

Volume 02 of 03 - Annexure 13: Card Printing and Personalization Technology

Two Stage Bidding Procedure

FOR THE

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

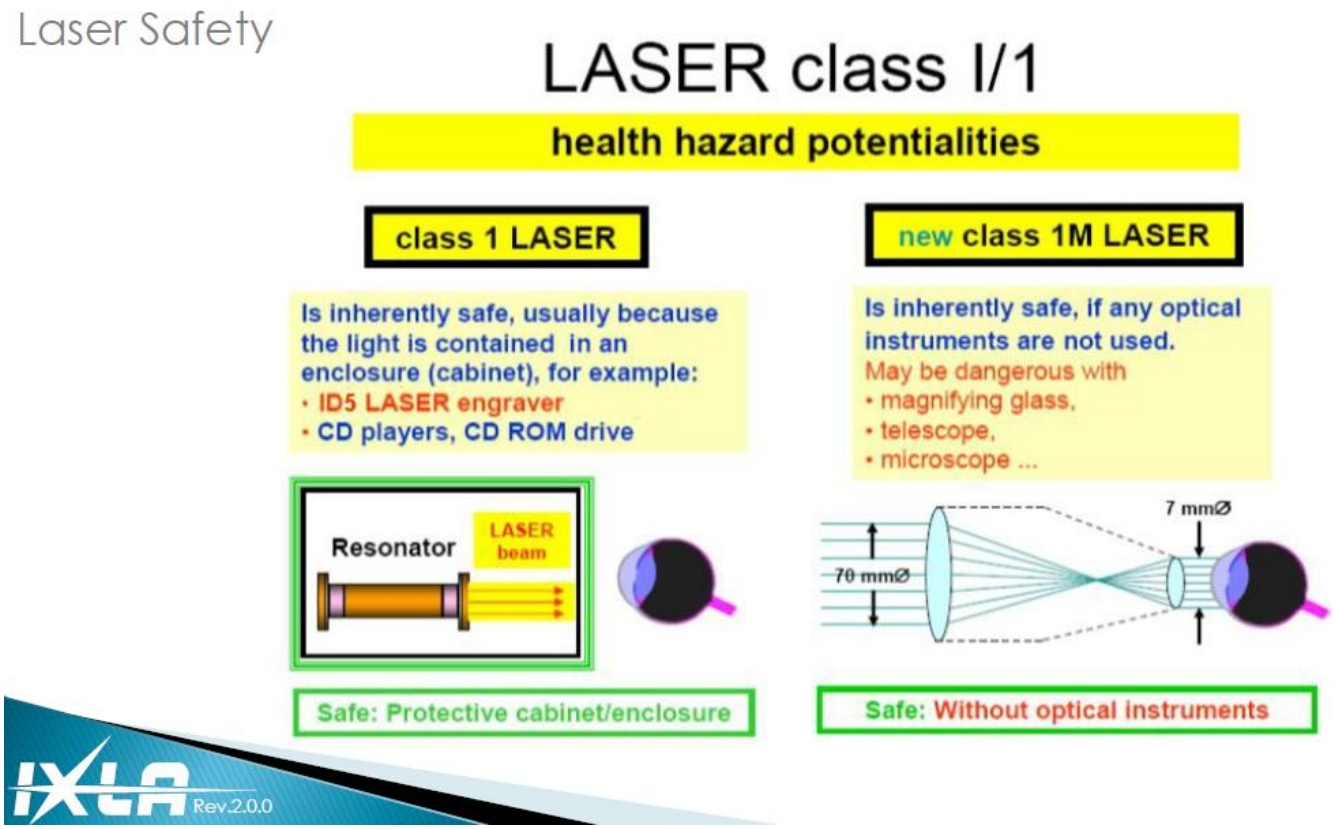
INVITATION FOR BIDS No: NISG/SLUDI-2025

June, 2025
Amended: January 2026

Table of Contents

12.1. Card Printing Personalization Technology 3

12.1. Card Printing Personalization Technology



Laser Safety

LASER class IV/4

health hazard potentialities

class 4 LASER

Very dangerous for eye and skin!
LASERs can burn skin, and in some cases, even scattered light can cause eye and/or skin damage.
The generated LASER inside of the ID5 engraver is a class 4 LASER (continuous wave PM = 100W / 1064 nm)

Secondary hazards of the LASER

- ignition of flammable materials!
- danger of explosion in the area of an explosive atmosphere!

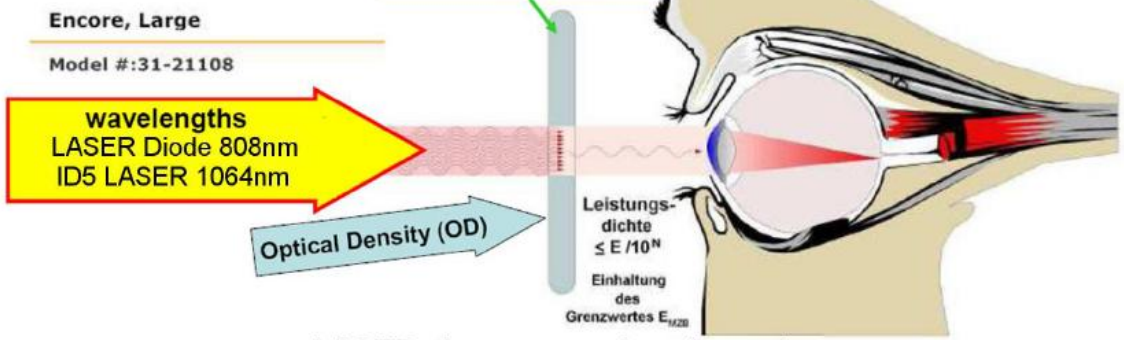
- PVC- cards engraving → generate toxic gas!

IXLA Rev.2.0.0

Laser Safety

Safety goggles (eye glasses) for service:

Eye glass:
- Grade of protection of the filters (OD)
- Wavelength (nm)



LASER classes → reduce hazard

4 → 2 → 1

IXLA Rev.2.0.0

Safety goggles for service

Description: Ga, diodes,Yag, 770-1080nm

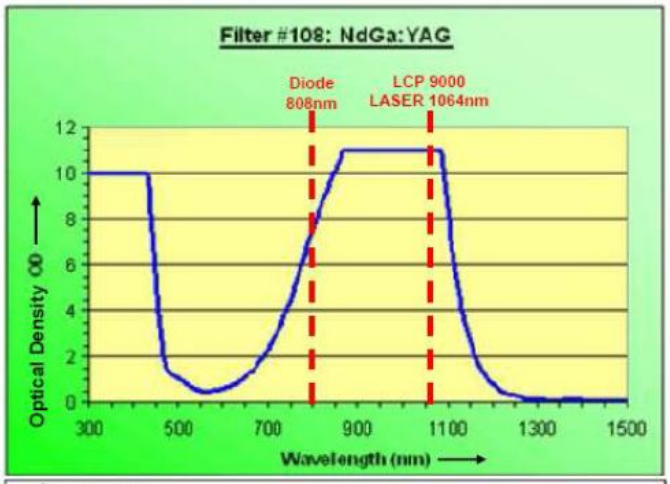
Encore, Large

Model #:31-21108

- Stylish, comfortable OTG spectacle
- Adjustable temple length
- Meets ANSI Z136.1 and European
- EN 207 European Norm

Specifications

OD >9 @ 190-420nm
OD >1 @ 670nm
OD >5 @ 770-810nm
OD >7 @ 810-1100nm
OD >10 @ 1064nm
OD >5 @ 9,000-11,100nm
OD >7 @ 10,600nm



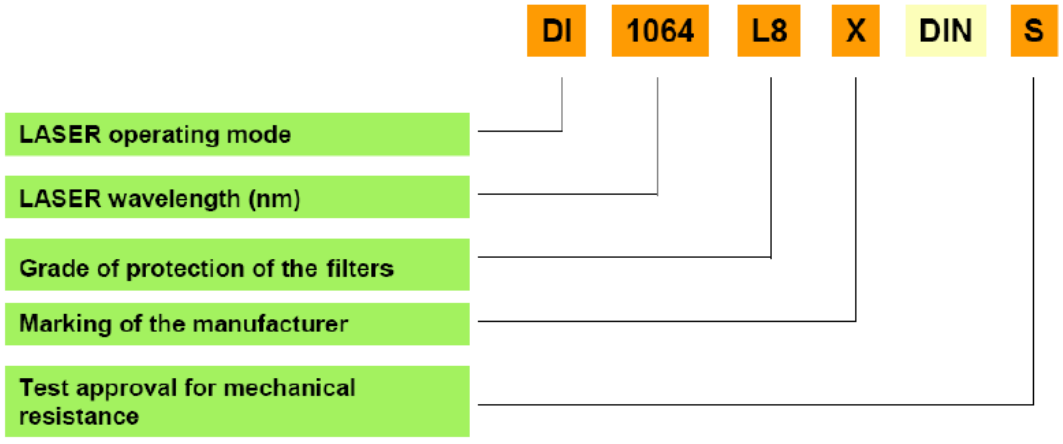
WARNING:
Always ensure that the wavelength(s) listed on your eyewear correspond to the wavelength(s) of the laser being used. Use of this product for protection against wavelength(s) not listed on the eyewear may result in serious personal injury, including blindness.

IXLA Rev.2.0.0

LASER SAFETY GOGGLES

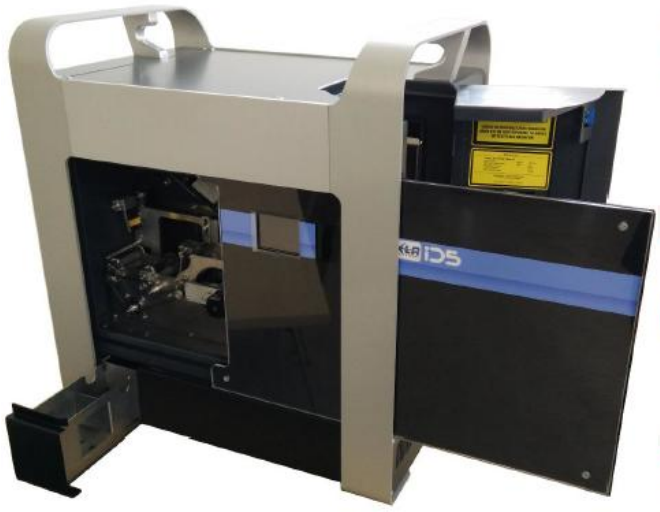
(safety eye glasses)

LASER safety goggles **needs a marking according DIN EN 207.**



IXLA Rev.2.0.0

Laser Safety Interlock



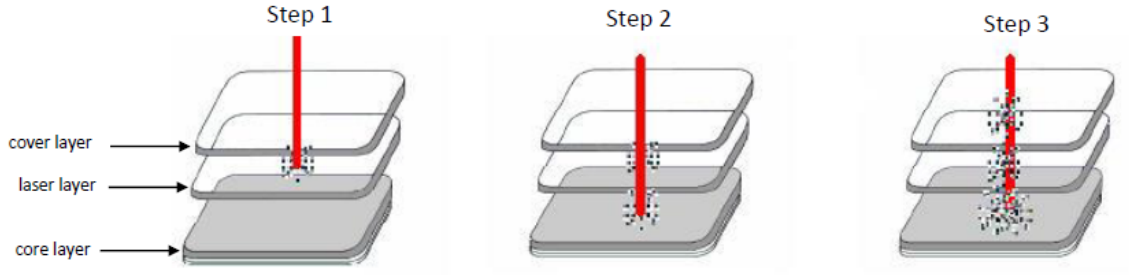
HARD INTERLOCK: this is main emergency interlock that immediatly stops emission. It is a black connector located near the main power button

SOFT INTERLOCK 1: is located behind the main door, if opened it needed a laser reset to restore the standard operativity mode

SOFT INTERLOCK 2: is connected to the reject bin locked by the door, if opened it needed a laser reset to restore the standard operativity mode

IXLA Rev.2.0.0

Laser Engraving in Detail - Polycarbonate with overlay



Step 1: Laser beam passes through clear cover layer with no reaction. Laser beam then hits laser layer. The pigments in this layer react immediately. When the molecules in the receptive layer are hit by a laser beam they change to tiny carbon bubbles. These form the black color.

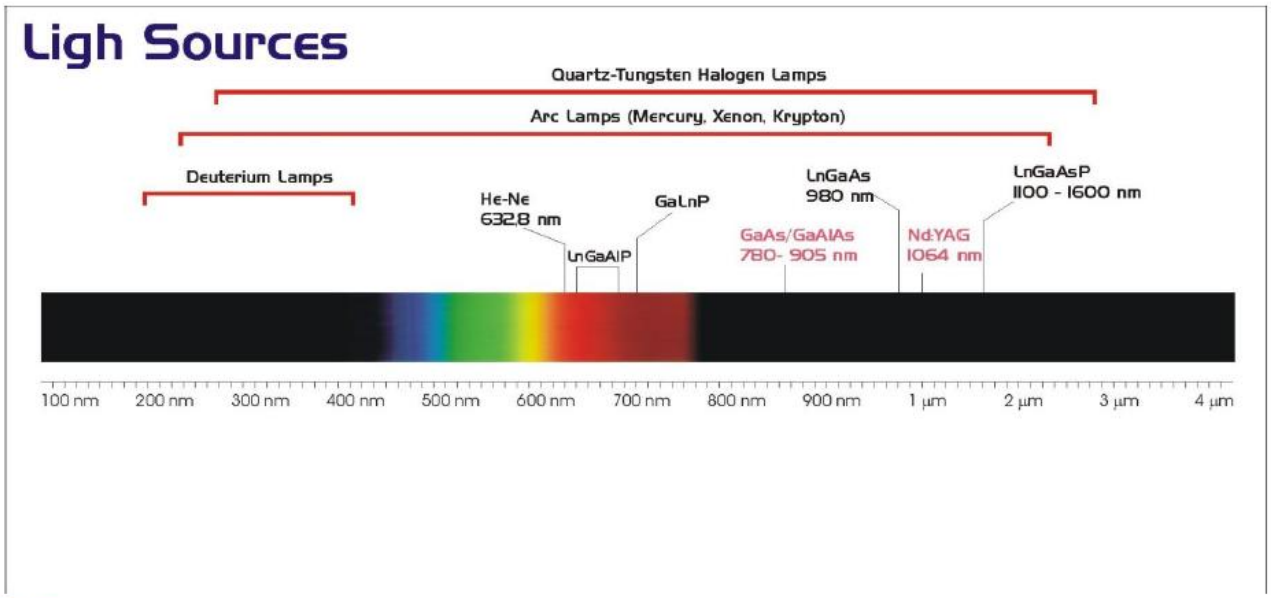
Step 2: Laser beam hits the receptive opaque core layer the material reacts immediately. The interaction between the different materials start;

Step 3: Additional energy is generated by the beam. The material continues to react due to increasing temperature. Pigments from the laser layer melts into the top layer from the reverse side.

Varying the energy levels of the beam can add different security features such as tactile (raised textured) printing. The accuracy of the laser beam is measured in microns thereby resolutions for personalization, and micro-printing of variable information, previously unattainable, are now available.

IXLA Rev.2.0.0

Laser Engraving in Detail



Materials

1. Polycarbonate
2. PVC
3. PET-G
4. ABS
5. Other.

SEE SAMPLES

Engraving Tests: Different Materials

Polycarbonate	Laserable PVC	Others
Best results	Medium results	Material Dependent
Easy mark setup	Complex mark setup	
High efficiency in laser radiation absorption	Less efficiency in laser radiation absorption = heat	
Picture marking is fast and reliable in one pass	Best result if pictures are marked with correct setting of line index step	

IXLA Rev.2.0.0

ID5-20 System Description & Features

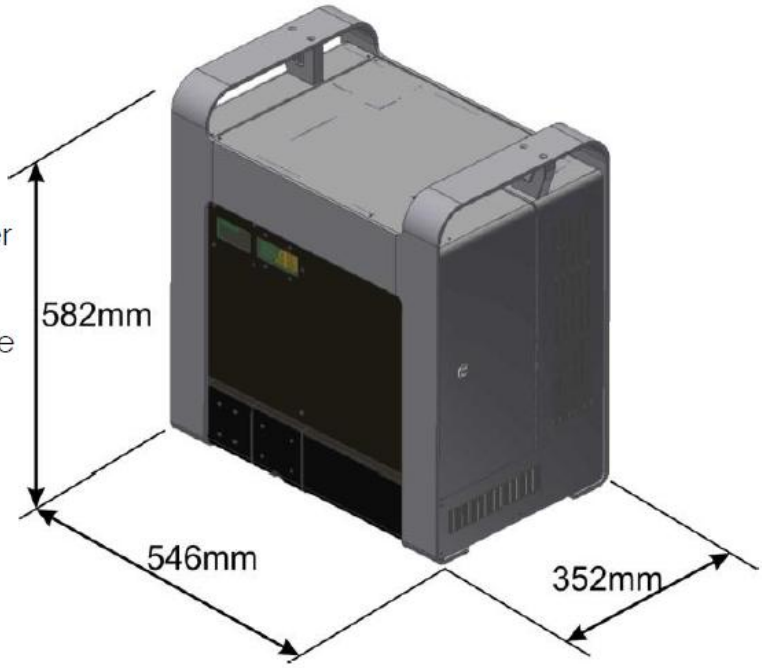
General characteristics:

•Marking
Monochrome laser marking, resolution up to 600 dpi

•Laser Engraving Speed
Up to 200 Plastic card cards per hour laser engraving only, depending on card material, print density and card coverage of print data

•Cards Types
ISO 7810: ABS, PET, and Polycarbonate

•Interface
Ethernet LAN



IXLA Rev.2.0.0

ID5-20 System Description & Features

Environmental conditions

•Working temperature:	min 15°C max 35°C
•Working Humidity:	min 10% max 80% without condensation
•Storage temperature:	min -5°C max 70°C
•Storage Humidity:	min 20% max 70% without condensation
•Cooling:	Air to air (integrated)

Laser

•Laser medium	Nd:YV04
•Wavelength	1064 nm
•Laser Spot	50 um

Power Supply

•Power Supply	90Va.c. to 240Va.c.
•Frequency	50-60 Hz
•Power	300W

MTBF: 2200 Hours
MTTR: 30 minutes

IXLA Rev.2.0.0

ID5-20 cards Personalization Laser System

ID5-20: Laser Engraving System

Options:

- ❑CLI/MLI laser marking
- ❑Internal CHIP - RFID
- ❑Internal Barcode reader
- ❑X/Y Autopositioning
- ❑OCR/OCV

IXLA Rev.2.0.0

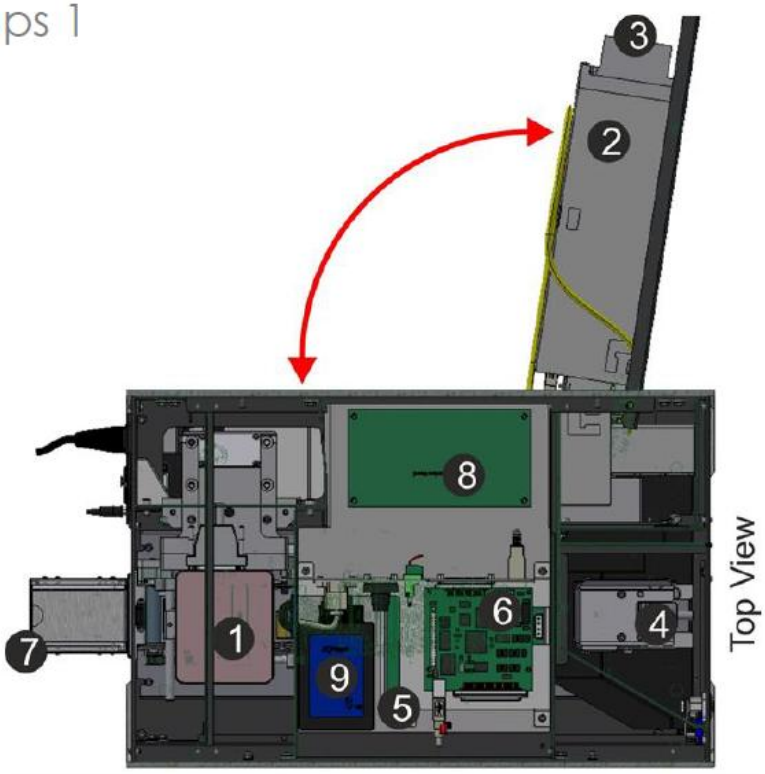
Machine opening

- Using the relative Key. Open door 1 to load 1 card in the stacker
- Pull the front cover on the right side to open the front cover
- Pull out the tray to get the rejected cards

IXLA Rev.2.0.0

Machine Functional Groups 1

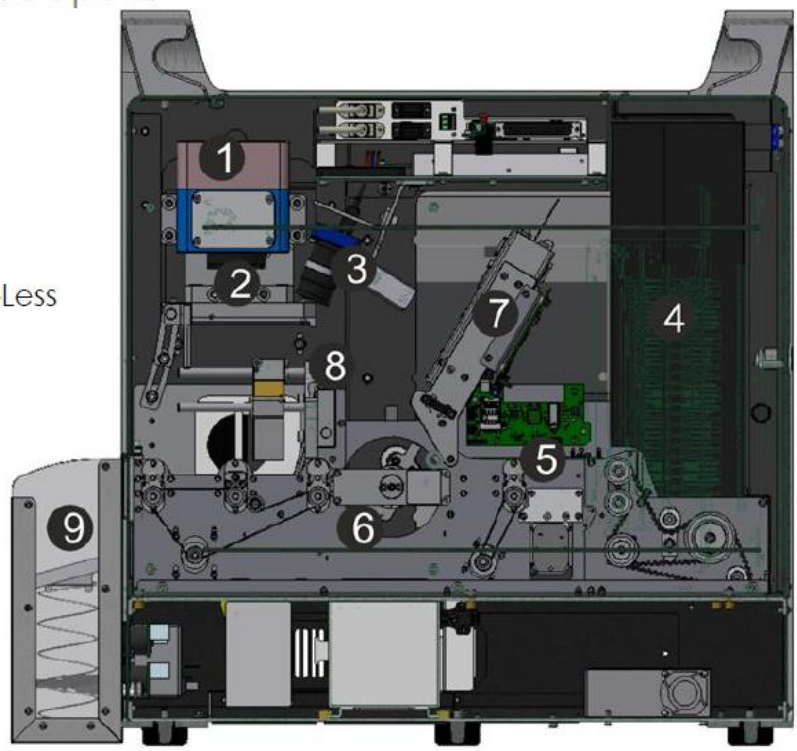
1 Scanner head
2 Laser rack
3 Air cooling
4 Card feeder
5 USC-1 laser controller board
6 Embedded PC
7 Cards output bin
8 Fiber laser interface boards
9 SSD hard disk



IXLA Rev.2.0.0

Machine Functional Groups 2

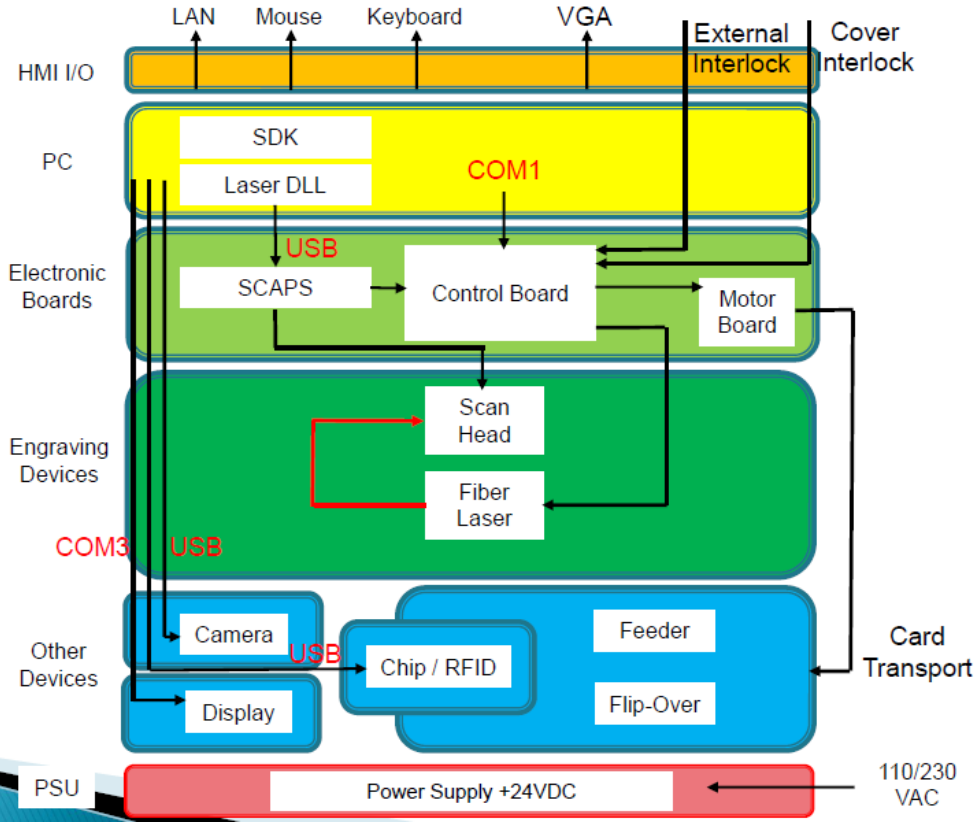
1 Scanner head
2 160mm F-theta lens
3 XY auto positioning kit
4 Card feeder
5 Card Encoder Contact, C-Less
6 Card Flipover
7 Magnetic stripe encoder
8 CLI/MLI Mirrors
9 Cards output bin



Front View

IXLA Rev.2.0.0

Block Diagram



IXLA Rev.2.0.0

NATIONAL INSTITUTE FOR SMART GOVERNMENT ON BEHALF OF

THE GOVERNMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

Ministry of Digital Economy

BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS

Volume 02 of 03 - Annexure 14: List of Indicative Trainings

Two Stage Bidding Procedure

FOR THE

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

INVITATION FOR BIDS No: NISG/SLUDI-2025

June, 2025
Amended: January 2026

Table of Contents

14.1. List of Indicative Trainings 3

14.1. List of Indicative Trainings

S. No.	Type	Domain	Duration per batch	Outcome
1.	Technical Training	Biometrics Solution (To be provided in partnership with Biometric Solution Provider) + Manual Adjudication + Biometric SDK	1 week	Hands on understanding of the ABIS and IDMS, Software Development Kits, its integration and Troubleshooting guidelines
2.		Authentication (To be provided in partnership with Biometric Solution Provider + Authentication Devices)	1 week	Hands on understanding of the Authentication Services, Software Development Kits, and authentication Services
3.		Security (Basic)	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
4.		Security (Advance)	4 weeks	Advanced knowledge of network security architecture, data Centre security, threats and situation management, software security, etc.
5.		Technology	5 days	Database management, network management, virtualization, container platforms, server storage management, back up and replication management
6.		BCP + Data Center Operations	2 days	Awareness on disaster policy, disaster management and BCP, DC and DR Operations
7.		Application (COTS and Bespoke)	5 days	Understanding of application development and maintenance, testing, portals management, user acceptance, release management
8.		MOSIP	5 days	Understanding of MOSIP Components, MOSIP Technology, Functionalities and Features, Support Mechanism, Service Levels, etc.
9.	Support Functions Training	Registration System (Enrolment, Quality Check, Enrolment Devices)	1 week	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.
10.		Contact Centre	3 days	Understanding of Call Logging, Call Forwarding, Call Resolution mechanisms, FAQs, CRM etc.
11.		Technical Helpdesk	2 days	Understanding of call/ticket logging, call/ticket forwarding, and resolution mechanisms, FAQs, etc.

NATIONAL INSTITUTE FOR SMART GOVERNMENT ON BEHALF OF

THE GOVERNMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

Ministry of Digital Economy

BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS

Volume 02 of 03 - Annexure 15: Transition Framework

Two Stage Bidding Procedure

FOR THE

APPOINTMENT OF MASTER SYSTEM INTEGRATOR (MSI) FOR VALIDATION, UPGRADING, IMPLEMENTING AND MAINTINAING THE "UNIQUE DIGITAL IDENTITY (SL-UDI) PROJECT" OF GOVERNMENT OF SRI LANKA

INVITATION FOR BIDS No: NISG/SLUDI-2025

June, 2025
Amended: January , 2026

Table of Contents

1. TRANSITION **3**

1.1 BACKGROUND 3

1.2 TRANSITION FRAMEWORK 3

1.3 ~~TRANSITION PROCESS~~ 6

1.4 CURRENT STATE 6

1.4.1 Transition of MSI to MSP/ GoSL Nominated Agency *7*

1.4.2 This section has been deleted *7*

*1.4.3 Implementation of GoSL Data Centers** *7*

*1.4.4 Implementation of Data Centre IT operations** *7*

*1.4.5 Implementation of IT Help Desk** *7*

1.5 NON-TECHNICAL ASPECTS TRANSITION 7

1.5.1 Transition of Contracts (Termination/takeover/replacement/extension) *7*

1.5.2 Transition of Documentation *8*

1.5.3 Governance *8*

1.6. GUIDELINES FOR KNOWLEDGE TRANSFER 8

1. Transition

This section is to provide guidance to MSI for transitioning of the SL UDI Project to the selected MSP (by GoSL) & interfacing with the required data elements of e-NIC project as per the scope of work.

1.1 Background

The MSI for SL-UDI shall be required to manage various transitions during the tenure of the contract which could be triggered at various milestones during the implementation. The purpose of this section is to provide the broad Transition Framework within which the MSI would be required to validate, build, implement, and operate the MSI's scope of work and the roles and responsibilities of different stakeholders during various transitions.

The purpose of transition is to

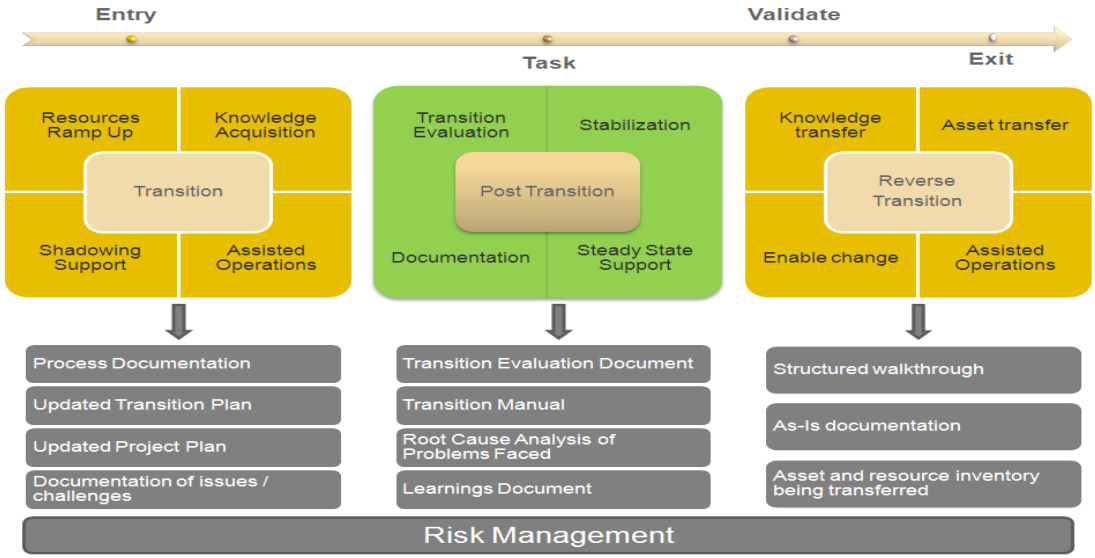
i. Enable MSI to understand existing System and be the single point of responsibility as the Master System Integrator for implementing SL UDI Project services
ii. Enable planned delivery of ~~smooth taker over of~~ SL-UDI project including ~~and~~ other service providers engaged by MSI/ MSP as per the scope of work defined in Volume 2 of this RFP
iii. ~~Help Integration of the existing data & various applications and utilization of the capacity at the GoSL Data Centre and installed Hardware~~.

1.2 Transition framework

The objective of this section is to define generic guidelines about transition methodology for the MSI for effective management of the transition of responsibilities. It is expected that all transition activities shall follow a three-phase approach which will include:

i. Pre-transition phase
ii. Transition phase and
iii. Post transition phase

The deliverables expected out of each transition activity is also depicted in the diagram below.



The three phases - Pre-Transition, Transition and Post Transition are detailed out below.

i. **Pre Transition Phase: Pre-Transition** is broken down into 4 sub phases:

   a. **Scope Definition**: This phase should begin with identification of the resources responsible for carrying out the transition. MSI and the GoSL team will define the scope of the activities It will be MSI's responsibility to manage the transition of activities.

   b. **Study of Existing Operations (As-Is Architecture):** The current operations of DRP, in issuing NICs should be studied and documented. After the study of As–Is architecture, MSI will work out a plan for To-Be architecture. The scope of architecture will be limited to implementation & maintenance of proposed SL UDI solution (such as MOSIP Application, ABIS Solution components and COTs products)

   c. **Transition Planning:** This phase should involve developing transition plan from MSI to MSP for identifying the skill set requirements for each job, deploying team members with requisite skills and developing and fine tuning the knowledge acquisition plans. Initial support and risk management plans are also to be developed during this phase.

   d. **Define Success Criteria**: Finalizing the schedule and quality requirements will be done in this phase. The success criteria for the transition will be defined.

ii. **Transition Phase:** There can be 4 sub phases in the **transition** phase

   a. **Resources Ramp Up**: In this phase, the MSP should acquire the resources that are required to start supporting the operations. The plan for ramp up of resources should be implemented during this stage.

b. **Knowledge Acquisition**: In this phase, MSI should mobilise the core team for knowledge acquisition from GoSL and Knowledge transfer to MSP. GoSL ~~PIA~~ shall provide a detailed walkthrough of Application, Solution Design and Deployment Architecture of any systems related with SL-UDI to MSI Team for the understanding of the existing GoSL process require to issue UDI. . MSI team will then go through the knowledge build-up through discussions, demonstrations and study of existing processes and their alignment to the SL-UDI Program~~. IT infrastructure of DRP (network diagrams, monitoring equipment, databases, etc.) and various processes to be documented (if necessary). During this exercise, PIA and DRP will provide the detailed walkthrough of the source code and all relevant documents.~~

c. **Shadowing Support**: During this phase, each team member of MSP shall observe the activities under his purview done by MSI. In this phase, process application knowledge is built, and hands-on application and infrastructure know-how is acquired by MSP. This knowledge can be documented for future use.

d. **Assisted Operations**: This activity is the reverse of shadowing support where the MSP team members will carry out the activities under the supervision of MSI. A continuous knowledge-gap analysis is performed and the team members can be taken through the knowledge acquisition phase again. At the end of this stage, the MSP team is expected to be ready for transition.

iii. **Post transition phase:** Post transition phase will consist of 3 parts

a. **Steady State Support**: At the start of this phase (post Go Live of SL UDI Solution Implementation) , full-fledged floor operations and quality control will start with planned shifts. Ongoing process improvement programs, reports, reviews, and training programs will be initiated to enable smooth execution of support operations. A continuous quality check is done during the initial stage. Also, MSI teams are regularly involved in identifying opportunities and executing incremental steps aimed at improving performance, while reducing repetitive incidents for higher availability and improved reliability.

b. **Transition Evaluation**: Transition evaluation starts when MSP is able to provide a stable steady-state support for the operations. Transition evaluation can be done on schedule variances, number of incidents reported and the criteria set as per defined SLAs ~~initially~~. A detailed report of root cause analysis and remedial measures shall be created by the MSI as per defined SLAs.

c. **Documentation**: This documentation involves the completion of overall documentation about the processes included under MSP's responsibility. Also, the problems faced during

the transition, their causes, steps taken to resolve and precautionary measures suggested can be documented.

1.3 ~~Transition process~~

~~A transition of legacy system to the modern system comprises of four key elements which are the Current State, Transition Triggers, Transition Process and Future State. The MSI shall be required to define transition process for each area of transition. At a broad level, the transition process of the MSI should comprise of three steps:~~

i. ~~**Step 1:** The MSI would work with the GoSL team/respective Service Provider to create a detailed transition plan covering all the steps and would have this approved by GoSL. In addition, the SME team of the MSI and the respective Service Provider of GoSL will do a knowledge capture of the applications, data, processes, policies and all other activities relevant for the transition. Asset acquisition / transfer of asset is not envisaged presently. If there is a need for asset acquisition/transfer, the MSI will do a due-diligence on the same. The MSI will also identify potential risks and put in place mitigation plans for the same keeping in mind uninterrupted on going services as the goal.~~

ii. ~~**Step 2**: The MSI would work with the respective Service Provider / GoSL to document the processes and procedures, including the system configuration, application configuration, environments, testing, QA and acceptance procedures. The MSI will co-perform the activities of the vendor with respective vendor's supervision (knowledge try-out).~~

iii. ~~**Step 3**: In this phase the MSI will take complete ownership of the assigned responsibilities and will be accountable for the services and the corresponding SLAs defined for the MSI.~~

~~The timeline for the implementation of the various transition steps will be specific to each module which is being transitioned.~~

1.4 Current state

There are multiple vendors managing different components of SL-UDI system.

i. **Data Centre Service Provider ("DCSP"):** Currently there is no data centre or data centre service provider for SL UDI project, GoSL will provide the required Tier 3 Data Centre colocation facility as with the following arrangement.
   a. Racks for IT components – Should be provided by MSI
   b. Power, Cooling, and Building Management System (BMS) – Will be provided by GoSL
   c. Space for the Operations – Will be provided by GoSL DCSP
   d. Network connectivity – Network connectivity till cage will be provided by GoSL
   e. Physical Security – will be provided by GoSL

f. Cyber Security Infrastructure – Should be provided by MSI.

ii. Current Application (eNIC) Interfacing; SLUDI system should access e-NIC system and retrieve applicant's data through secure API which would be exposed by e-NIC and consumed by SLUDI. The SLUDI (MOSIP) relevant module should access this demographic information from eNIC system and auto-populate the relevant fields in MOSIP modules for the applicant. MOSIP relevant module would have features to display, edit the details of the applicant and append (data entry) the empty columns. **Exception:** When data is not available in e-NIC system and hence not retrievable , SL, then the relevant module of SLUDI (MOSIP) should have the functionality to insert applicant data directly from the MOSIP UX (User Interface).

1.4.1 Transition of MSI to MSP/ GoSL Nominated Agency

i. Transition of MSI activities would be done to MSP/GoSL nominated agency as per scope of work defined in Vol 2 of this RFP.

ii. MSP would also follow the proposed Transition framework (section 1.2) of this document and would shadow the MSI to build knowledge base from day of inception of the SL UDI project.

iii. MSP will take part in the QA activities as auditing for the Release 1 and 2 of SL-UDI in a supervisory role. MSI will perform the Knowledge Transfer to MSP for QA purposes~~. Independent Validation and Verification (IV&V) will be done by MSP.~~

1.4.2 This section has been deleted

1.4.3 Implementation of GoSL Data Centers*

This section has been deleted

1.4.4 Implementation of Data Centre IT operations*

This section has been deleted.

1.4.5 Implementation of IT Help Desk*

This section has been deleted.

1.5 Non-Technical Aspects Transition

1.5.1 Transition of Contracts (Termination/takeover/replacement/extension)

Process of transition: The transition is triggered either by expiry of current contracts or termination of contracts. GoSL will be the deciding authority with respect to continuation of the current contractual terms of the respective service with the MSI or re-negotiate the terms and conditions or issue a new tender for the same.

1.5.2 Transition of Documentation

The MSI coming onboard within T+15 months (where T is the start date of MSI) will setup a configuration management and a Knowledge Management system to store all the process documents, soft copy of product manuals, Architecture and Design documents and all other artifacts of SL-UDI. The MSI will also be required to secure the access to this system and provide access to it based on the GoSL Information Security policies.

1.5.3 Governance

During the course of transition of various assets and services to the MSP, the MSI and other vendors will be governed by GoSL and its policies.

1.6. Guidelines for Knowledge Transfer

This section provides broad guidelines for the Knowledge Transfer as part of the transition. The guidelines are provided for reference only and should not be considered as a definite scope of transition and/or exit management.

The Knowledge Transfer exercise will have to undergo a formal cycle of planning, preparation, execution, assessment, and closure. At each stage, the MSI and MSP will co-work and co-create the required work/activities stream and share the proposed plan with GoSL for go ahead. For assessment various methodologies may be adopted which may include reverse knowledge transfer from MSP to MSI.

NATIONAL INSTITUTE FOR SMART GOVERNMENT ON BEHALF OF

THE GOVERNMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

Ministry of Digital Economy

BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS

Volume 02 of 03 - Annexure 16: RACI Matrix

Two Stage Bidding Procedure

FOR THE

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

INVITATION FOR BIDS No: NISG/SLUDI-2025

June, 2025
Amended : January, 2026

Table of Contents

1.1 RACI MATRIX 3

1.1 RACI Matrix

Project RACI Matrix

#	Task / Activity	Responsible	Accountable	Consulted	Informed
1.	IT Infrastructure Setup	MSI	MSI	PMC	MSP & GOSL
2.	High availability Auto-scaling capacity for peak loads	MSI	MSI	PMC	MSP & GOSL
3.	Mirror of production topology and data flows	MSI	MSP	PMC	MSP & GOSL
4.	Business Continuity and Disaster Recovery, to achieve RPO ≤ 1 hour, RTO ≤ 4 hours, Failover orchestration and DR drills	MSI	MSI	PMC	MSP & GOSL
5.	Capacity Planning - Model current and projected transaction volumes (daily authentications, enrollments) and plan CPU, memory, storage, and network needs	MSI	MSI	PMC	GOSL and MSP
6.	Platform Selection – Choice of technology stack (example OS, DB, Container Orchestration Platform etc.)	MSI	MSI	GOSL	GOSL
7.	Store all IaC (for VMs etc.) in version-controlled repositories	MSI	MSI	PMC	GOSL and MSP

#	Task / Activity	Responsible	Accountable	Consulted	Informed
8.	Customization of MOSIP & development of bespoke components	MSI	MSI	PMC & GOSL	GOSL
9.	System and components testing, Integration testing, and performance testing	MSI	MSI	PMC	GOSL
10.	User Acceptance Testing & Operations Stabilization Period	GoSL & MSI	GoSL & MSP	PMC	GOSL
11.	Hardening and Baseline Configuration	MSI	MSI	PMC	GOSL
12.	- Data Centre Hosting Space including Required Caging, - Physical Infrastructure (entire non-IT), non-DC space for contact centre & helpdesk, Enrolment Centres, Service Centre - Bandwidth (Inter and Intra bandwidth connectivity to DC, DR, NOC, SOC, Helpdesk, Contact Centres, Enrolment Centres etc) , PRI Lines, Toll free Numbers, Internet Dongles and Internet Connectivity and Bandwidth & Connectivity to India Offshore Development and Support Centre " - Email Solution, Email IDs & Services - Power Extension Board - SMS Gateway and Payment Gateway	GOSL	GOSL	MSI, PMC	MSI, PMC -

#	Task / Activity	Responsible	Accountable	Consulted	Informed
13.	Network Segmentation & Security Zones	MSI	GOSL (MSP)	MSP & PMC	GOSL
14.	Zone Design and Firewall & ACLs	MSI	GOSL (MSP)	MSP & PMC	GOSL
15.	Data Residency and Sovereignty	GOSL (MSP)	GOSL (MSP)	PMC	-
16.	Local Data, HSM Keys and Tape Media Storage at Remote Site (provided by GoSL including Firesafe and Bio Metric Storage)	GOSL	GOSL	MSI, PMC	MSI, PMC -
17.	Shipping & Retrieval of Backup Tape Media to and from remote site.	MSP	MSP/ GoSL	GoSL	MSI
18.	Encryption and Key Management	GOSL (MSP)	GOSL (MSP)	MSI & PMC	-
19.	Legal, Compliance Control and Audit	GOSL (MSP)	GOSL (MSP)	MSI & PMC	-
20.	NOC Operation#	MSI	MSP	-	GOSL & PMC
21.	NOC Monitoring and Alerting##	MSP	MSI	-	GOSL & PMC
22.	SOC Operation#	MSI	MSP	-	GOSL & PMC
23.	SOC Monitoring and Alerting##	MSP	MSI	-	GOSL & PMC
24.	Contact Center Operations & Call Center Agents	MSP	MSP	GoSL	GoSL
25.	Contact Center Technical & IT Support	MSI	MSP	PMC	GoSL
26.	Threat Detection and SIEM log analysis	MSI	MSI	GOSL	GOSL
27.	SOC L3 Incident Troubleshooting and Resolution	MSI	MSP	GOSL	GOSL
28.	Collaboration with business process owners/service providers/user agencies	MSP	MSP/GOSL	-	-

#	Task / Activity	Responsible	Accountable	Consulted	Informed
29.	Component Inventory & Version Control	MSP	MSI	-	PMC & GOSL
30.	Incident Response, Escalation, and Resolution	MSP	MSI	GOSL & PMC	GOSL
31.	Security Standards & Zero trust Operation – Compliance with security & other frameworks such as ISO 27001, 27701 etc.	MSI	GOSL	PMC	-
32.	Application Performance Monitoring & Infrastructure Metrics	MSP	MSI	PMC	GOSL
33.	Training & Capacity Building	MSI	MSI	PMC & GOSL	-
34.	Knowledge Transfer & Collaboration	MSI	MSP	PMC & GOSL	GOSL
35.	Shadowing Periods - MSP staffs shadow with MSI during live operations and maintenance tasks	MSI	MSP	PMC & GOSL	GOSL
36.	1. Warranty, Support, Escalation, Device Manager for existing devices procured by GoSL. 2. Transportation of Laptops, Monitors, Biometric devices, Printers, Kits & Edge devices to Enrolment centres	MSP/GoSL	MSP/GoSL	PMC	MSI

 # NOC and SOC Technical operations will be provided by MSI under supervision of GoSL/MSP
During first year of operations, MSI and MSP will jointly work to provide monitoring and alert services.